ТРУДЫ

ИНСТИТУТА СИСТЕМНОГО ПРОГРАММИРОВАНИЯ РАН

PROCEEDINGS OF THE INSTITUTE FOR SYSTEM PROGRAMMING OF THE RAS

ISSN Print 2079-8156
Том 31 Выпуск 2

ISSN Online 2220-6426
Volume 31 Issue 2

Институт системного
программирования
им. В.П. Иванникова РАН

Москва, 2019

ИСП РАН

ISSN 2079-8156 (Print), ISSN 2220-6426 (Online)

Труды Института системного программирования РАН
Proceedings of the Institute for System Programming of the RAS

Труды ИСП РАН – это издание с двойной анонимной системой рецензирования, публикующее научные статьи, относящиеся ко всем областях системного программирования, технологий программирования и вычислительной техники. Целью издания является формирование научно-информационной среды в этих областях путем публикации высококачественных статей в открытом доступе.

Издание предназначено для исследователей, студентов и аспирантов, а также практиков. Оно охватывает широкий спектр тем, включая, в частности, следующие:

- операционные системы;
- компиляторные технологии;
- базы данных и информационные системы;
- параллельные и распределенные системы;
- автоматизированная разработка программ;
- верификация, валидация и тестирование;
- статический и динамический анализ;
- защита и обеспечение безопасности ПО;
- компьютерные алгоритмы;
- искусственный интеллект.

Журнал издается по одному тому в год, шесть выпусков в каждом томе.

Поддерживается открытый доступ к содержанию издания, обеспечивая доступность результатов исследований для общественности и поддерживая глобальный обмен знаниями.

Труды ИСП РАН реферируются и/или индексируются в:

Proceedings of ISP RAS are a double-blind peer-reviewed journal publishing scientific articles in the areas of system programming, software engineering, and computer science. The journal's goal is to develop a respected network of knowledge in the mentioned above areas by publishing high quality articles on open access.

The journal is intended for researchers, students, and practitioners. It covers a wide variety of topics including (but not limited to):

- Operating Systems.
- Compiler Technology.
- Databases and Information Systems.
- Parallel and Distributed Systems.
- Software Engineering.
- Software Modeling and Design Tools.
- Verification, Validation, and Testing.
- Static and Dynamic Analysis.
- Software Safety and Security.
- Computer Algorithms.
- Artificial Intelligence.

The journal is published one volume per year, six issues in each volume.

Open access to the journal content allows to provide public access to the research results and to support global exchange of knowledge. **Proceedings of ISP RAS** is abstracted and/or indexed in:

УДК004.45

Адрес: 109004, г. Москва, ул. А. Солженицына, дом 25.
Телефон: +7(495) 912-44-25
E-mail: info-isp@ispras.ru
Сайт: http://www.ispras.ru/proceedings/

Address: 25, Alexander Solzhenitsyn st., Moscow, 109004, Russia.
Tel: +7(495) 912-44-25
E-mail: info-isp@ispras.ru
Web: http://www.ispras.ru/en/proceedings

Содержание

Table of Contents

DOI: 10.15514/ISPRAS-2019-31(2)-0

Editorial: Special Issue on «Advanced Computing: from Theory to Practice»

[1,2,3] *A.N. Tchernykh, ORCID: 0000-0001-5029-5212 <chernykh@cicese.mx>*
[4] *A. Hadjali, ORCID: 0000-0002-4452-1647 <allel.hadjali@ensma.fr>*
[1] *Centro de Investigación Científica y Educación Superior de Ensenada*
Carretera Ensenada-Tijuana No.3918 Zona Playitas, Ensenada, Baja California, 22860, México
[2] *Ivannikov Institute for System Programming of the Russian Academy of Sciences,*
25, Alexander Solzhenitsyn st., Moscow, 109004, Russia
[3] *South Ural State University,*
Chelyabinsk, 76 Lenina St., Chelyabinsk, 454080, Russ
[4] *LIAS/ENSMA, The Laboratory of Computer Science and Automatic Control for Systems,*
Université de Poitiers, France

Abstract. This special issue contains selected papers that had been submitted to Proceedings of the Institute for System Programming of the Russian Academy of Sciences. Thirteen submissions from nine countries (England, Mexico, China, Uruguay, Spain, Pakistan, Cuba, Dominican Republic, and Russia) cover several important topics in rapidly expanding area of research and development related with Advanced Computing. Authors show a spectrum of approaches to solve complex problems such as: data-oriented scheduling, scientific workflows, cloud computing, evolutionary algorithms, content distribution networks, soft computing, parallel programming model for multicore machines, high performance computing, data mining, software birth-marking, anomaly detection, swarm robotics, neural networks, machine learning, security, secret-sharing schemes, heterogeneous distributed computing, and Internet of Things.

Keywords: data-oriented scheduling; scientific workflows; cloud computing; evolutionary algorithms; content distribution networks; soft computing; parallel programming model for multicore machines; high performance computing' data mining; software birthmarking; anomaly detection; swarm robotics; neural networks; machine learning; security; secret-sharing schemes; heterogeneous distributed computing; Internet of Things.

For citation: Tchernykh A.N., Hadjali A. Editorial: Special Issue on «Advanced Computing: from Theory to Practice». Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019, pp. 7-14 (in English and Russian). DOI: 10.15514/ISPRAS-2019-31(2)-0

This special issue contains selected papers that had been submitted to Proceedings of the Institute for System Programming of the Russian Academy of Sciences. Thirteen submissions from nine countries (England, Mexico, China, Uruguay, Spain, Pakistan, Cuba, Dominican Republic, and Russia) cover several important topics in rapidly expanding area of research and development related with Advanced Computing.

Authors show a spectrum of approaches to solve complex problems such as: data-oriented scheduling, scientific workflows, cloud computing, evolutionary algorithms, content distribution networks, soft computing, parallel programming model for multicore machines, high performance computing, data mining, software birth-marking, anomaly detection, swarm robotics, neural networks, machine learning, security, secret-sharing schemes, heterogeneous distributed computing, and Internet of Things.

The objective of this special issue is to publish and overview recent trends in the interdisciplinary areas of parallel and distributed computing, applications and technologies.

We hope that the set of selected papers provides the community with a better understanding of the current research areas, introducing new research, development, and deployment efforts in advance computing.

Papers in the first group deal with a broad spectrum of soft computing. The first paper entitled «Soft computing methods for design and optimization of cloud-based Content Distribution Networks» by Nesmachnow Cánovas S.E., Goñi Bofrisco G., Dorronsoro Díaz B., and Tchernykh A.N. deals with the application of soft computing methods for solving the problem of designing and optimizing cloud-based content distribution networks. A multi-objective evolutionary approach is applied to solve the resource provisioning problem and a greedy heuristic method to address the online routing of contents. The optimization objectives are the minimization of VM, network and storage cost, and the maximization of the QoS for the end-user. The second paper entitled «Virtual Savant for the Knapsack Problem: learning for automatic resource allocation» by Massobrio R., Dorronsoro Díaz B., and Nesmachnow Cánovas S.E. presents the application of a novel soft computing method Virtual Savant that uses machine learning techniques to compute solutions to a given optimization problem. It learns from a reference algorithm to generate a new program that can solve the same optimization problem in a massively parallel fashion. The proposed approach is evaluated to solve the Knapsack problem, which models different variants of resource allocation problems.

Papers in the second group deal with an advance of neural networks. The first paper entitled «Hybrid Model for Efficient Anomaly Detection in Short-timescale GWAC Light Curves and Similar Datasets» by Sun Y., Zhao Z., Ma X., and Du Z. studies the astronomy problem of a real-time search for short-timescale gravitational ML events from a huge number of light curves. For time series analysis and to meet the challenge of big data, the authors apply a hybrid model considering Autoregressive Integrated Moving Average (ARIMA), machine learning called Long-Short Term Memory Networks (LSTM), and neural networks. The paper entitled «The theoretical approach to the search for a global extremum in the training of neural networks Mitigating MAC Layer Performance Anomaly of Wi-Fi Networks through Adaptable Channelization» by Vershkov N.N., Kuchukov V.A., and Kuchukova N.N. deals with the training of artificial neural networks using the correlation index by the method based on a mathematical model of an artificial neural network represented as an information transmission system.

Networking problems are discussed in paper entitled «Mitigating MAC Layer Performance Anomaly of Wi-Fi Networks through Adaptable Channelization» by Hussain A., Safyan M., Ul Qayyum Z., Sarwar S., Iqbal M., Saqib N [5]. The authors propose mechanisms to mitigate the effect of MAC layer performance anomaly by using adaptable width channelization in WLANs.

Robotics vision and path planning in unknown terrain are discussed in the paper entitled «Wireless integration to optimize environmental recognition and calculate the trajectory of a group of robots» by Ivanov M.V., Sergiyenko O.Yu., Tyrsa V.V., Lindner L., Rodriguez-Quiñonez J.C., Flores-Fuentes W., Rivas-Lopez M., Hernández-Balbuena D., and Nieto Hipólito J.I. The authors study the influence of common knowledge sharing about surroundings on the robotic group navigation. They describe the structure of real-time laser technical vision system as the main environment-sensing tool for robots. Proposed the dynamic data-transferring network models the robotic swarm and group by using leader-changing system.

Efficient execution of large-scale scientific applications in cloud computing are discussed in three papers. The first paper entitled «Continuous integrating modules of distributed applied software packages in Orlando Tools» by Feoktistov A.G., Gorsky S.A., Sidorov I.A., Kostromin R.O., Fereferov E.S., and Bychkov I.V. proposes an integration of Grid and cloud computing and new approach of complex debugging, joint testing, and analysis of the execution time of software module versions in such a heterogeneous distributed computing environment. The authors combine the methodology for creating software packages with modern development practices based on continuous integration using knowledge about the specific problems. The second paper

entitled «A semi-automatic approach for parallel problem solving using the Multi-BSP model» by Alaniz M.O. and Nesmachnow Cánovas S.E. proposes parallel programming model for multicore machines that extends the classic Bulk Synchronous Parallel model. The authors introduce a semi-automatic approach for solving problems applying parallel algorithms using the Multi-BSP model and engine. They design algorithms by applying a recursive methodology over the hierarchical tree already built by the benchmark, focusing on three atomic functions based in a divide-and-conquer strategy. The third paper entitled «Data-Oriented scheduling with Dynamic-Clustering fault-tolerant technique for Scientific Workflows in Clouds» by Ahmad Z., Jehangiri A.I., Iftikhar M., Umer A.I., and Afzal I. discusses large scale scientific applications structured as scientific workflows. The authors consider task failures, deadline constraints, budget constraints, and improper management of tasks. They provide fault-tolerant techniques with data-oriented scheduling for execution of scientific workflows in cloud computing.

Application of the Internet of Things concept to the area of livestock farming is presented in the paper entitled «Internet of Things for evaluating foraging and feeding behavior of cattle on grassland-based farming systems: concepts and review of sensor technologies» by Garay Alvarez G.R., Bertot Valdés J.A., and Perez-Teruel K. The authors overview the movement, foraging and feeding ecology as well as sensors technologies that could be embedded into an IoT-based platform for Precision Livestock Farming (PLF). They classify existed techniques according to their applicability to ecological studies in the fields of foraging and feeding behavior and extend IoT to farm animals, i.e., real-time monitoring technologies aimed at managing the smallest manageable production unit's temporal variability.

Three papers in the last group deal with an advance of security. The first paper entitled «Secure and Reliable Data Transmission Over MANET Based On Principles of Computationally Secure Secret Sharing» by Chervyakov N.I., Deryabin M.A., Nazarov A.S., Babenko M.G., Kucherov N.N., Gladkov A.V., and Radchenko G.I. proposes a new approach to organizing data transfer through MANET based on node disjoint multipath routing and modular coding of data. The authors use a computationally secure secret sharing scheme based on the residue number system, which ensures the confidentiality of data and reliability of their transmission. The second paper entitled «Graphs Resemblance based Software Birthmarks through Data Mining for Piracy Control» by Sarwar S., Ul Qayyum Z., Safyan M., Iqbal M., and Mahmood Y. emphasizes the need for protecting intellectual property rights (IPR) hampered by software piracy requiring effective measures for software piracy control. The authors propose a novice birthmarking approach that is based on hybrid of text-mining and graph-mining techniques. The last paper entitled «Efficient Number Comparison in the Residue Number System based on Positional Characteristics» by Babenko M.G., Tchernykh A.N., Chervyakov N.I., Kuchukov V.A., Miranda-López V., Rivera-Rodriguez R., and Du Z. addresses homomorphic encryption that ensures the confidentiality of the stored information and performing calculations over encrypted data without preliminary decoding it. The authors propose a new efficient method to compute the positional characteristic in the positional number system to improve performance and resource consumption.

We believe that this special issue is a good representation of current issues in the context of advanced computing. As guest editors, we would like to thank the authors for their valuable contributions and the reviewers for their rigorous reviews and efforts. Special thanks to the Editor-in-Chief, Prof. A.I. Avetisyan, Corresponding member of RAS for offering us the opportunity to edit this special issue.

Предисловие к специальному выпуску «Продвинутые компьютерные методы: от теории к практике»

[1,2,3] *А.Н. Черных, ORCID: 0000-0001-5029-5212 <chernykh@cicese.mx>*
[4] *А. Хаджали, ORCID: 0000-0002-4452-1647 <allel.hadjali@ensma.fr>*
[1] *Центр научных исследований и высшего образования,*
Мексика, 22860, Нижняя Калифорния, Энсенада, ш. Тихуана-Энсенада, 3918
[2] *Институт системного программирования РАН им. В.П. Иванникова,*
109004, Россия, г. Москва, ул. А. Солженицына, д. 25.
[3] *Южно-Уральский государственный университет,*
454080, Россия, г. Челябинск, ул. Ленина, 76
[4] *Лаборатория компьютерных наук и автоматического управления системами,*
Университет Пуатье, Франция

Аннотация. В этом специальном выпуске содержатся избранные статьи, представленные в Труды Института системного программирования Российской академии наук. Тринадцать материалов из девяти стран (Англии, Мексики, Китая, Уругвая, Испании, Пакистана, Кубы, Доминиканской Республики и России) охватывают несколько важных тем в быстро расширяющейся области исследований и разработок, связанных с продвинутыми компьютерными методами. Авторы демонстрируют спектр подходов для решения сложных задач, таких как ориентированное на данные планирование, потоки научных работ, облачные вычисления, эволюционные алгоритмы, сети распространения контента, мягкие вычисления, модели параллельного программирования для многоядерных машин, высокопроизводительные вычисления, интеллектуальный анализ данных, защита авторских прав на программное обеспечение, обнаружение аномалий, групповая робототехника, нейронные сети, машинное обучение, безопасность, схемы разделения секрета, гетерогенные распределенные вычисления и Интернет вещей.

Ключевые слова: ориентированное на данные планирование; потоки научных работ; облачные вычисления; эволюционные алгоритмы; сети распространения контента; мягкие вычисления; модели параллельного программирования для многоядерных машин; высокопроизводительные вычисления; интеллектуальный анализ данных; защита авторских прав на программное обеспечение; обнаружение аномалий; групповая робототехника; нейронные сети; машинное обучение; безопасность; схемы разделения секрета; гетерогенные распределенные вычисления; Интернет вещей

Для цитирования: Черных А.Н., Хаджали А. Предисловие к специальному выпуску «Продвинутые компьютерные методы: от теории к практике». Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 7-14 (на английском и русском языках). DOI: 10.15514/ISPRAS-2019-31(2)-0

В этом специальном выпуске содержатся избранные статьи, представленные в Труды Института системного программирования Российской академии наук. Тринадцать материалов из девяти стран (Англии, Мексики, Китая, Уругвая, Испании, Пакистана, Кубы, Доминиканской Республики и России) охватывают несколько важных тем в быстро расширяющейся области исследований и разработок, связанных с продвинутыми компьютерными методами.

Авторы демонстрируют спектр подходов для решения сложных задач, таких как ориентированное на данные планирование, потоки научных работ, облачные вычисления, эволюционные алгоритмы, сети распространения контента, мягкие вычисления, модели параллельного программирования для многоядерных машин, высокопроизводительные вычисления, интеллектуальный анализ данных, защита авторских прав на программное обеспечение, обнаружение аномалий, групповая робототехника, нейронные сети, машинное

обучение, безопасность, схемы разделения секрета, гетерогенные распределенные вычисления и Интернет вещей.

Целью этого специального выпуска является краткое ознакомление читателей с последними тенденциями в междисциплинарных областях параллельных и распределенных вычислений, приложений и технологий.

Мы надеемся, что отобранные статьи помогут сообществу лучше понять текущие области исследований, познакомиться с новыми исследованиями, разработками и усилиями по внедрению продвинутых компьютерных методов.

Статьи первой группы затрагивают различные аспекты мягких вычислений. В первой статье под названием «Конструирование и оптимизация сетей распространения контента», авторами которой являются Итурриага Фабра С.Д., Несмачнов Кановас С.Е., Гони Бофриско Н., Дорронзоро Диаз Б. и Черных А.Н., рассматривается применение методов мягких вычислений для решения проблемы проектирования и оптимизации облачных сетей распространения контента. Многоцелевой эволюционный подход применяется для решения проблемы предоставления ресурсов, а жадный эвристический метод – для онлайн-маршрутизации контента. Цели оптимизации – минимизация виртуальных машин, стоимости сети и хранилища, а также максимизация качества обслуживания конечного пользователя. Вторая статья под названием «Виртуальный Эрудит для решения задачи о рюкзаке: обучение автоматическому распределению ресурсов», авторами которой являются Массобрио Р., Дорронзоро Диаз Б. и Несмачнов Кановас С.Е., представляет применение нового метода мягких вычислений «Виртуальный савант» (Virtual Savant), в котором используются методы машинного обучения для получения решения заданной задачи оптимизации. На основе эталонного алгоритма система учится генерировать новую программу, которая может решить ту же задачу оптимизации в массивно-параллельном режиме. Оценка предложенного подхода основывается на решении задачи о рюкзаке, которая моделирует различные варианты задач распределения ресурсов.

Статьи второй группы относятся к тематике нейронных сетей. В первой статье, озаглавленной «Гибридная модель для эффективного обнаружения аномалий в кратковременных последовательностях кривых блеска GWAC и аналогичных наборах данных», авторами Сан И., Жао З., Ма С. и Ду Чж. исследуется астрономическая проблема поиска в реальном времени кратковременных гравитационных ML-событий в огромном количестве кривых блеска. Для анализа временных рядов и решения проблемы больших данных авторы применяют гибридную модель, сочетающую черты метода авторегрессионной интегрированной скользящей средней (ARIMA), метода машинного обучения на основе сети с долгой краткосрочной памятью (LSTM) и методов нейронных сетей. В статье под названием «Теоретический подход к поиску глобального экстремума при обучении нейронных сетей» Вершкова Н.А., Кучукова В.А., Кучуковой Н.Н. рассматривается обучение искусственных нейронных сетей с использованием индекса корреляции на основе метода, основанного на математической модели искусственной нейронной сети, которая представляется в виде системы передачи информации.

Сетевые проблемы обсуждаются в статье «Сглаживание аномалий производительности сетей Wi-Fi на уровне MAC путем адаптивного выделения каналов» Хуссейна А., Сафьяна М., Сарвара С., Уль Кайума З., Икбала М. и Сакиба Н.А.. Авторы предлагают механизмы для сглаживания влияния аномалий производительности уровня MAC с использованием адаптивного выделения каналов в беспроводных локальных сетях.

Машинное зрение в робототехнике и планирование маршрутов роботов в неизвестной местности обсуждаются в статье «Интеграция беспроводной связи для оптимизации распознавания окружения и расчёта траектории движения группы роботов». Авторы: Иванов М.В, Сергиенко О.Ю., Тырса В.В, Линднер Л., Родригес-Киньонес Х.С., Флорес-Фуэнтес В., Ривас-Лопес М., Эрнандес-Бальбуэна Д. и Нието Иполито Х.И. В статье

изучается влияние обмена общими знаниями об окружающей среде на навигацию группы роботов. Авторы описывают структуру лазерной системы технического зрения в реальном времени как основного инструмента, чувствительного к окружающей среде роботов. Предложенная динамическая сеть передачи данных моделирует группу роботов с использованием системы смены лидеров.

Эффективное выполнение крупномасштабных научных приложений в облачных средах обсуждается в трех статьях. В первой статье под названием «Непрерывная интеграция функционального наполнения распределенных пакетов прикладных программ» Феоктистов А.Г., Горский С.А., Сидоров И.А., Костромин Р.О., Фереферов Е.С. и Бычков И.В. предлагают интеграцию grid и облачных сред, а также новый подход к комплексной отладке, совместному тестированию и анализу времени выполнения программных модулей в такой гетерогенной распределенной вычислительной среде. Авторы объединяют методологию создания пакетов программного обеспечения с современными методами разработки, основанными на непрерывной интеграции на основе знаний о конкретных проблемах. В статье «Полуавтоматический подход к параллельному решению задач с использованием модели Multi-BSP» ее авторы Аланиз М.О. и Несмачнов Кановас С.Е. предлагают модель параллельного программирования для многоядерных машин, которая расширяет классическую модель BSP (Bulk Synchronous Parallel). Авторы представляют полуавтоматический подход к решению задач на основе параллельных алгоритмов с использованием модели Multi-BSP и системы ее поддержки. Они разрабатывают алгоритмы, применяя рекурсивную методологию к иерархическому дереву, уже построенному на основе бенчмарка, концентрируясь на трех элементарных функциях и применяя стратегию «разделяй и властвуй». В третьей статье этой группы «Ориентированное на данные планирование с применением отказоустойчивого метода динамической кластеризации для поддержки научных потоков работ в облаках», авторами которой являются Ахмад З., Джехангири А.И., Ифтихар М., Умер А.И. и Афзал И. обсуждаются крупномасштабные научные приложения, структурированные как научные процессы. Авторы рассматривают сбои задач, ограничения по срокам, бюджетные ограничения и неправильное управление задачами. Они предоставляют отказоустойчивые методы с ориентированным на данные планированием для выполнения научных потоков работ в облачных средах.

Применению концепции Интернета вещей в области животноводства посвящена статья «Интернет вещей для оценки поведения крупного рогатого скота при поиске корма и кормлении в пастбищных системах земледелия: концепции и обзор сенсорных технологий», которую написали Гарай Альварес Г.Р., Бертот Вальдес Х. и Перес-Теруэль К. Авторы рассматривают экологические аспекты перемещения, кормодобывания и кормления крупного рогатого скота, а также технологии датчиков, которые могут быть встроены в основанную на Интернете вещей платформу для поддержки точного животноводства. Они классифицируют существующие методы в соответствии с их применимостью к экологическим исследованиям в области кормодобывания и кормления и распространяют технологию Интернета вещей на сельскохозяйственных животных, то есть на обеспечение мониторинга в реальном времени, помогающему управлять изменчивостью во времени наименьшей управляемой производственной единицы.

Три статьи последней группы посвящены актуальным проблемам безопасности. Статья «Безопасная и надежная передача данных в MANET на основе принципов вычислительно стойкого разделения секрета», написана Червяковым Н.И., Дерябиным М.А., Назаровым А.С., Бабенко М.Г. и Кучеровым Н.Н., Гладковым А.В. и Радченко Г.И. В ней предлагается новый подход к организации передачи данных в MANET, основанный на непересекающейся по узлам мультитрактовой маршрутизации и модульном кодировании данных. Авторы используют вычислительно безопасную схему разделения секрета, основанную на системе остаточных классов, которая обеспечивает конфиденциальность

данных и надежность их передачи. В статье Сарвара С., Уль Кайума З., Сафьяна М., Икбала М. и Махмуда Я. «Выявление характерных особенностей программ для борьбы с компьютерным пиратством на основе интеллектуального анализа графов» подчеркивается необходимость защиты прав интеллектуальной собственности (ПИС), которая затрудняет компьютерное пиратство, для борьбы с которым требуются эффективные меры. Авторы предлагают собственный подход к выявлению характерных особенностей программ (software birthmark), основанный на сочетании методов интеллектуального анализа текста и анализа графов. Последняя статья под названием «Эффективное сравнение чисел в системе остаточных классов на основе позиционных характеристик», авторами которой являются Бабенко М.Г., Черных А.Н., Червяков Н.И., Кучуков В.А., Миранда-Лопес В., Ривера-Родригес Р. и Ду Чж., посвящена гомоморфному шифрованию, которое обеспечивает конфиденциальность хранимой информации и выполнение вычислений над зашифрованными данными без предварительного их декодирования. Авторы предлагают новый эффективный метод для вычисления позиционной характеристики в позиционной системе счисления для повышения производительности и сокращения потребления ресурсов.

Мы считаем, что этот специальный выпуск хорошо отражает текущие проблемы в продвинутых компьютерных методов. Как приглашенные редакторы, мы хотели бы поблагодарить авторов за их ценный вклад и рецензентов за их работу и тщательно подготовленные рецензии. Особая благодарность главному редактору проф. А.И. Аветисяну, члену-корреспонденту РАН за предоставленную нам возможность подготовить этот специальный выпуск.

Информация об авторах / Information about authors

Андрей Николаевич ЧЕРНЫХ, приглашенный редактор выпуска, получил степень кандидата наук в Институте точной механики и вычислительной техники РАН. В настоящее время он является профессором Центра научных исследований и высшего образования в Энсенаде, Нижняя Калифорния, Мексика. В научном плане его интересуют многоцелевая оптимизация распределения ресурсов в облачной среде, проблемы безопасности, планирования, эвристики и метаэвристики, энергосберегающие алгоритмы, интернет вещей и т.д.

Andrei TCHERNYKH, guest editor of this issue, received his PhD degree at the Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences. Now he is holding a full professor position in computer science at CICESE Research Center, Ensenada, Baja California, Mexico. He is interesting in grid and cloud research addressing multi-objective resource optimization, both, theoretical and experimental, security, uncertainty, scheduling, heuristics and meta-heuristics, adaptive resource allocation, energy-aware algorithms and Internet of Things.

Аллел ХАДЖАЛИ, приглашенный редактор выпуска, получил степень PhD в Университете Поля Сабатье, Тулуза, Франция. В настоящее время он является профессором Лаборатории компьютерных наук и автоматического управления системами, Университет Пуатье, Франция. Его научные интересы включают использование и анализ данных большого объема, извлечение данных, рекомендательные системы, качество данных, методы вычислительного интеллекта в системах поддержки принятия решений.

Allel HADJALI, guest editor of this issue, received his PhD degree at the University Paul Sabatier, Toulouse 3, France. Currently, he is a professor at the The Laboratory of Computer Science and Automatic Control for Systems, Université de Poitiers, France . He is interesting in massive data exploitation and analysis, data extraction, recommendation systems, data quality, computational intelligence techniques in decision making.

DOI: 10.15514/ISPRAS-2019-31(2)-1

Конструирование и оптимизация сетей распространения контента

[1] *С.Д. Итурриага Фабра, ORCID: 0000-0002-0212-7916 <siturria@fing.edu.uy>*
[1] *С.Е. Несмачнов Кановас, ORCID: 0000-0002-8146-4012 <sergion@fing.edu.uy>*
[1] *Н. Гони Бофриско, ORCID: 0000-0002-4552-9210 <gerardo.goni@fing.edu.uy>*
[2] *Б. Дорронзоро Диаз, ORCID: 0000-0003-0481-790X <bernabe.dorronsoro@uca.es>*
[3,4,5] *А.Н. Черных, ORCID: 0000-0001-5029-5212 <chernykh@cicese.mx>*

[1] *Республиканский университет,*
Уругвай, 11300, Монтевидео, ул. Хулио Эррера-и-Рейссиг, 565
[2] *Кадисский университет,*
Испания, 11001, Кадис, ул. Анча, 16
[3] *Центр научных исследований* и *высшего образования,*
Мексика, 22860, Нижняя Калифорния, Энсенада, ш. Тихуана-Энсенада, 3918
[4] *Институт системного программирования РАН им. В.П. Иванникова,*
109004, Россия, г. Москва, ул. А. Солженицына, д. 25.
[5] *Южно-Уральский государственный университет,*
454080, Россия, г. Челябинск, ул. Ленина, 76

Аннотация. В данной статье представлено применение мягких вычислительных методов для решения задачи проектирования и оптимизации облачных сетей распространения контента (CDN). Для решения проблемы выделения ресурсов для построения сетевой инфраструктуры применяется многоцелевой подход с учетом цели минимизации стоимости виртуальных машин, сети и хранилища, а также максимизации качества обслуживания, предоставляемого конечным пользователям. Предлагается конкретная модель посредничества, которая позволяет одной облачной CDN размещать нескольких поставщиков контента, применяющих стратегию совместного использования ресурсов. На основе предложенной модели посредничества изучаются три многоцелевых эволюционных подхода оффлайновой оптимизации предоставления ресурсов, а для решения проблемы онлайновой маршрутизации контента предлагается жадный эвристический метод. Экспериментальная оценка предложенного подхода выполняется на наборе реалистичных частных случаев. Полученные экспериментальные результаты показывают, что предложенный подход эффективен для проектирования и оптимизации облачных сетей распространения контента: общие затраты снижаются на 10,34% при сохранении высокого уровня качества обслуживания.

Ключевые слова: облачные вычисления; оптимизация; эволюционные алгоритмы; сети распространения контента

Для цитирования: Итурриага Фабра С.Д., Несмачнов Кановас С.Е., Гони Бофриско Н., Дорронзоро Диаз Б., Черных А.Н. Конструирование и оптимизация сетей распространения контента. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 15-20. DOI: 10.15514/ISPRAS-2019-31(2)-1

Design and optimization of Content Distribution Networks

[1] *S.D. Iturriaga Fabra, ORCID: 0000-0002-0212-7916 <siturria@fing.edu.uy>*
[1] *S.E. Nesmachnow Cánovas, ORCID: 0000-0002-8146-4012 <sergion@fing.edu.uy>*
[1] *G. Goñi Bofrisco, ORCID: 0000-0002-4552-9210 <gerardo.goni@fing.edu.uy>*
[2] *B. Dorronsoro Díaz, ORCID: 0000-0003-0481-790X <bernabe.dorronsoro@uca.es>*
[3,4,5] *A.N. Tchernykh, ORCID: 0000-0001-5029-5212 <chernykh@cicese.mx>*
[1] *Universidad de la República*
Julio Herrera y Reissig 565, Montevideo, 11300, Uruguay
[2] *Universidad de Cádiz*
C/Ancha 16, Cádiz, 11001, Spain
[3] *Centro de Investigación Científica y Educación Superior de Ensenada*
Carretera Ensenada-Tijuana No.3918 Zona Playitas, Ensenada, Baja California, 22860, México
[4] *Ivannikov Institute for System Programming of the Russian Academy of Sciences,*
25, Alexander Solzhenitsyn st., Moscow, 109004, Russia
[5] *South Ural State University,*
Chelyabinsk, 76 Lenina St., Chelyabinsk, 454080, Russia

Abstract. This article presents the application of soft computing methods for solving the problem of designing and optimizing cloud-based Content Distribution Networks (CDN). A multi-objective approach is applied to solve the resource provisioning problem for building the infrastructure for the network, considering the objectives of minimizing the cost of the virtual machines, network, and storage, and the maximization of the quality-of-service provided to end-users. A specific brokering model is proposed to allow a single cloud-based CDN to be able to host multiple content providers applying a resource sharing strategy. Following the proposed brokering model, three multiobjective evolutionary approaches are studied for the offline optimization of resource provisioning and a greedy heuristic method is proposed for addressing the online routing of contents. The experimental evaluation of the proposed approach is performed over a set of realistic problem instances. The obtained experimental results indicate that the proposed approach is effective for designing and optimizing cloud-based Content Distribution Networks: total costs are reduced by up to 10.34% while maintaining high quality-of-service values.

Keywords: cloud computing; optimization; evolutionary algorithms; content distribution networks.

For citation: Iturriaga Fabra S.D., Nesmachnow Cánovas S.E., Goñi Bofrisco G., Dorronsoro Díaz B., Tchernykh A.N. Soft computing methods for design and optimization of cloud-based Content Distribution Networks. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 15-20 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-1

1. Введение

Термин «сеть распространения контента» (Content Distribution Network, CDN), часто заменяемый термином «сеть доставки контента» (content delivery network), используется для обозначения распределенных сетей для доставки услуг и контента пользователям. CDN являются ключевыми инфраструктурами для эффективного предоставления по всему миру масштабируемых интернет-услуг, способными соответствовать конкретным соглашениям об уровне обслуживания между поставщиками услуг и конечными пользователями, что позволяет обеспечивать высокое качество обслуживания (Quality of Service, QoS). Основной целью CDN является распространение контента среди конечных пользователей с высокой доступностью и высокой производительностью. Для достижения этой цели CDN должна включать большое число серверов, распределенных по центрам обработки данных по всему миру. Поскольку требуется большая компьютерная инфраструктура, бизнес-модель CDN экономически невыгодна для небольших поставщиков контента, у которых нет собственных центров обработки данных или подобных крупных вычислительных систем. Традиционным решением этой проблемы, позволяющим создать прибыльную бизнес-модель для небольших поставщиков контента, является аренда услуг CDN у крупных поставщиков

CDN. Однако в последние пять лет наблюдается растущая тенденция к использованию глобальной распределенности и эластичности облачных сервисов для создания облачных CDN [1,2,3,4]. Одной из основных проблем подхода облачных CDN является предоставление необходимых ресурсов в облаке. Это хорошо известная трудная проблема, которая была свойственна большинству облачных программных решений [5].

Мы представляем подход к решению проблемы предоставления ресурсов облачному поставщику CDN. Подход основан на учете точек зрения как поставщика облачных услуг, так и конечных пользователей. В базовой модели предлагается одновременная оптимизация системных и пользовательских метрик, что расширяет общие подходы, представленные в предыдущих работах из соответствующих литературных источников. Вводится многоцелевая модель оптимизации для учета затрат на одновременную оптимизацию, включая расходы на аренду виртуальных машин (ВМ), ресурсов хранения данных и обеспечения требуемой пропускной способности сети, а также QoS, предоставляемое конечным пользователям.

В предлагаемой модели учитываются некоторые особенности современных облачных платформ, в том числе, географическое расположение ресурсов, наличие скидок на оптовые покупки и возможность аренды зарезервированных экземпляров. Кроме того, представлена общая бизнес-модель, включающая понятие агента виртуального брокера [6], где брокер использует мультитенантный подход для снижения затрат на одновременное управление несколькими поставщиками контента. Эта мультитенантная модель позволяет брокеру воспользоваться льготными ценами для массовых виртуальных машин и стратегиями совместного использования ресурсов.

Мы разработали три многоцелевых эволюционных алгоритма (MultiObjective Evolutionary Algorithm, MOEA) для решения проблемы предоставления облачных ресурсов и жадный эвристический алгоритм для решения подзадачи маршрутизации запросов контента. Предложенные алгоритмы оцениваются на наборе реалистичных примеров, построенных с использованием методологии, предложенной Бусари и др. [7]. Эта методология учитывает несколько общих характеристик, выявленных в рабочих нагрузках Web, таких как Zipf-подобное распределение популярности контента, распределение «с тяжелым хвостом» (heavy-tailed) размеров контента большого количества контента, к которому обращаются только один раз

2 Сравнение предлагаемой бизнес-модели с обычной бизнес-моделью

В традиционной бизнес-модели (Business As Usual, BAU) отсутствует сущность «брокер». В такой модели каждый поставщик контента должен развернуть свою собственную индивидуальную облачную CDN. В этом разделе мы представляем экономию бюджета, рассчитанного по предлагаемой нами модели, по сравнению с моделью BAU. В большинстве реальных сценариев нас будут интересовать решения с высоким качеством обслуживания. Поэтому для сравнения мы будем принимать во внимание только решения с QoS от 0,95 и выше.

На рис. 1 представлена средняя экономия расходов, получаемая при применении предлагаемой нами модели, по сравнению с моделью BAU.

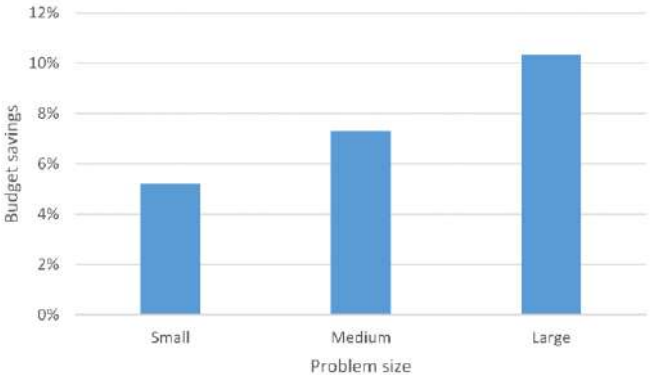


Рис. 1. Средняя экономия расходов на обеспечение решений с высоким качеством обслуживания (QoS≥0,95) по сравнению с обычным сценарием бизнеса

Fig. 1. Average budget savings of computed high quality of service solutions (QoS≥0.95) when compared to a business as usual scenario.

Результаты показывают уменьшение экономии при уменьшении размера решаемой задачи. Это связано с тем, что чем крупнее задача, тем больше возможностей для ее улучшения ее решения. Наш подход наиболее эффективен при работе с крупноразмерными задачами, вычислительными решениями со средней экономией бюджета на 10,34 ± 0,21%. Для задач среднего размера расчетная средняя экономия бюджета составляет 7,30 ± 0,19%, а для небольших - 5,21 ± 0,26%. Результаты показывают, что наша система бизнес-модели и алгоритм планирования обеспечивают экономию бюджета в среднем примерно на 7,6%.

3 Заключение и планы на будущее

В данной работе рассматривается многоцелевая проблема предоставления ресурсов в облаке для создания облачной CDN. Цели оптимизации – минимизация виртуальных машин, стоимости сети и хранилища, а также максимизация QoS для конечного пользователя.

Рассматривается модель мультитенантного брокера, когда в одной облачной CDN может размещаться несколько поставщиков контента. Введен новый объект – брокер, служащий для управления мультитенантной облачной CDN. Предлагается точная математическая формулировка, а набор примеров строится в соответствии с реалистичной методологией, представленной Бусари и др. [7].

Из-за своей сложности предложенная задача разделена на две подзадачи, для решения которых требуются алгоритмы оптимизации. Одной из подзадач является предоставление облачных ресурсов, а другой – онлайн-маршрутизация запросов контента. Сравнение предлагаемой модели брокерства с моделью BAU показывает, что наш подход способен снизить стоимость облачных ресурсов на 5,2-10,3% при сохранении высоких значений QoS. Эти результаты говорят о том, что предлагаемый нами подход достаточен для развертывания облачных CDN с меньшим бюджетом по сравнению с моделью BAU.

Основные направления будущей работы включают создание более широкого набора частных случаев и построение более точной функции QoS. С одной стороны, больший набор примеров обеспечит более глубокое понимание эффективности предложенной модели. С другой стороны, более точная функция QoS, основанная, например, на фактических измерениях сети, поможет обеспечить более реалистичные решения

Список литературы / References

[1] Gao G., Zhang W., Wen Y., Wang Z., Zhu W. Towards Cost-Efficient Video Transcoding in Media Cloud: Insights Learned from User Viewing Patterns. IEEE Transactions on Multimedia, vol. 17, no. 8, 2015, pp. 1286–1296.

[2] Hu M., Luo J., Wang Y., Veeravalli B. Practical resource provisioning and caching with dynamic resilience for cloud-based content distribution networks. IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, 2014, pp. 2169–2179.

[3] Jokhio F., Ashraf A., Lafond S., Lilius J. A computation and storage trade-off strategy for cost-efficient video transcoding in the cloud. In Proc. of the 39th Euromicro Conference Series on Software Engineering and Advanced Applications, 2013, pp. 365–372.

[4] Xiao W., Bao W., Zhu X., Wang C., Chen L., Yang L.T. Dynamic request redirection and resource provisioning for cloud-based video services under heterogeneous environment. IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 7, 2016, pp. 1954–1967.

[5] Zhang J., Huang H., Wang X. Resource provision algorithms in cloud computing: A survey. Journal of Network and Computer Applications, vol. 64, 2016, pp. 23–42.

[6] Nesmachnow S., Iturriaga S., Dorronsoro B. Efficient heuristics for profit optimization of virtual cloud brokers. IEEE Computational Intelligence Magazine, vol. 10, no. 1, 2015, pp. 33-43.

[7] Busari M., Williamson C. ProWGen: a synthetic workload generation tool for simulation evaluation of web proxy caches. Computer Networks, vol. 38, no. 6, 2002, pp. 779 – 794.

Информация об авторах / Information about authors

Сантьяго Дамиан ИТУРРИАГА ФАБРА получил степень PhD в области компьютерных наук в Республиканском университете в 2018 г. В настоящее время он является штатным исследователем и учебным ассистентом в Институте компьютерных наук Инженерного факультете Республиканского университета в Монтевидео, Уругвай. Его основные научные интересы включают в себя методы высокопроизводительных вычислений и метаэвристики для решения задач оптимизации.

Santiago Damian ITURRIAGA FABRA obtained Ph.D. degree in computer science from Universidad de la República (Uruguay) in 2017. Now he is the full-time researcher and teaching assistant at the Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Uruguay. His main research interests include high performance computing and metaheuristics methods for solving optimization problems.

Серджо Энрике НЕСМАЧНОВ КАНОВАС обладает степенью PhD в области компьютерных наук, полученной в Республиканском университете, Уругвай. В настоящее время он занимает должность профессора в Вычислительном центре Института компьютерных наук Инженерного факультета Республиканского университета. Основные научные интересы: параллельные и распределенные вычисления, научные вычисления, эволюционные алгоритмы и метаэвристика, а также численные методы.

Sergio Enrique NESMACHNOW CÁNOVAS has a Ph.D. degree in Computer Science from Universidad de la República, Uruguay. He currently holds an Aggregate Professor position in the Numerical Center (CeCal) at Computer Science Institute, Engineering Faculty. His main research interests are parallel and distributed computing, scientific computing, evolutionary algorithms and metaheuristics, and numerical methods.

Херардо ГОНИ БОФРИСКО выполняет исследования в Центре информационных технологий Республиканского университета. Его основным научным интересом являются компьютерные сети.

Gerardo GOÑI BOFRISCO does research in Computer Engineering at Servicio Central de Informática of Universidad de la República. His main research interest is computer networking.

Бернабе ДОРРОНСОРО ДИАЗ получил степень PhD в университете Малаги, Испания. В настоящее время он является научным сотрудником факультета компьютерных наук и

инженерии Кадисского университета. Он удостоен стипендии Рамона-и-Кахала в Кадисском университете, Испания. В число его научных интересов входят автоматическое программирование, многоцелевая оптимизация, машинное обучение, управление ресурсами в центрах данных, облачные вычисления, эволюционные алгоритмы и т.д.

Bernabé DORRONSORO DÍAZ has a Ph.D. degree in Computer Science from University of Málaga. Currently he is a researcher assistant at the Computer Science Engineering Department of the University of Cadiz, Spain. He is the Ramón y Cajal Fellow at University of Cádiz. His research interests include automatic programming, multi- and many-objective optimization, exact approaches, machine learning, resource management for data-centers, cloud computing, sustainable computing, evolutionary algorithms, ets.

Андрей Николаевич ЧЕРНЫХ получил степень кандидата наук в Институте точной механики и вычислительной техники РАН. В настоящее время он является профессором Центра научных исследований и высшего образования в Энсенаде, Нижняя Калифорния, Мексика. В научном плане его интересуют многоцелевая оптимизация распределения ресурсов в облачной среде, проблемы безопасности, планирования, эвристики и метаэвристики, энергосберегающие алгоритмы, интернет вещей и т.д.

Andrei TCHERNYKH received his PhD degree at the Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences. Now he is holding a full professor position in computer science at CICESE Research Center, Ensenada, Baja California, Mexico. He is interesting in grid and cloud research addressing multi-objective resource optimization, both, theoretical and experimental, security, uncertainty, scheduling, heuristics and meta-heuristics, adaptive resource allocation, energy-aware algorithms and Internet of Things.

DOI: 10.15514/ISPRAS-2019-31(2)-2

Virtual Savant for the Knapsack Problem: learning for automatic resource allocation

[1,2] *R. Massobrio, ORCID: 0000-0002-0040-3681 <renzom@fing.edu.uy>*
[1] *B. Dorronsoro Díaz, ORCID: 0000-0003-0481-790X <bernabe.dorronsoro@uca.es>*
[2] *S.E. Nesmachnow Cánovas, ORCID: 0000-0002-8146-4012 <sergion@fing.edu.uy>*
[1] *Universidad de Cádiz, Av. de la Universidad, 10, 11519, Cádiz, España*
[2] *Universidad de la República, Herrera y Reissig 565, 11300, Montevideo, Uruguay*.

Abstract. This article presents the application of Virtual Savant to solve resource allocation problems, a widely-studied area with several real-world applications. Virtual Savant is a novel soft computing method that uses machine learning techniques to compute solutions to a given optimization problem. Virtual Savant aims at learning how to solve a given problem from the solutions computed by a reference algorithm, and its design allows taking advantage of modern parallel computing infrastructures. The proposed approach is evaluated to solve the Knapsack Problem, which models different variant of resource allocation problems, considering a set of instances with varying size and difficulty. The experimental analysis is performed on an Intel Xeon Phi many-core server. Results indicate that Virtual Savant is able to compute accurate solutions while showing good scalability properties when increasing the number of computing resources used.

Keywords: virtual savant; machine learning; parallel computing; resource allocation; knapsack problem; many-core.

For citation: Massobrio R., Dorronsoro Díaz B., Nesmachnow Cánovas S.E. Virtual Savant for the Knapsack Problem: learning for automatic resource allocation. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 21-32. DOI: 10.15514/ISPRAS-2019-31(2)-2

Acknowledgements. The work of Renzo Massobrio and Sergio Nesmachnow is partly supported by ANII and PEDECIBA, Uruguay. The work of Renzo Massobrio is partly supported by Fundación Carolina, Spain. Bernabé Dorronsoro acknowledges the Spanish MINECO and ERDF for the support provided under contracts TIN2014-60844-R (the SAVANT project) and RYC-2013-13355.

Виртуальный Эрудит для решения задачи о рюкзаке: обучение автоматическому распределению ресурсов

[1,2] *Р. Массобрио, ORCID: 0000-0002-0040-3681 <renzom@fing.edu.uy>*
[2] *Б. Дорронзоро Диаз, ORCID: 0000-0003-0481-790X <bernabe.dorronsoro@uca.es>*
[1] *С.Е. Несмачнов Кановас, ORCID: 0000-0002-8146-4012 <sergion@fing.edu.uy>*
[1] *Республиканский университет,*
Уругвай, 11300, Монтевидео, ул. Хулио Эррера-и-Рейссиг, 565
[2] *Кадисский университет,*
Испания, 11001, Кадис, ул. Анча, 16

Аннотация. В этой статье представлено применение метода Виртуального Эрудита (Virtual Savant) для решения проблем распределения ресурсов, широко изученной области с несколькими реальными приложениями. Virtual Savant – это новый метод мягких вычислений, в котором используются методы машинного обучения для вычисления решений данной проблемы оптимизации. Цель Virtual Savant – научиться решать данную проблему с помощью решений, рассчитанных по эталонному алгоритму, а

его дизайн позволяет использовать преимущества современных параллельных вычислительных инфраструктур. Предложенный подход оценивается на решении задачи о рюкзаке, которая моделирует различные варианты задач распределения ресурсов, учитывая набор экземпляров разного размера и сложности. Экспериментальный анализ проводился на многоядерном сервере Intel Xeon Phi. Результаты показывают, что Virtual Savant способен вычислять точные решения, демонстрируя хорошие свойства масштабируемости при увеличении объема используемых вычислительных ресурсов.

Ключевые слова: виртуальный эрудит; машинное обучение; параллельная обработка; распределение ресурсов; задача о рюкзаке; многоядерные процессоры

Для цитирования: Массобрио Р., Дорронзоро Диаз Б., Несмачнов Кановас С.Е. Виртуальный Эрудит для решения задачи о рюкзаке: обучение автоматическому распределению ресурсов. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 21-32 (на английском языке). DOI: 10.15514/ISPRAS-2019-31(2)-2

Благодарности. Работа Р. Массобрио и С. Несмачнова частично поддерживается ANII и PEDECIBA, Уругвай. Работа Р. Массобрио частично поддерживается Фондом Каролина, Испания. Б. Дорронсоро благодарит испанские фонды MINECO и ERDF за поддержку, предоставляемую по контрактам TIN2014-60844-R (проект SAVANT) и RYC-2013-13355.

1. Introduction

Resource allocation refers to the assignment of a number of available resources or assets to different issues or items. Resource allocation is an important concept that models several situations and problems arising in economics, strategic planning, project management, scheduling, logistics, production, engineering, and many other related areas [1].

Many resource allocation problems are modeled by the general framework formulated by the Knapsack Problem (Knapsack Problem) [2]. Knapsack Problem is a combinatorial optimization problem that, given a set of items with associated weights and profits, proposes determining the number of each item to include in a collection (i.e., the knapsack) in order to maximize the total profit while ensuring that the total weight is less than or equal to a given limit (i.e., the knapsack capacity). Different allocation problems are modeled by considering the capacity of the knapsack as the available amount of a given resource and the items as activities to which the resource can be allocated.

This article describes a generic paradigm that proposes applying a computational intelligence approach to find accurate solutions to resource allocation problems modeled by the 0/1 Knapsack Problem in short computation times. 0/1 Knapsack Problem is a binary version of the Knapsack Problem where each item is considered as an atomic unit, i.e., each item can be included in the knapsack as a unit or discarded (i.e., it cannot be split to fill the knapsack). This binary version of the Knapsack Problem allows modeling interesting resource allocation problems such as activities in project management, scheduling and location problems, feature selection, among others.

The Virtual Savant paradigm is applied to solve the 0/1 Knapsack Problem, which models allocation problems. Virtual Savant is a novel method that uses machine learning techniques to learn how a reference algorithm solves a given problem [3]. Virtual Savant is inspired by the savant syndrome, a rare condition in which a human demonstrates mnemonic or computing abilities far superior to what would be considered normal. As an example, some patients with savant syndrome (*savants*) are able to enumerate and identify huge prime numbers without the underlying knowledge of what a prime number is, or accurately determine the day of the week of a given date extremely fast. Reported evidence suggests that patients with savant syndrome use pattern recognition in order to efficiently solve problems [4,5,6].

The Virtual Savant paradigm proposes applying a learning approach using computational intelligence to predict the results computed by a reference algorithm that solves a given problem [7,3]. Virtual Savant receives as input a set of problem instances and the results computed by the

reference algorithm, which is used to train a machine learning classifier. Once the training phase is completed, Virtual Savant can be applied to solve new, unknown, and even larger problem instances.

In this way, the Virtual Savant paradigm aims at learning the behavior of a given resolution algorithm in order to generate a completely different program that reproduces an analogous but unknown process to compute accurate results for the same problem. Furthermore, the resulting generated program is lightweight and can take advantage of modern massively parallel computing architectures to provide a fast and powerful problem solving schema.

Following previous works [8,9], this article describes a deeper study on how to solve the 0/1 Knapsack Problem using Virtual Savant. The first evaluation of Virtual Savant in a parallel environment (Intel Xeon Phi 7250 server) to solve the 0/1 Knapsack Problem is presented. The accuracy of the proposed approach is studied as well as its parallel capabilities and performance on a many-core computing environment. Experimental results when solving 0/1 Knapsack Problem instances of varying size and difficulty suggest that the proposed approach is able to compute competitive solutions while showing good scalability properties when increasing the number of processing elements.

The article is organized as follows. Section 2 presents the 0/1 Knapsack Problem formulation, introduces Virtual Savant and presents an overview of the related literature. Section 3 outlines the application of Virtual Savant to the 0/1 Knapsack Problem. Section 4 presents the experimental evaluation of the proposed approach and, finally, Section 5 presents the conclusions and main lines of future work.

2. Problem and method

This section introduces the 0/1 knapsack problem, describes the Virtual Savant paradigm, and presents a review of the related literature.

2.1 0/1 Knapsack Problem formulation

The 0/1 Knapsack Problem is a classic combinatorial optimization problem which is proven to be *NP*-hard [10]. The mathematical formulation is as follows. Given a set I of items, each with a profit p_i and a weight w_i, the 0/1 Knapsack Problem consists in finding a subset of items that maximizes the total profit, without exceeding the weight capacity W of the knapsack.

Eq. 1 shows the problem formulation, where $x_i \in \{0,1\}$ indicates whether item i is included or not in the knapsack.

$$argmax \left\{ \sum_{i=1}^{n} p_i x_i \left| \sum_{i=1}^{n} w_i x_i \leq W \right. \right\} \quad (1)$$

Despite its straightforward formulation, the 0/1 Knapsack Problem has a large solution space and is frequently used as a benchmark to evaluate optimization algorithms. Additionally, the 0/1 Knapsack Problem can be used to model several optimization problems with direct real-world applications in many fields.

In the context of this work, the 0/1 Knapsack Problem is useful to evaluate the Virtual Savant paradigm for several reasons: i) it is a *NP*-hard optimization problem; ii) it allows studying the behavior of Virtual Savant in problems with binary variables and simple constraints; iii) a large dataset of problem instances is publicly available with varying size and difficulty.

2.2 Virtual Savant

Virtual Savant is a novel paradigm to automatically generate programs that solve optimization problems in a massively parallel fashion [11]. The paradigm is inspired by the savant syndrome, a rare condition in which a person with significant mental disabilities has certain abilities far in excess of what would be considered normal [5]. People with this condition (*savants*) usually excel at one specific skill such as art, memory, rapid calculation, or musical abilities. The methods used

by savants to solve problems are not fully understood due to the difficulties in communicating with them, since the syndrome is usually associated with autism. The main hypothesis states that savants learn through pattern recognition [4]. This mechanism allows savants to solve a given problem without understanding the underlying principles (e.g., being able to enumerate prime numbers without understanding what a prime number is).

In analogy to the savant syndrome, Virtual Savant consists in training a machine learning classifier to automatically learn how to solve an optimization problem from a set of observations, which are usually obtained from a reference algorithm that solves the same problem. Once the training phase is completed, Virtual Savant can emulate the reference algorithm to solve new, unknown, and even larger problem instances, without the need of any further training. The Virtual Savant paradigm consists of two phases: *classification*, where results for unknown problem instances are predicted, and *improvement*, where predicted results are further improved using specific search procedures.

2.3 Related work

The 0/1 Knapsack problem has been widely studied in the operations research field. Nemhauser and Ullman [12] presented an exact algorithm to solve the 0/1 Knapsack Problem based on dynamic programming. The proposed algorithm was devised to solve capital allocation problems with constrained budgets, in the field of economics. Later, an optimized implementation of the original Nemhauser-Ullman algorithm was proposed by Harman et al. [13]. This version was applied to solve instances of the Next Release Problem, an optimization problem from software engineering where the goal is to determine the features to include in a new release of a given software product [14]. The optimized implementation by Harman et al. is used in our work to train the proposed Virtual Savant for 0/1 Knapsack Problem.

Few articles were found in the related literature applying machine learning techniques to solve optimization problems, in line with the Virtual Savant proposal.

Vinyals et al. [15] introduced Pointer Networks (*ptr-nets*), a model based on recurrent neural networks. Similarly to the approach applied in Virtual Savant, *ptr-nets* are trained by observing solved instances of a given problem and the proposed scheme is also able to deal with variable size outputs. The proposed model was applied to solve three different discrete combinatorial optimization problems: finding planar convex hulls, computing Delaunay triangulations, and solving the planar Travelling Salesman Problem. Experimental results indicated that the trained models were able to address problem instances larger than those seen during training and find competitive results for the studied problems.

More recently, Hu et al. [16] applied a similar approach to the one proposed by Vinyals et al. to the three-dimensional bin packing problem, a specific variant of an allocation problem. A deep reinforcement learning approach is used to decide the sequence to pack items in a bin, while the empty space and the spatial orientation in which the items are placed inside the bin are calculated by heuristic methods. The reported experimental results showed that the proposed approach outperformed a specific heuristic for the problem. Improvements of 5% on average over the baseline results were obtained for the problem instances studied.

Our previous works were able to obtain promising results when applying Virtual Savant to a task scheduling problem [17,18,7,11]. The application of Virtual Savant to the 0/1 Knapsack Problem has been previously studied in [8,9]. This article extends those two previous works by evaluating the parallel capabilities of the Virtual Savant model in a many-core parallel infrastructure.

3. Virtual Savant for the 0/1 Knapsack Problem

This section describes the application of the Virtual Savant paradigm to the 0/1 Knapsack Problem. The Virtual Savant implementation for the 0/1 Knapsack Problem uses Support Vector Machines (SVMs) for the classification phase. SVMs are trained using Nemhauser-Ullmann as a reference algorithm, which computes exact solutions for the 0/1 Knapsack Problem [13]. Each

item of the problem instance is considered individually during the training phase of Virtual Savant. Therefore, each feature vector holds the weight and profit of the item, along with the capacity of the knapsack. The classification label is 0/1, indicating whether the reference algorithm included (or not) the item in the knapsack. Thus, a single solution of the reference algorithm provides as many observations as the number of items in the instance. The LIBSVM framework with a Radial Basis Function kernel was used [19]. A specific fork of the LIBSVM package was designed to improve training times on many-core architectures [20]. Fig. 1 outlines the training scheme for Virtual Savant to solve the 0/1 Knapsack Problem.

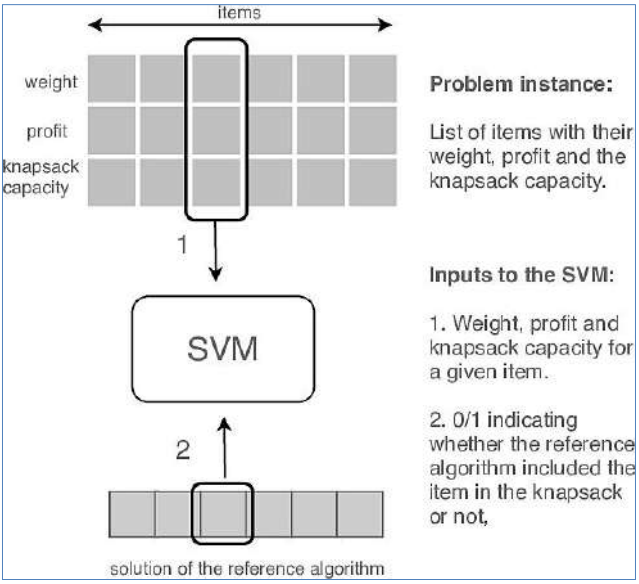


Fig. 1. Training scheme of Virtual Savant for the 0/1 Knapsack Problem

Fig. 2 presents the complete model of Virtual Savant to solve the 0/1 Knapsack Problem. Once the learning process is completed, Virtual Savant uses (in parallel) multiple instances of the trained SVM to predict whether or not to include each item in the knapsack. These decisions are independent for each item, providing Virtual Savant with a high degree of parallelism. The output of the classification phase is a vector that holds, for each item, the probability of including it in the knapsack. Since the length of the training vectors is fixed (3 features + 1 label), there is no need to re-train the SVM to solve problem instances of different size (i.e., with varying number of items). This allows Virtual Savant to easily scale to problem instances of larger dimensions, without requiring any additional training process.

The improvement phase takes as input the resulting vector of probabilities computed in the prediction phase. One candidate solution is generated per computing resource available, by randomly sampling according to the probabilities of including each item. Finally, a local search heuristic is applied over each generated solution. The local search operator considered in this work is very simple, just performing random modifications on the items to include or not. On each step of the local search, a randomly-chosen bit in the solution is flipped, the new solution is evaluated, and the local search continues from that solution if an improvement is made. Algorithm 1 describes the method to evaluate the score of a solution in the local search procedure, considering a solution with profit P, weight W, overweight $O = W - C$, where C is the knapsack capacity; $k > 0$; $m \in (0,1)$. P, W, and O are scaled using the minimum and maximum weight and profit values in the problem instance. The improvement phase, as well as the prediction phase, is

massively parallel, since more local searches can be spawned as more computing resources are available.

Algorithm 1. Score assignment for solutions during the local search

```
input: solution, instance
scale (W, P, O, C, instance)
if O≤0 then
   return P
else if O ≤ m · C then
   return P − k · O
else
   return −O
```

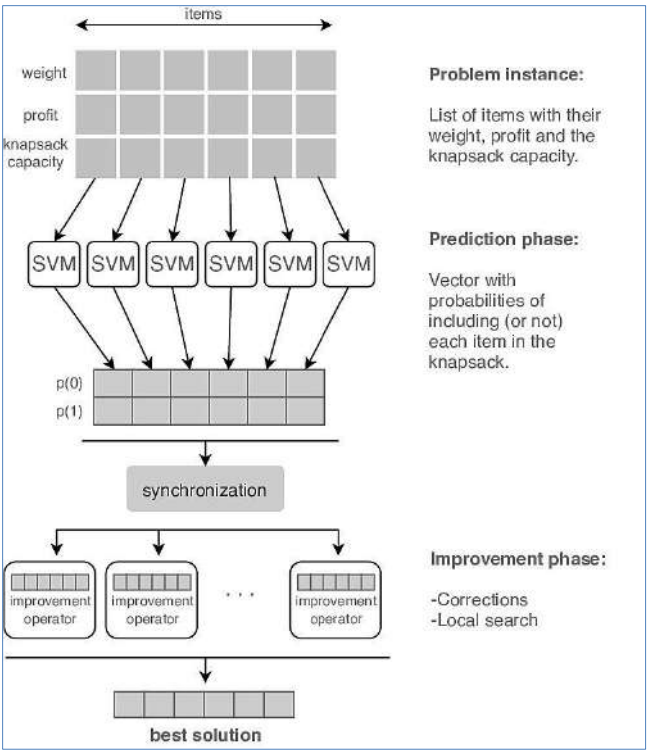


Fig. 2. Model of Virtual Savant applied to the 0/1 Knapsack Problem

Two corrections schemes are included in the improvement phase in order to ensure that the returned solution satisfies the knapsack capacity restriction:

- *Greedy correction by profit (CP)*: iteratively removes the item with lower benefit until the total weight is lower than, or equal to, the knapsack capacity.
- *Greedy correction by weight (CW)*: iteratively searches for the items with weight higher than, or equal to, the overweight of the solution and removes the one with the lowest weight among them. If no item satisfies this condition, it removes the one with the highest weight.

The corrections are applied to each tentative solution after the local search, to ensure that the

returned solution satisfies the knapsack capacity constraint. After all local searches and corrections are completed, the overall best solution found is returned.

4. Experimental analysis

This section reports the experimental analysis of the proposed Virtual Savant for the 0/1 Knapsack Problem.

4.1 Problem instances

The evaluation was performed over benchmark problem instances with different size and correlation between weight and profit of items. The correlation is related to the difficulty to solve an instance [13]. The benchmark includes 50 datasets, each with instances of size 100 to 1500 items (stepsize: 100). For each problem size, correlation varies from 0.0 to 1.0 (stepsize: 0.05). The benchmark, including a total of 15.750 problem instances, is publicly available at ucase.uca.es/nrp.

4.2 SVM training

The training phase was performed using dataset 1, to evaluate three different feature configurations. Results show that the best accuracy results were achieved when using item weight, item profit, and knapsack capacity. Regarding the size of the training set, results show that training with 15% of dataset 1 allows achieving good accuracy metrics. Increasing the number of observations results in marginal accuracy improvements, while significantly increasing training times.

The parameters for the SVM (C) and the RBF kernel (γ) were configured prior to the experimental evaluation. Cross-validation was performed over a set of 5.000 samples randomly selected from dataset 1. Results suggest that the best results are computed with C=8192 and γ=0.5. Average accuracy for all datasets increased from 89.35% to 90.48% after parameter configuration. For the improvement phase, the parameters of the score assignment function in the local search were configured to m=0.2 and k=2 and the stopping criterion was set to 1000 iterations.

4.3 Experimental results

After configuration, the trained SVM was used to evaluate the complete Virtual Savant model on datasets 2 to 5. These datasets are completely new for the algorithm, as they were not used during the training phase. The experimental evaluation focused on both the quality of the solutions and the performance and scalability when using a massively parallel computing infrastructure.

4.3.1 Hardware platform

A many-core computing infrastructure was used in the experimental analysis, in order to evaluate the capabilities of Virtual Savant to compute accurate results over a massively parallel platform. A typical many-core computing infrastructure consists of tens or thousands of simpler independent cores. The use of many-core processors has been increasing in the past years, with extensive applications in embedded systems and high-performance computing platforms [21].

Many-core architectures can be programmed using the standard CPU model without needing specific knowledge about the underlying parallel hardware. Even without including platform-specific features, many-core systems offer support for serial legacy code [22]. The evaluation of Virtual Savant for the 0/1 Knapsack Problem was performed on an Intel Xeon Phi 7250 processor with 68 cores and 64GB RAM.

4.3.2 Scalability

Virtual Savant approach is elastic and adapts to the underlying hardware platform: if more computing resources are available, Virtual Savant can use them on both the prediction and the improvement phase. In the prediction phase, the computational load of predicting whether each

item is included or not in the knapsack is balanced among the computing resources available. In the improvement phase, Virtual Savant takes advantage of available resources to execute more local searches on tentative solutions, thus increasing the probability of computing more accurate results.

The scalability of Virtual Savant when using a varying number of computing elements was evaluated for the prediction and improvement phases. Fig. 3 reports the average execution time (in seconds) for all problem instances studied when varying the number of threads.

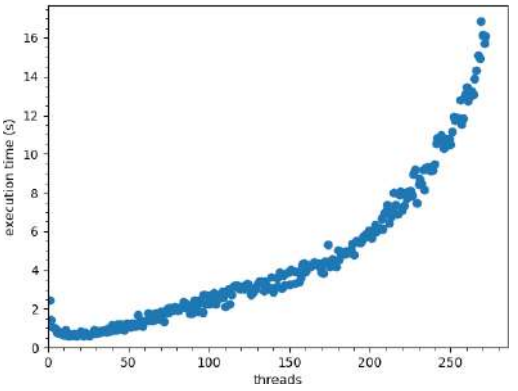


Fig. 3. Execution time varying the number of threads

Results show that Virtual Savant scales very well when increasing the number of threads up to the number of cores available. When more threads are spawned, the performance starts degrading due to threads sharing resources. Consequently, the remainder of the experimental evaluation was performed using 68 threads. These results confirm the good scalability properties of Virtual Savant.

4.3.3 Virtual Savant: prediction phase accuracy

Boxplots in Figs. 4 and 5 correspond to the accuracy achieved during the prediction phase of Virtual Savant grouping problem instances by size and weight/profit correlation, respectively. The median prediction accuracy of the SVM is larger than 90% for all problem sizes studied. No significant differences are noticed among instances of different sizes. On the other hand, significant differences can be observed in the accuracy of the prediction phase on instances with varying weight/profit correlation. Instances with weight/profit correlation of 0.5 are the simplest to predict for the SVM, with a median accuracy value of over 97%. Additionally, in the worst case, the median accuracy of the SVM is larger than 80%.

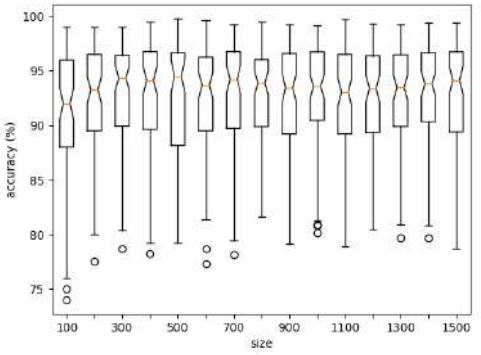


Fig. 4. Prediction accuracy for instances grouped by size.

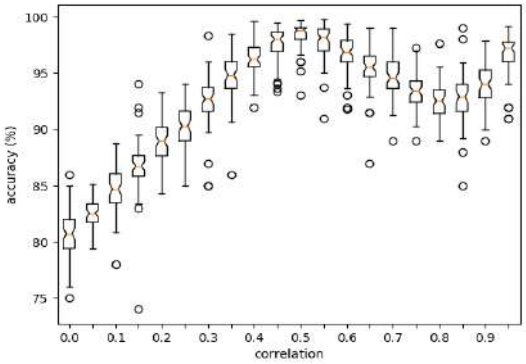


Fig. 5. Prediction accuracy for instances grouped by weight/profit correlation.

4.3.4 Virtual Savant: quality of solutions

Results computed by Virtual Savant were compared with the known optima for the studied instances, to evaluate the efficacy of the proposed approach. Table 1 reports the average ratio to the optima for problem instances grouped by size. Table 2 reports the average ratio to the optimum, grouping instances by the correlation between weight and profit of items.

Results achieved by Virtual Savant grouped by instance size differ from the known optima in just 2-4% on average for all problem instances studied. This is an encouraging result considering that the improvement phase of Virtual Savant consists in a straight-forward local search which does not incorporate any specific knowledge of the problem, thus making it potentially extensible to other related optimization problems. When looking at results grouped by weight/profit correlation, Virtual Savant allows computing accurate results for all problem instances studied. In the worst case, Virtual Savant differs from the optimum in 6% on average (for instances with no correlation between weight and profit).

Table 1. Average ratio to optimum with varying size

size	100	200	300	400	500	600	700	800
ratio	0.98	0.98	0.98	0.97	0.97	0.97	0.97	0.97
size	900	1000	1100	1200	1300	1400	1500	
ratio	0.97	0.97	0.97	0.97	0.97	0.97	0.96	

Table 2. Average ratio to optimum with varying correlation

correlation	0	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45
ratio	0.94	0.95	0.96	0.97	0.97	0.98	0.98	0.99	0.99	0.99
correlation	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95
ratio	0.99	0.98	0.97	0.97	0.96	0.96	0.96	0.96	0.97	0.98

5. Conclusions and future work

This article presents the application of Virtual Savant to the 0/1 Knapsack Problem. Virtual Savant learns from a reference algorithm in order to generate a new program that can solve the same optimization problem in a massively parallel fashion. Experimental results show that Virtual Savant allows computing competitive results in reduced execution times thanks to its scalability when using multiple computing elements. The experimental analysis, performed on a many-core infrastructure, showed the good scalability properties of the Virtual Savant paradigm and its elasticity to adapt to modern massively-parallel computing infrastructures.

The main lines of future work include applying other machine learning classifiers, using different

heuristics and metaheuristics for the improvement phase, and evaluating over larger problem instances.

References

[1]. Luss H. Equitable Resource Allocation. John Wiley & Sons, Inc., 2012.

[2]. Vanderster D. C. Resource Allocation and Scheduling Strategies Using Utility and the Knapsack Problem on Computational Grids. PhD thesis, Victoria, B.C., Canada, 2008.

[3]. Pinel F., Dorronsoro B., Bouvry, and Khan S. Savant: Automatic parallelization of a scheduling heuristic with machine learning. In Proc. of the World Congress on Nature and Biologically Inspired Computing, 2013, pp. 52–57.

[4]. Treffert D. The savant syndrome: an extraordinary condition. A synopsis: past, present, future. Philosophical Transactions of the Royal Society B: Biological Sciences, vol. 364, no. 1522, 2009, pp.1351–1357.

[5]. Treffert D. Extraordinary People: Understanding Savant Syndrome. iUniverse, 2006.

[6]. Bouvet L., Donnadieu S., Valoptdois S., Caron C., Dawson M., and Mottron L. Veridical mapping in savant abilities, absolute pitch, and synesthesia: an autism case study. Frontiers in Psychology, vol. 5, no.106, 2014.

[7]. Pinel F., Dorronsoro B., and Bouvry P. The virtual savant: Automatic generation of parallel solvers. Information Sciences, vol. 432, 2018, pp. 411–430.

[8]. Massobrio R., Dorronsoro B., Palomo-Lozano F., Nesmachnow S., and Pinel F. Generación automática de programas: Savant Virtual para el problema de la mochila. In XI Congreso Español de Metaheurísticas, Algoritmos Evolutivos y Bioinspirados, pages 1–10, 2016.

[9]. Massobrio R., Dorronsoro B., Nesmachnow S., and Palomo-Lozano F. Automatic program generation: Virtual savant for the knapsack problem. In Proc. of the International Workshop on Optimization and Learning, 2018, pp. 1–2

[10]. Kellerer H., Pferschy U., and Pisinger D. Knapsack Problems. Springer, 2004.

[11]. Pinel F. and Dorronsoro B. Savant: Automatic Generation of a Parallel Scheduling Heuristic for Map-Reduce. International Journal of Hybrid Intelligent Systems, vol. 11, no. 4, 2014, pp. 287–302.

[12]. Nemhauser G. L. and Ullmann Z. Discrete dynamic programming and capital allocation. Management Science, vol. 15, no. 9, 1969, pp. 494–505.

[13]. Harman M., Krinke J., Medina-Bulo I., Palomo F., Ren J., and Yoo S.. Exact scalable sensitivity analysis for the next release problem. ACM Transactions on Software Engineering and Methodology, vol. 23, no. 2, 2014, pp. 1–31.

[14]. Bagnall A., Rayward-Smith V., and Whittley I. The next release problem. Information and Software Technology, vol. 43, no. 14, 2001, pp. 883–890.

[15]. Vinyals O., Fortunato M., and Jaitly N. Pointer networks. In Advances in Neural Information Processing Systems 28, pp. 2692–2700, 2015.

[16]. Hu H., Zhang X., Yan X., Wang L., and Xu Y. Solving a new 3d bin packing problem with deep reinforcement learning method. CoRR, abs/1708.05930, 2017.

[17]. Dorronsoro B. and Pinel F. Combining machine learning and genetic algorithms to solve the independent tasks scheduling problem. In Proc. of the 3rd IEEE International Conference on Cybernetics, 2017, pp. 1–8.

[18]. Massobrio R., Dorronsoro B., and Nesmachnow S. Virtual savant for the heterogeneous computing scheduling problem. In Proc. of the International Conference on High Performance Computing & Simulation, 2018 , pp. 1–7.

[19]. Chang C.-C. and Lin C.-J. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, vol. 2, no. 27, 2011, pp. 1–27.

[20]. Massobrio R., Nesmachnow S., and Dorronsoro B. Support Vector Machine Acceleration for Intel Xeon Phi Manycore Processors. In Proc. of the Latin America High Performance Computing Conference, 2017, pp. 1–14.

[21]. Jeffers J., Reinders J., and Sodani A. Intel Xeon Phi Processor High Performance Programming: Knights Landing Edition. Elsevier Science, 2016.

[22]. Rodríguez, S., Parodi, F., and Nesmachnow, S. Parallel evolutionary approaches for game playing and

verification using Intel Xeon Phi. Journal of Parallel and Distributed Computing, 2018. DOI: 10.1016/j.jpdc.2018.07.010

Информация об авторах / Information about authors

Рензо МАССОБРИО является преподавателем и исследователем на инженерном факультете Республиканского университета, Уругвай с 2014 года. Получил степень магистра наук в области компьютерных наук в Республиканском университете. Сфера его научных интересов – вычислительный интеллект, метаэвристика и высокопроизводительные вычисления, применяемые для решения сложных задач оптимизации.

Renzo MASSOBRIO is a teaching and research assistant at the Faculty of Engineering, Universidad de la República, Uruguay since 2014. He holds a degree of M.Sc. in Computer Science both from Universidad de la República. His research interests are computational intelligence, metaheuristics, and high-performance computing applied to solving complex optimization problems.

Бернабе ДОРРОНСОРО ДИАЗ получил степень PhD в университете Малаги, Испания. В настоящее время он является научным сотрудником факультета компьютерных наук и инженерии Кадисского университета. Он удостоен стипендии Рамона-и-Кахала в Кадисском университете, Испания. В число его научных интересов входят автоматическое программирование, многоцелевая оптимизация, машинное обучение, управление ресурсами в центрах данных, облачные вычисления, эволюционные алгоритмы и т.д.

Bernabé DORRONSORO DÍAZ has a Ph.D. degree in Computer Science from University of Málaga. Currently he is a researcher assistant at the Computer Science Engineering Department of the University of Cadiz, Spain. He is the Ramón y Cajal Fellow at University of Cádiz. His research interests include automatic programming, multi- and many-objective optimization, exact approaches, machine learning, resource management for data-centers, cloud computing, sustainable computing, evolutionary algorithms, ets.

Серджо Энрике НЕСМАЧНОВ КАНОВАС обладает степенью PhD в области компьютерных наук, полученной в Республиканском университете, Уругвай. В настоящее время он занимает должность профессора в Вычислительном центре Института компьютерных наук Инженерного факультета Республиканского университета. Основные научные интересы: параллельные и распределенные вычисления, научные вычисления, эволюционные алгоритмы и метаэвристика, а также численные методы.

Sergio Enrique NESMACHNOW CÁNOVAS has a Ph.D. degree in Computer Science from Universidad de la República, Uruguay. He currently holds an Aggregate Professor position in the Numerical Center (CeCal) at Computer Science Institute, Engineering Faculty. His main research interests are parallel and distributed computing, scientific computing, evolutionary algorithms and metaheuristics, and numerical methods.

DOI: 10.15514/ISPRAS-2019-31(2)-3

Гибридная модель для эффективного обнаружения аномалий в кратковременных последовательностях кривых блеска GWAC и аналогичных наборах данных

И. Сан, ORCID: 0000-0003-0545-3175 <sunying1304@126.com>
З. Жао, ORCID: 0000-0002-3638-0290 <xiaoemma6@163.com>
С. Ма, ORCID: 0000-0001-6622-6318 <matnt2008@126.com>
Чж. Ду, ORCID: 0000-0002-8435-1611 <duzh@tsinghua.edu.cn>
Факультет компьютерных наук и технологий, Университет Цинхуа, Китай

Аннотация. Раннее оповещение во время обзора неба дает важную возможность обнаруживать одиночные планеты с малой массой. В статье представлен гибридный метод, в котором комбинируется модель ARIMA (интегрированная модель авторегрессии – скользящего среднего), рекуррентные нейронные сети (RNN) LSTM (нейронная сеть с блоками долго-кратковременной памяти) и GRU (управляемый рекуррентный нейрон), обеспечивающий возможность поиска кратковременных событий микролинзирования (ML) в режиме реального времени на основе данных, получаемых путем высокочастотной широкоугольной съемки звездного неба. Метод обеспечивает мониторинг всех наблюдаемых кривых блеска и выявление событий ML на ранних стадиях. Экспериментальные результаты показывают, что гибридные модели обеспечивают бо́льшую точность и требуют меньше времени на настройку параметров. ARIMA + LSTM и ARIMA + GRU могут повысить точность на 14,5% и 13,2% соответственно. При обнаружении аномалий в кривых блеск, GRU может достичь почти того же результата, что и LSTM, затрачивая на 8% меньшее время. Те же модели применимы и к набору данных ЭКГ в базах данных MIT-BIH по аритмии с похожим паттерном аномалий, и в обоих случаях мы можем сократить на 40% временя, которое требуется исследователям для настройки модели, с сохранением 90% точности.

Ключевые слова: гравитационное линзирование; рекурентные нейронные сети; ARIMA; предупреждения и прогнозы на основе временных рядов

Для цитирования. Сан И., Жао З., Ма С., Ду Чж. Гибридная модель для эффективного обнаружения аномалий в кратковременных последовательностях кривых блеска GWAC и аналогичных наборах данных. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 33-40. DOI: 10.15514/ISPRAS-2019-31(2)-3

Благодарности. Исследование частично поддерживалось Программой базовых исследований и разработок КНР (грант No.2016YFB1000602), Базовой лабораторией космической астрономии и технологии Национальной астрономической обсерватории Китайской академии наук, Национальным фондом естественных наук КНР (гранты 61440057, 61272087, 61363019, 61073008, 11690023) и Фондом исследовательского центра МОЕ в области дистанционного образования (грант No. 2016ZD302)

Hybrid Model for Efficient Anomaly Detection in Short-timescale GWAC Light Curves and Similar Datasets

Y. Sun, ORCID: 0000-0003-0545-3175 <sunying1304@126.com>
Z. Zhao, ORCID: 0000-0002-3638-0290 <xiaoemma6@163.com>
X. Ma, ORCID: 0000-0001-6622-6318 <matnt2008@126.com>
Z. Du, ORCID: 0000-0002-8435-1611 <duzh@tsinghua.edu.cn>
Department of Computer Science and Technology, Tsinghua University

Abstract. Early warning during sky survey provides a crucial opportunity to detect low-mass, free-floating planets. In particular, to search short-timescale microlensing (ML) events from high-cadence and wide- field survey in real time, a hybrid method which combines ARIMA (Autoregressive Integrated Moving Average) with LSTM (Long-Short Time Memory) and GRU (Gated Recurrent Unit) recurrent neural networks (RNN) is presented to monitor all observed light curves and identify ML events at their early stages. Experimental results show that the hybrid models perform better in accuracy and less time consuming of adjusting parameters. ARIMA+LSTM and ARIMA+GRU can achieve improvement in accuracy by 14.5% and 13.2%, respectively. In the case of abnormal detection of light curves, GRU can achieve almost the same result as LSTM with less time by 8%. Same models are also applied to MIT-BIH Arrhythmia Databases ECG dataset with similar abnormal pattern and we yield from both sets that we can reduce up to 40% of time consuming for researchers to adjust the model to 90% accuracy.

Keywords: gravitational lensing; recurrent neural networks; ARIMA; time series prediction and alarming

For citation: Sun Y., Zhao Z., Ma X., Du Z. Hybrid Model for Efficient Anomaly Detection in Short-timescale GWAC Light Curves and Similar Datasets. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 33-40 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-3

Acknowledgements. This research is supported in part by Key Research and Development Program of China (No.2016YFB1000602), the Key Laboratory of Space Astronomy and Technology, National Astronomical Observatories, Chinese Academy of Sciences, Beijing, 100012, China, National Natural Science Foundation of China (Nos. 61440057,61272087,61363019 and 61073008,11690023), MOE research center for online education foundation (No 2016ZD302).

1. Введение

Астрономия является отправной точкой взрыва информации, и это первая область, которая встретилась с проблемой больших данных [1]. В этой статье мы используем данные мини-GWAC (Ground-based Wide Angle Camera, наземная широкоугольная камера) в качестве образцов для обучения и тестирования. Мы исследуем проблему поиска в реальном времени гравитационных ML-событий кратковременного масштаба в огромном наборе кривых блеска, применяя гибридные модели ARIMA-LSTM и ARIMA-GRU. Мы также пытаемся выработать подход, который мог бы применяться в области финансов и других областях, подобно исследованиям, выполняемым в Корнелле [2]. Эксперименты для оценки производительности этих двух моделей выполнялись на наборе данных мини-GWAC.

Мы также применяем свои модели к базе данных аритмии MIT-BIH, характеристики которой схожи с набором данных GWAC: аномальные ситуации похожи одна на другую, а нормальные ситуации ведут себя беспорядочно. База данных аритмии MIT-BIH [5] содержит 48 получасовых выдержек из двухканальных амбулаторных записей ЭКГ, полученных от 47 субъектов, которые обследовались в лаборатории аритмии BIH между 1975 и 1979 годами.

2. Гибридные модели ARIMA-LSTM и ARIMA-GRU

Данные детектирования света, полученные с помощью мини-GWAC, содержат более 900 файлов временных рядов для каждой планеты. Очевидно, что стоит предположить наличие

у этих данных линейной, так и нелинейной частей [3]. Таким образом, мы можем представить данные следующим образом:

$$x_t = L_t + N_t + \varepsilon_t$$

Здесь L_t представляет линейность данных в момент времени t, а N_t обозначает нелинейность. Значение ε_t представляет погрешность. В предыдущей работе [4] на линейных задачах отличные результаты показала интегрированная модель авторегрессии – скользящего среднего (Autoregressive Integrated Moving Average, ARIMA), обеспечивая в целом точность более 85%. Это традиционный метод прогнозирования временных рядов. С другой стороны, модель долго-кратковременной памяти (LSTM) может обнаруживать в наборе данных нелинейные тренды. Наша гибридная модель ARIMA-LSTM позволяет обнаруживать как линейные, так и нелинейные тренды.

3. Методика проведения экспериментов

3.1 Наборы данных и среда проведения экспериментов

Наборы данных GWAC и mini GWAC: Данные GWAC до недавнего времени не были открыты, поэтому наши алгоритмы тестируются на наборе данных mini-GWAC. Система Mini-GWAC состоит из 12 комплектов широкоугольных камер. Она была построена и размещена в обсерватории Синлун Национальной астрономической обсерватории. В этой статье мы используем данные мини-GWAC в качестве примеров для обучения и тестирования. Для каждой планеты набор данных мини-GWAC содержит в среднем 980 текстовых файлов. В каждом файле мы можем получить 900 данных, составляющих часть временных рядов.

База данных аритмии MIT-BIH– набор данных ЭКГ: Мы обнаружили в наборе данных ЭКГ характеристики, схожие с набором данных GWAC: аномальные ситуации похожи одна на другую, а нормальные ситуации ведут себя беспорядочно. База данных аритмии MIT-BIH [5] содержит 48 получасовых выдержек из двухканальных амбулаторных записей ЭКГ, полученных от 47 субъектов, которые обследовались в лаборатории аритмии BIH между 1975 и 1979 годами.

3.2 Алгоритм

Алгоритм 1 представляет собой краткое описание нашего метода. На первом этапе для прогнозирования приблизительных результатов используется ARIMA. Размер окна составляет 20% от длины массива. Для каждого окна производится результат. После получения результата окно перемещается на шаг вперед, чтобы предсказать следующее значение. Однако между реальностью и предсказанием имеются некоторые остатки. Поэтому для более точного прогнозирования остатки рассчитываются и используются в качестве входных данных на втором этапе, где они являются обучающими наборами в RNN. Таким образом, на втором шаге обучающие наборы используются для прогнозирования нелинейной части. Наконец, на последнем этапе окончательные прогнозы представляют собой сумму значений, предсказанных ARIMA, и остатков. Такие прогнозы более точны, чем прогнозы, сделанные только с помощью ARIMA.

```
1.   Result = []
2.   Resid = emptylist
3.   for dataset in datasets do
4.     Predict = []
5.     Models = emptylist
6.     Order = arima.aicminorder
7.     if unstable: then
8.        Model = diff(model)
```

```
    end if
    Model = fitarima(dataset, order)
    Add residual[0] to Resid
    Add predict[0] to Predict
    Add predict to Result
  end for
  Save Result[-1], Resid
```

Алгоритм 1. Гибридная модель ARIMA-LSTM/ARIMA-GRU
Algorithm 1. ARIMA-LSTM/ARIMA-GRU Hybrid Model

4. Результаты экспериментов и их оценка

4.1 Результаты тестирования на наборе данных mini-GWAC

В этом подразделе мы выявляем три аспекта эффективности модели: точность, затрачиваемое время и сложность вычислений. Точность определяется тем, насколько рано выдаются оповещения и насколько часто появляются ложные предсказания. Другими словами, модель должна быть одновременно точной при прогнозировании и чувствительной к аномальным случаям. На рис. 1 точка оповещения помечена вертикальной красной линией. Чем меньше время оповещения, тем лучше работает модель. Ложное предсказание – это расхождение предсказанного и реального значений.

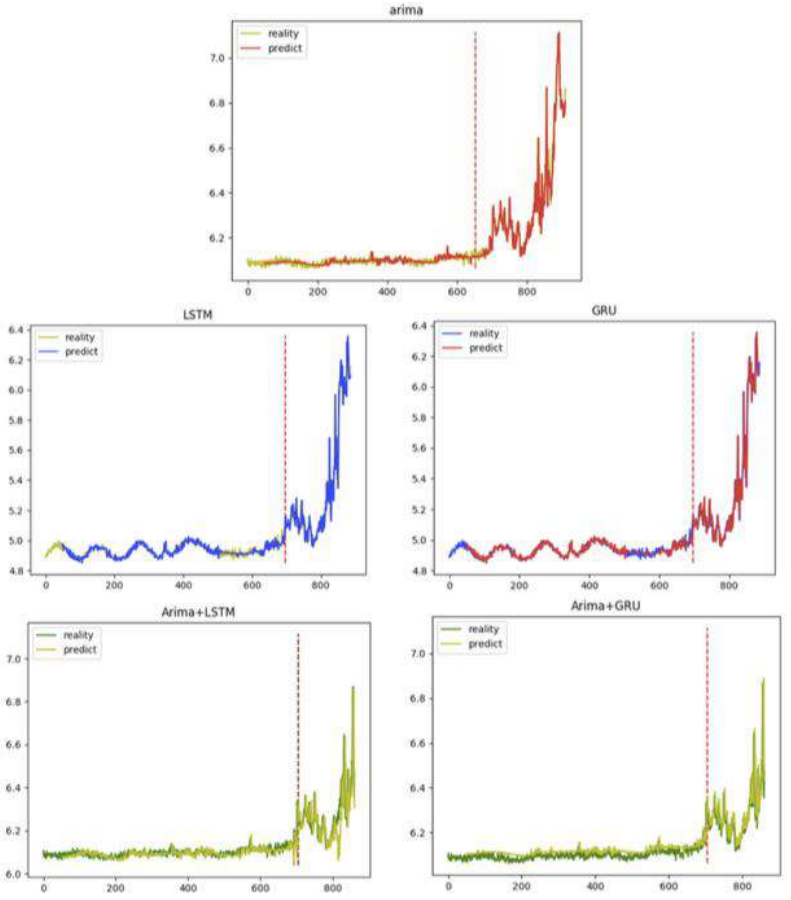


Рис. 1. Тестирование разных алгоритмов на наборе данных mini-GWAC
Fig. 1. Testing different algorithms on mini-GWAC dataset

Результаты для набора данных мини-GWAC приведены в табл. 1.

a) При кратковременном прогнозирования событий гравитационного микролинзирования с использованием набора данных мини-GWAC GRU обучается быстрее, чем LSTM.

b) Своевременность оповещения у проверенных методов различается мало. Точность немного лучше у гибридных моделей. LSTM ведет себя более надежно, чем GRU.

c) Методы GRU проще и, следовательно, их легче модифицировать, добавляя, например, вентили при потребности ввода в сеть дополнительных данных. Это приводит к сокращению времени обучения и сложности вычислений.

d) ARIMA может достигать меньшего времени оповещения и времени работы, но имеется высокая частота ложных предсказаний. За счет сокращения времени работы на 15% гибридные модели ARIMA и LSTM или GRU могут улучшить точность на 14,5% и 13,2% соответственно.

Табл. 1. Результаты оценки разных алгоритмов на наборе данных mini-GWAC
Table 1. Evaluation results of different algorithms on the mini-GWAC dataset

Алгоритмы	**Точность / время оповещения**	**Время выполнения**
ARIMA	81.60% / 41.7%	0.349 сек.
LSTM	93.72% / 42.6%	0.478 сек.
GRU	93.28% / 43.3%	0.440 сек.
ARIMA-LSTM	96.11% / 42.2%	0.406 сек.
ARIMA-GRU	94.83% / 42.8%	9.413 сек.

4.2 Результаты тестирования на базе данных аритмии MIT-BIH

Результаты всех моделей показаны на рис. 2, и хотя результаты не так убедительны, как в предыдущем подразделе, они позволяют прийти к некоторым выводам.

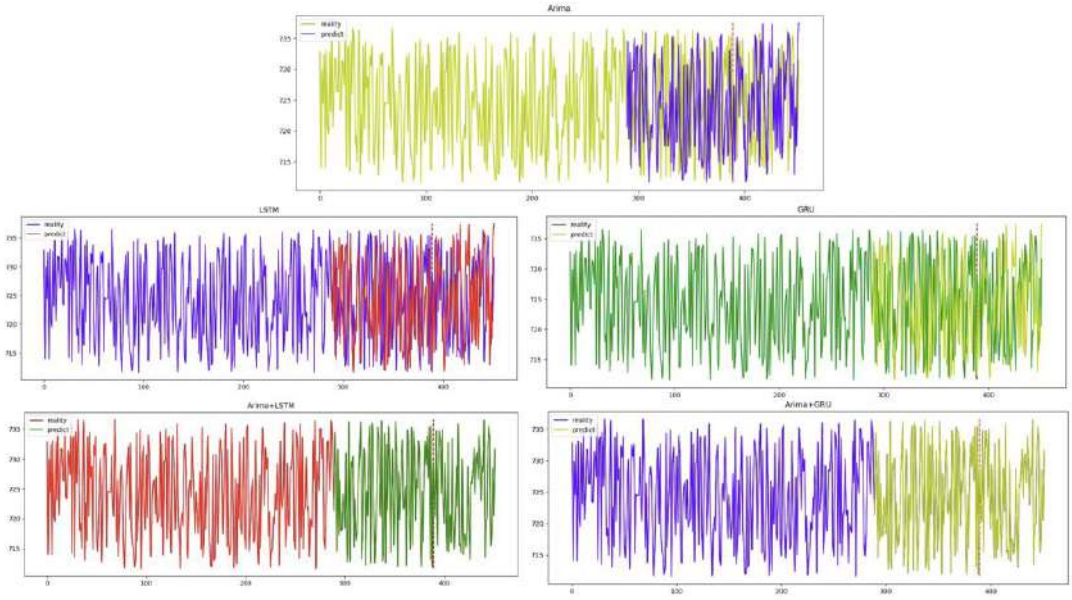


Рис. 1. Тестирование разных алгоритмов на наборе данных ECG
Fig. 2. Test on ECG dataset of different algorithms

a) Для набора данных ECG ARIMA-LSTM работает лучше, чем ARIMA-GRU, обеспечивая большую точности, и меньшее время выполнения.
b) Из-за параметров RNN точность LSTM и GRU составляет всего около 50%, но в сочетании с ARIMA они могут обеспечить точность свыше 90%.
c) Время выполнения намного больше, чем для наборов данных GWAC.

Табл. 1. Результаты оценки разных алгоритмов на наборе данных ECG
Table 1. Evaluation results of different algorithms on the ECG dataset

Алгоритмы	Точность / время оповещения	Время выполнения
ARIMA	91.47% / 37.9%	4.12 сек.
LSTM	52.22% / 30.8%	7.61 сек.
GRU	50.30% / 30.8%	7.78 сек.
ARIMA-LSTM	93.26% / 37.9%	9.82 сек.
ARIMA-GRU	93.01% / 37.9%	9.85 сек.

6. Заключение

Результаты тестирования на описанных наборах данных демонстрируют, что наш метод способствует не только повышению эффективности, но и уменьшению затрат времени исследователями. При все более широком использовании нейронных сетей настройка параметров является наиболее сложной и трудоемкой частью процесса. Поскольку наша модель в основном полагается на ARIMA, сокращение требований RNN позволяет экономить до 40-80% времени при решении той же проблеме. Это может помочь сэкономить время на настройку машинного обучения.

В целом, мы полагаем, что наша работа способствует формированию важного подхода в компьютерном прогнозировании временных рядов. Дальнейшая работа будет направлена на усиление модели и повышение ее производительности с экспериментальным тестированием на наборе данных GWAC, сокращению времени работы, особенно в процессе обучения нейронной сети.

Список литературы / References

[1]. V. Mayer-Schnberger, K. Cukier. Big data: A revolution that will transform how we live, work and think. Houghton Mifflin Harcourt, 2013, 256 p.
[2]. Sima Siami-Namini, Akbar Siami Namin, Forecasting Economics and Financial Time Series: ARIMA vs. LSTM, arXiv:1803.06386, 2018, 19 p.
[3]. G. Jenkins G.E.P. Box. Time series analysis, forecasting and control. Holden-Day, San Francisco, CA, 1970.
[4]. G.P. Zhang. Time series forecasting using a hybrid arima and neural network model. Neurocomputing, vol. 50, 2003, pp. 159-175.
[5] MIT-BIH Arrythmia Database: https://physionet.org/physiobank/database/mitdb/

Информация об авторах / Information about authors

Инь САН работает в Национальной лаборатории информатики и технологии, факультет компьютерных наук и технологий, Университет Цинхуа, Китай.

Ying SUN is working at Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, China.

Зиджун ЖАО работает в Национальной лаборатории информатики и технологии, факультет компьютерных наук и технологий, Университет Цинхуа, Китай.

Zijun ZHAO is working at Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, China.

Сяобин МА работает в Национальной лаборатории информатики и технологии, факультет компьютерных наук и технологий, Университет Цинхуа, Китай.

Xiaobin MA is working at Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, China.

Чжихуэй ДУ получил степень PhD в области компьютерных наук и технологий в Пекинском университете, КНР в 1998 г. В настоящее время он работает доцентом на факультете компьютерных наук и технологий университета Цинхуа, КНР. В число научных интересов входят параллельное программирование, высокопроизводительные, облачные, энергосберегающие вычисления и анализ больших данных.

Zhihui DU received the degree of PhD in Computer Science & Technology from Peking University, China in 1998. Currently he is the associate professor at the Department of Computer Science and Technology of Tsinghua University, China. His research interests include parallel computing, high performance/cloud/energy efficient computing, and Big Data analysis.

DOI: 10.15514/ISPRAS-2019-31(2)-4

Теоретический подход к поиску глобального экстремума при обучении нейронных сетей

[1] *Н.А. Вершков, ORCID: 0000-0001-5756-7612 <vernick61@yandex.ru>*
[2] *В.А. Кучуков, ORCID: 0000-0002-1839-2765 <vkuchukov@ncfu.ru>*
[2] *Н.Н. Кучукова, ORCID: 0000-0002-8070-0829 <nkuchukova@ncfu.ru>*
[1] *Ставропольский краевой институт развития образования, повышения квалификации и переподготовки работников образования,*
355002, г. Ставрополь, ул. Лермонтова, д. 189А
[2] *Северо-Кавказский федеральный университет,*
355009, Россия, г. Ставрополь, ул. Пушкина, 1

Аннотация. В статье рассматривается вопрос поиска глобального экстремума при обучении искусственных нейронных сетей с помощью корреляционного показателя. Предложенный метод базируется на математической модели искусственной нейронной сети, представленной в виде системы передачи информации. Эффективность предлагаемой модели подтверждается широким применением ее в системах передачи информации для анализа и восстановления полезного сигнала на фоне различных помех: гауссовых, сосредоточенных, импульсных и т.п. Проводится анализ сходимости обучающей и полученной экспериментально последовательностей на основе корреляционного показателя. Подтверждается возможность оценки сходимости обучающей и экспериментально полученной последовательностей на основе взаимно-корреляционной функции как мере их энергетической схожести (различия). Для оценки предложенного метода проводится сравнительный анализ с используемыми в настоящее время целевыми показателями. Исследуются возможные источники ошибок метода наименьших квадратов и возможности предлагаемого показателя по их преодолению.

Ключевые слова: искусственные нейронные сети; корреляционная функция; спектральный анализ

Для цитирования: Вершков Н.А., Кучуков В.А., Кучукова Н.Н. Теоретический подход к поиску глобального экстремума при обучении нейронных сетей. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 41-52. DOI: 10.15514/ISPRAS-2019-31(2)-4

Благодарность. Работа выполнена при поддержке стипендии Президента РФ молодым ученым и аспирантам СП-2236.2018.

The Theoretical Approach to the Search for a Global Extremum in the Training of Neural Networks

[1] *N.A. Vershkov, ORCID: 0000-0001-5756-7612 <vernick61@yandex.ru>*
[2] *V.A. Kuchukov, ORCID: 0000-0002-1839-2765 <vkuchukov@ncfu.ru>*
[2] *N.N. Kuchukova, ORCID: 0000-0002-8070-0829 <nkuchukova@ncfu.ru>*
[1] *Stavropol Regional Institute for the Development of Education, Training and Retraining of Educators, 189 A, Lermontov st., Stavropol, 355002, Russia*
[2] *North-Caucasus Federal University, 1, Pushkin st., Stavropol, 355009, Russia*

Abstract. The article deals with the search for the global extremum in the training of artificial neural networks using the correlation index. The proposed method is based on a mathematical model of an artificial neural network, represented as an information transmission system. The efficiency of the proposed model is

confirmed by its broad application in information transmission systems for analyzing and recovering the useful signal against the background of various interferences: Gaussian, concentrated, pulsed, etc. The analysis of the convergence of training and experimentally obtained sequences based on the correlation index is carried out. The possibility of estimating the convergence of the training and experimentally obtained sequences by the cross-correlation function as a measure of their energy similarity (difference) is confirmed. To evaluate the proposed method, a comparative analysis is carried out with the currently used target indicators. Possible sources of errors of the least squares method and the possibility of the proposed index to overcome them are investigated.

Keywords: artificial neural network; correlation function; spectral analysis

For citation: Vershkov N.N., Kuchukov V.A., Kuchukova N.N. The theoretical approach to the search for a global extremum in the training of neural networks. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 41-52 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-4

Acknowledgement. This work was supported by the scholarship of the President of the Russian Federation to young scientists and graduate students SP-2236.2018.

1. Введение

Человеческая деятельность в современном мире связана с накоплением и обработкой больших объемов информации. Одним из механизмов для анализа накопленной информации и построения моделей анализа данных являются искусственные нейронные сети (ИНС). Теоретической основой ИНС является теорема Колмогорова–Арнольда [1, 2], важнейшим следствием которой является возможность представления функции нескольких переменных в виде суперпозиции функций меньшего числа переменных, т.е. $f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{2n+1} h_i(\sum_{k=1}^{n} \varphi_{ki}(x_k))$, где h_i, φ_{ki} – непрерывные функции, причем φ_{ki} не зависят от *f*. Дальнейшие теоретические разработки имели прикладное значение: примером может служить теорема Хехт–Нильсена [3]. Теорема Хехт-Нильсена доказывает возможность представления функции многих переменных достаточно общего вида с помощью двухслойной нейронной сети с прямыми полными связями с *N* компонентами входного сигнала, *2N+1* компонентами первого слоя с заранее известными ограниченными функциями активации и *N* компонентами второго слоя с неизвестными функциями активации. Кроме того, известна классическая теорема Вейерштрасса [4] о возможности приближения функции *n* переменных с любой точностью с помощью полинома. Такой подход интересен, когда существует линейная разделимость классов. Более общая теорема Стоуна [4] утверждает возможность приближения многочленом любого конечного набора функций. Таким образом, с помощью ИНС возможна реализация практически любой, сколь угодно сложной функции любого количества переменных.

Большинство современных обучающих алгоритмов основано на принципе обучения Хебба [5]. В настоящее время алгоритмы обучения ИНС представлены значительным многообразием и различаются по видам решаемых задач. Однако их основным математическим аппаратом является векторная алгебра и метод градиентного спуска, опирающийся на дифференциальный анализ слоев ИНС первого и второго порядка. Сейчас, в т.ч. благодаря достижениям команды Хинтона [6], уделяется большое внимание «глубокому обучению» (Deep Learning). Интерес к «глубоким нейронным сетям» связан с ограничениями, которыми обладает персептрон [7]. Использование многослойных сетей изначально было ограничено вычислительными сложностями их обучения. Благодаря идеям команды Хинтона стало возможным обучение многослойных ИНС [8]. Основными достижениями стало применение автоэнкодеров и автоассоциаторов. Автоэнкодеры и автоассоциаторы применялись для поиска скрытых взаимосвязей и корреляций признаков во входной информации. Автоэнкодер, изменяя f и g, стремится выучить тождественную функцию $x = f(g(x))$, минимизируя функционал ошибки $L\left(x, f\left(g(x)\right)\right)$. При этом семейства функций энкодера g и декодера f ограничены, чтобы автоэнкодер был вынужден

отбирать наиболее важные свойства сигнала. Таким образом, современное развитие методов обучения ИНС является в большей степени эмпирическим, чем математическим. Несмотря на достигнутые успехи и сокращение времени обучения в десятки, а иногда и в сотни раз, в данном направлении остается ряд задач, требующих теоретического осмысления. К ним, в первую очередь, относится задача поиска глобального экстремума целевой функции и конечность алгоритма обучения [9]. Проблема в том, что многослойная ИНС имеет очень сложную передаточную характеристику с множеством локальных минимумов и максимумов. Поиск глобального минимума является вычислительно сложной задачей и требует совершенствования современных алгоритмов обучения.

В этой работе мы проанализировали возможность использования методов, широко используемых в теории передачи информации для распознавания сигнала на фоне шума и сосредоточенных помех, для поиска экстремума целевой функции при обучении ИНС с учителем. Нами была предложена и проанализирована математическая модель ИНС как системы передачи информации, а также предложена целевая функция для оценки качества обучения в виде показателя взаимно-корреляционной функции экспериментально полученной и обучающей последовательностей. Предложенный подход позволит уменьшить вычислительную сложность алгоритма поиска глобального экстремума за счет модификации алгоритма обучения.

Статья организована следующим образом. В разд. 2 исследуются информационные процессы, происходящие в ИНС и предлагается математическая модель нейронной сети как системы передачи информации. Разд. 3 посвящен исследованию сходимости обучающей и экспериментально полученной последовательности и определению целевой функции как двумерной взаимно-корреляционной функции. В разд. 4 проводится сравнительный анализ предложенного метода с существующими для получения оценки эффективности обучения. В Заключении определяются основные направления исследования нейронных сетей как системы передачи информации.

2. Модель нейронной сети как системы передачи информации

Для анализа каналов связи широко применяется теория передачи информации и управления в условиях помех – гауссовых, сосредоточенных, импульсных [10]. При ближайшем рассмотрении многие ее положения могут быть использованы для анализа и процесса обучения ИНС. Обучающая последовательность ИНС рассматривается в виде набора пар векторов $\{X_i, Y_i\}, i = 0,1, \dots, n$. При этом на каждое входное воздействие X_i ИНС дает отклик Y_i^k, где каждому значению k соответствует набор значений W_k, которые являются весами сети. Основной задачей (целью обучения) является подбор такого набора $\{W_k\}$, при котором на каждое воздействие X_i получаемый отклик Y_i^k отличается от Y_i на приемлемую величину δ. В математическом виде это будет выглядеть как $W_k \left(\delta \underset{min}{\longrightarrow} \{Y_i^k, Y_i\}\right), \forall\, i = 0,1, \dots, n.$

2.1 Информационная модель ИНС

Для перехода к информационной модели введем ряд условий. Набор входных векторов может быть представлен в виде последовательности значений $X_1, X_2, \dots, X_n$, изменяющихся во времени. Будем считать, что отсчеты X_i следуют через равные промежутки времени Δt или, иначе говоря, $X_i(t)$ являются дискретными отсчетами функции $x(t)$. Тогда можно говорить о конечной во времени функции $x(t)$, подаваемой на вход ИНС, определенной на интервале $t \in [t_0, t_n]$. Поскольку каждому входному значению обучающей выборки X_i соответствует выходное значение (отклик), то можно говорить о выходной последовательности Y_i, следующей через промежутки времени Δt на интервале $t \in [t_0, t_n]$. Таким образом, последовательность Y_i является дискретизацией выходной функции $y(t)$. Кроме того, процесс обучения ИНС представляет собой периодический повтор входных

отсчетов $\{X_i\}$ для каждого набора весов $\{W_k\}$ с целью получения выходной последовательности $\{Y_i^k\}$. Если градиент изменения весов $\{W_k\}$ невелик, то выходную функцию $y_k(t)$ можно считать периодической, а изменения, возникающие под воздействием изменения $\{W_k\}$, можно считать помехой $\mu(t)$ (шумом). При этом шум не обязательно является «белым», т.е. подчиняется гауссовому закону. Чтобы не вводить дополнительных ограничений, функции $x(t)$, $y(t)$ и $y_k(t)$ будем считать сложными широкополосными сигналами. Таким образом, обобщенная модель ИНС может быть представлена как $y_k(t) = f_1(f_2(\dots f_m(x(t), W_k^m), \dots W_k^2), W_k^1)$, где f_i – передаточная функция i-того слоя ИНС, W_k^i – k-тый набор весов i-того слоя, создающий возмущение (помеху, шум) $\mu_i(t)$ в i-том слое вследствие неточного подбора весов. Понятно, что анализ модели ИНС в таком виде затруднен сложностью аналитического представления объекта исследования.

2.2 Анализ предлагаемой модели ИНС

Для анализа работы системы передачи информации воспользуемся представлением функции $x(t)$ в обобщенной спектральной форме [11]:

$$x_r(t) = \sum_{k=k_{r1}}^{k_{rn}} a_{kr}\varphi_k(t)\,, t \in [t_1, t_n], \tag{2.1}$$

где координатные функции $\varphi_k(t)$ удовлетворяют условию ортогональности

$$\frac{1}{T}\int_0^T \varphi_k(t)\varphi_j(t)dt = \begin{cases} 0, \text{при } k \neq j \\ \frac{1}{T}\int_0^T \varphi_k^2(t)dt, \text{при } k = j \end{cases},$$

а коэффициенты разложения

$$a_{kr} = \frac{1}{\int_0^T \varphi_k^2(t)dt}\int_0^T x_r(t)\varphi_k(t)dt.$$

Из (2.1) следует, что количество элементарных функций (составляющих) $a_{kr}\varphi_k(t)$ равно $N_r = k_{rn} - k_{r1} + 1$. Для формирования сложных сигналов обычно используют совокупность координатных функций как некоторое подмножество полной ортогональной системы функций: тригонометрических, Лаггера, Лежандра, Эрмита, Уолша, Чебышева и т.п. [11]. Представление (2.1) позволяет более наглядно представить формирование и обработку сложных функций в частотно-временной области. Подобный подход может быть применен к ИНС, особенно в тех случаях, когда функция активации нейрона линейна. Такой подход используется для анализа линейных адаптивных систем [12]. Для нелинейной функции подобный подход вычислительно сложнее, т.к. выходной сигнал не всегда может быть представлен в виде суперпозиции составляющих без искажения.

Для отображения исходной функции времени $x(t)$ и отклика $y(t)$ в спектральной области используют преобразование Фурье [13]:

$$x(t) = a_0^x + \sum_{n=1}^{\infty} a_n^x \cos n\omega_0 t + \sum_{n=1}^{\infty} b_n^x \sin n\omega_0 t$$

$$y(t) = a_0^y + \sum_{n=1}^{\infty} a_n^y \cos n\omega_0 t + \sum_{n=1}^{\infty} b_n^y \sin n\omega_0 t$$

Т.е. любую периодическую функцию можно представить в виде бесконечной суммы колебаний, кратных основной частоте ω_0. Поскольку обучающая последовательность представляет собой набор дискретных значений, то, используя формулу Эйлера для тригонометрических функций, можно перейти к дискретному преобразованию Фурье (ДПФ):

$$x(t) = a_0^x + \frac{1}{2}\sum_{n=1}^{\infty}(a_n^x(e^{in\omega_0 t} + e^{-in\omega_0 t}) - ib_n^x(e^{in\omega_0 t} - e^{-in\omega_0 t}))$$

$$y(t) = a_0^y + \frac{1}{2}\sum_{n=1}^{\infty}(a_n^y(e^{in\omega_0 t} + e^{-in\omega_0 t}) - ib_n^y(e^{in\omega_0 t} - e^{-in\omega_0 t}))$$

Таким образом, задача обучения ИНС сводится к сравнению функций (сигналов) $y(t)$ и $y_k(t)$ и поиску такого набора $\{W_k\}$, чтобы отличия $y(t)$ и $y_k(t)$ были минимальны, т.е. $\delta = \min(y(t), y_k(t, W_k))$. Поскольку ИНС (в общем виде) является нелинейной системой, то применение спектрального анализа в классическом виде затруднено. Но для сравнения сложных широкополосных сигналов в теории передачи информации широко применяется метод сравнения энергий. Для определения меры схожести сложных широкополосных сигналов во временной области используют взаимно-корреляционную функцию (ВКФ) $B_{yy}(\tau) = \int_{-\infty}^{\infty} y(t)y_k(t-\tau)$, $\tau = [t_0, t_n]$. Мерой подобия эталонного $y(t)$ и выходного $y_k(t)$ сигналов является энергия разностного сигнала $\varepsilon = \int_{-\infty}^{\infty} y(t)y_k^*(t)dt$, где * – знак сопряжения по Гильберту. Согласно свойству преобразования Фурье [14], свертке функций $y(t)$ и $y_k(t)$ во временной области соответствует произведение Фурье-образов $B_{yy}(f) = \tilde{Y}(f)\tilde{Y}_k(f)$. В свою очередь, выходной сигнал можно представить (исходя из структуры нейрона) как $y_k(t) = f_i(\sum_{r=1}^{n} x_r(t)w_i^k)$. Желаемый отклик $y(t)$ определен заранее (до начала обучения), поэтому его спектр может быть также заранее рассчитан. Поэтому используя дискретное преобразование Фурье для вычисления корреляционной функции B_{yy}, можно получить выражение для поиска весов *n*-го слоя.

3. Математическая модель оценки сходимости отклика ИНС с обучающей последовательностью

Основным подходом для оценки сходимости фактического и желаемого отклика за все время изучения ИНС является широко применяемый в математической статистике метод наименьших квадратов (МНК) [15], для которого целевой функцией является суммарная квадратичная ошибка

$$E_\Sigma = \sum_n E(n), E(n) = \frac{1}{2}\sum_i e_i^2(n)$$

Здесь $E(n)$ – сумма квадратов ошибок $e_i(n)$ всех нейронов выходного слоя, т.е. $e_i(n) = Y_i - Y_i^k$. При этом математическая форма алгоритма обучения представлена как

$$\frac{\partial E_\Sigma}{\partial w_k} = \sum_n \frac{\partial E(n)}{\partial w_k}$$

которая именуется методом градиентного спуска. Выбирая соответствующим образом величину Δ как величину градиента и опираясь на минимум суммы квадратов ошибок, подбирают вектор изменения значений $\{W_k\}$. Этот метод используется в обучении ИНС, поскольку обладает рядом преимуществ. Во-первых, т.к. квадратичная функция имеет один ярко выраженный минимум, благодаря чему алгоритм поиска решения всегда конечен. Во-вторых, МНК является основой алгоритма наискорейшего спуска, применяемого в современных алгоритмах обучения.

3.1 Взаимно-корреляционная функция как мера сходства и различия

Рассмотрим ИНС как систему передачи информации с характеристикой, которую вычислительно сложно найти расчетными методами. При этом постановка задачи моделирования будет выглядеть следующим образом. На вход системы подается

последовательность входных воздействий $X_i(t)$, являющихся дискретными отсчетами обучающей функции $x(t)$. При изменении значений $\{W_k\}$ передаточная характеристика системы изменяется, меняя, в свою очередь, выходные отклики Y_i^k, являющимися дискретными отсчетами функции отклика $y_k(t)$. В распоряжении имеется набор значений Y_i, являющихся дискретными отсчетами целевой (обучающей) функции $y(t)$. Требуется подобрать такой набор значений весов $\{W_k\}$, при котором функция отклика $y_k(t)$ минимально отличается от целевой функции $y(t)$. Такая постановка задачи имеет ряд отличительных признаков от МНК, т.к. речь идет не о сумме квадратов отклонений значений векторов отклика от эталонного, а об отличии периодических функций $y_k(t)$ от $y(t)$ на отрезке времени $T = k(t_n - t_0)$, в течение которого $y(t)$ и $y_k(t)$ пробегают весь набор значений, определенных для обучения. Иными словами, речь идет об энергии разностного сигнала $\varepsilon(t)$, который рассматривался в разделе 2.2. Поскольку сравнение сигналов не может происходить на бесконечном отрезке частот, необходимо выбрать некоторую частоту среза ω_c, выше которой сравнение производится не будет. Тогда полная энергия ошибки за пределами частоты среза может быть определена как $E_\varepsilon = \int_0^T \varepsilon_y^2(t)dt = P_\varepsilon T$, где $\varepsilon_y(t)$ – ошибки обучающего и экспериментального сигналов, P_ε – средняя мощность ошибок сигналов. Полная энергия сигналов может быть определена как $E_y(t) = \int_0^T y(t)y_k(t)dt = P_y T$ на основании теоремы Рэйли:

$$\begin{cases} E_\varepsilon = \dfrac{1}{\pi}\displaystyle\int_{\omega_c}^{\infty} A_y^2(\omega)d\omega\,, \\ E_y = \dfrac{1}{\pi}\displaystyle\int_{0}^{\omega_c} A_y^2(\omega)d\omega \end{cases}$$

где $A(\omega) = |X(j\omega)|$ – амплитудный спектр сигнала. Используя соотношение из работы [17]:

$$\gamma = \frac{E_\varepsilon}{E_y} = \frac{\int_{\omega_c}^{\infty} A_y^2(\omega)d\omega + \int_{\omega_c}^{\infty} A_k^2(\omega)d\omega}{\int_0^{\omega_c} A_y^2(\omega)d\omega + \int_0^{\omega_c} A_k^2(\omega)d\omega}$$

придем к утверждению, что возможно построение фильтра, генерирующего сигнал, пропорциональный разнице энергий обучающей и фактически полученной последовательностей, а вид этого сигнала аналитически определяется выражением $g(t) = \frac{sin\omega_c(t-\tau)}{\omega_c(t-\tau)}$. Следовательно, в такой постановке задачи будет один глобальный экстремум, характеризующий степень отличия $y_k(t)$ от $y(t)$. Это условие позволяет, как и МНК, использовать значение энергии разностного сигнала в качестве целевой функции для решения задачи подбора оптимального набора $\{W_k\}$ и гарантирует конечность алгоритма.

Отличия и особенности структуры различных вариантов применяемых сложных функций в частотно-временной области описываются корреляционными функциями [11]. Двумерная взаимно-корреляционная функция отклика ИНС $y_k(t)$ и целевой функции $y(t)$ может быть определена как

$$R_k(\tau, \Omega) = \frac{1}{2T\sqrt{PP_k}} \int_{-\infty}^{\infty} y_k(t-\tau)y^*(t)e^{j\Omega t}dt$$

Здесь $P_{(k)} = \frac{1}{T}\int_{t_0}^{t_n} y_{(k)}^2(t)dt$ – мощности функций $y(t)$ и $y_k(t)$ соответственно, * - знак комплексного сопряжения, Ω и τ – сдвиги одной функции относительно другой по частоте и времени соответственно. Двумерная взаимно-корреляционная функция (ДВКФ) обладает тремя свойствами, которые позволяют использовать её в качестве целевой функции для

обучения ИНС. Во-первых, ДВКФ имеет глобальный максимум $R_k(0,0) = 2E$ (E – энергия сигнала $y(t)$) или для нормированной ДВКФ $R_k(0,0) = 1$. Во-вторых, она симметрична относительно максимума $\tau = 0, \Omega = 0$. В-третьих, объем ДВКФ постоянен и равен (для нормированных сигналов) $V = \frac{1}{2\pi}\iint R_k^2(\tau,\Omega)d\tau d\Omega = 1$.

3.2 Коэффициент взаимного различия как мера обучения ИНС

При анализе сложных сигналов в каналах с помехами, а также при оценке помехоустойчивости таких устройств важной является мера различимости структуры сигналов и воздействующих помех в частотно-временной области [11, 16]. Полагая, что $y_k(t)$ является смесью полезной функции $y(t)$ и помехи $\mu(t)$, возникающей в связи с неудачно подобранным набором значений W_i, количественное выражение этой меры может быть определено как коэффициент взаимного различия функции отклика $y_k(t)$ и целевой функции $y(t)$:

$$g_k^2 = \frac{l_x^2 + l_y^2}{4PP_k},$$

где $l_x = \frac{2y\mu}{T}\int_{t_0}^{t_n} y(t)y_k(t)dt$ и $l_y = \frac{2y\mu}{T}\int_{t_0}^{t_n} y(t)y_k^*(t)dt$. Коэффициент g_k^2 представляет собой нормированную величину, пропорциональную при $t = T$ мощности процесса на выходе фильтра, согласованного с $y(t)$ при прохождении через него $y_k(t) = y(t)\mu(t)$. Коэффициент взаимного различия определяет относительную величину перекрытия в частотно-временной области функций $y(t)$ и $y_k(t)$. Чем меньше его значение, тем меньше их взаимное влияние. Показатель g_k^2 представляет собой огибающую ДВКФ и зависит от вида и свойств функций. Следовательно, расчет $R(\Omega,\tau)$ для произвольных τ,Ω вычислительно сложен,. поэтому ограничимся его анализом в 2-х сечениях: для $\tau = 0, \Omega \neq 0$ и $\tau \neq 0, \Omega = 0$ (рис. 1). Для сигналов, ограниченных во времени прямоугольным окном $[0, t_n]$, показатель будет иметь вид, изображенный на рис. 1. На рис. 2 представлены срезы этой зависимости при изменяющихся значениях τ. Рис. 1 наглядно демонстрирует «синкулярный» характер показателя g вида $\mathrm{sinc}\, x = {\sin x}/{x}$ в трехмерном изображении. Он представляет собой нормированную величину, пропорциональную при $t = T$ мощности процесса на выходе фильтра, согласованного с $y(t)$. Использование нормирующего коэффициента $\frac{1}{2T\sqrt{PP_k}}$ приводит диапазон изменения коэффициента в отрезке $[0,1]$. Преимуществом предлагаемого показателя заключается в том, что если функции $y(t)$ и $y_k(t)$ ортогональны (в усиленном смысле), то показатель достигает своей левой границы. Если же функция $y_k(t)$ стремится к целевой функции $y(t)$, то показатель достигает правой границы. Также как квадратичная функция, показатель g имеет один глобальный экстремум и, таким образом, позволяет использовать его как целевую функцию поиска оптимального значения весов ИНС $\{W_k\}$. Кроме того, предлагаемый показатель не имеет такой чувствительности к выбросам, как МНК, т.к. является интегральным показателем.

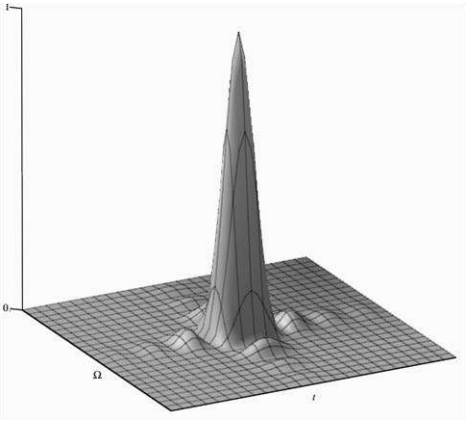


Рис. 1. Зависимость показателя g_k^2 от τ и Ω
Fig. 1. The dependence of the parameter g_k^2 on τ and Ω

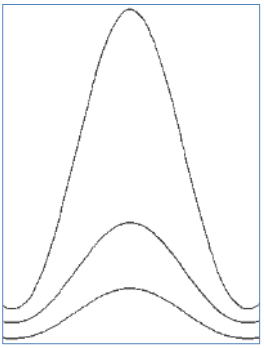


Рис. 2. Зависимость показателя g_k^2 от τ при различных $\Delta\Omega$
Fig. 2. The dependence of the parameter g_k^2 on τ at different $\Delta\Omega$

4. Сравнительная характеристика предлагаемого метода с существующими

Так сложилось в процессе построения и эволюции ИНС, что основным инструментом оценки достижения цели в процессе обучения стал МНК. МНК в общем виде – инструмент математической статистики, позволяющий получать несмещенную, эффективную и состоятельную оценку приближения получаемых и ожидаемых выходных значений, на основании которой принимается решение об изменении весовых параметров ИНС [18]. МНК применяется, как правило, для оценки статических моделей. Проблема МНК состоит в том, что матричная алгебра хотя и позволяет создание многопараметрических моделей, но они все являются линейными. Конечно, в общем случае, в качестве аппроксимирующей функции может быть использована квадратичная, экспоненциальная и любая другая. Однако в подавляющем большинстве случаев применяется именно линейная модель как наиболее простая из перечисленных. В тоже время линейная зависимость между ожидаемыми Y и фактическими $\hat{Y}$ значениями маловероятна вследствие нелинейности передаточной характеристики ИНС. Отсюда текущие проблемы с обучением ИНС – множество локальных экстремумов, отсутствие экстремумов на значительном промежутке значений весовых параметров $\{W_k\}$ и т.п. Одной из основных гипотез МНК является предположение о равенстве дисперсий отклонений, т.е. их разброс вокруг среднего

(нулевого) значения ряда должен быть величиной стабильной [18]. На практике дисперсии отклонений достаточно часто неодинаковы, то есть наблюдается гетероскедастичность. Это может быть следствием разных причин. Например, возможны ошибки в обучающих данных. Случайные неточности в исходной информации могут привести к получению некорректного результата. В процессе обучения ИНС является динамической системой с обратной связью, в которой изменение весовых параметров $\{W_k\}$ осуществляется на основе некоторой целевой функции $\delta(Y,\hat{Y})$, где Y – ожидаемые выходные значения, а $\hat{Y}$ – фактически полученные выходные значения, δ – функция невязки. Изменение параметров $\{W_k\}$, в свою очередь, ведет к изменению значений $\hat{Y}$. В теории управления такое поведение объекта называют параметрической идентификацией модели. Для процесса обучения важна обратная связь, т.к. движение значений весовых параметров $\{W_k\}$ в одном направлении чревато вхождением в «область насыщения», когда даже значительные изменения входных данных не вызывают никаких изменений на выходе. В нынешнем виде алгоритмы обучения отвергают эту динамику системы, наращивая суммарную ошибку невязки. Основным достоинством предлагаемого показателя является отсутствие каких-либо требований к виду выходной функции и зависимостью между Y и $\hat{Y}$. Взаимно-корреляционная функция вида $R=\frac{1}{K}\int_{-\infty}^{\infty} y(t)y_k(t-\tau)d\tau$ или $R=\frac{1}{K}\int_{-\infty}^{\infty} y(\Omega)y_k(\Omega-\Delta\Omega)d\tau$ (где K – нормирующий коэффициент) оценивает нормированную взаимную энергию функций $y(t)$ и $y_k(t)$, если они пересекаются на интервале τ (и имеют общий спектр). Обучающая последовательность $\{X_i,Y_i\}$ может быть представлена не в виде многомерных векторов, а в виде одномерных сигналов $x(t),y(y)$. Как видно из рис. 1, на всем протяжении показатель $g^2=R^2(\tau,\Omega)$ имеет один значительный локальный максимум и не зависит от передаточной характеристики ИНС. Поэтому градиент весовых параметров $\nabla\{W_k\}$ может иметь практически линейную зависимость от показателя g^2, а основной задачей управления обучением является отслеживание области высокой нелинейности выходной функции нейронов, что также может быть реализовано с помощью предлагаемого показателя. Если МНК представляет собой огибающую разницы амплитуд значений Y и $\hat{Y}$, то показатель g^2 несет в себе сравнение энергетических составляющих функций $y(t)$ и $y_k(t)$, причем не только во временном (фазовом) разрезе, но в частотном. Используя комплексное представление обучающих значений, предлагаемый показатель позволяет осуществлять поиск глобального максимума с учетом нелинейных (фазовых и частотных) изменений.

Таким образом, двумерная (комплексная) взаимно-корреляционная функция может служить математической моделью, которая позволяет отслеживать влияние параметров ИНС на отклонение фактических выходных значений от желаемых, а применение квадрата взаимно-корреляционной функции для анализа расхождений ожидаемой функции $y(t)$ и фактически полученной для набора весов $\{W_k\}$ функции $y_k(t)$ позволяет осуществлять оценку для всего обучающего множества. Предлагаемый подход позволит избежать «попадания» в локальный минимум за счет получения оценки по всей обучающей последовательности, а не по каждому конкретному значению. Таким образом, применение показателя g^2 является решением задачи поиска глобального экстремума целевой функции и обеспечивает конечность алгоритма обучения.

5. Заключение

В работе предложена модель ИНС как системы преобразования и передачи информации. Для анализа степени искажений в процессе обучения предлагается использовать комплексный показатель, который можно охарактеризовать как коэффициент взаимного различия обучаемой и фактически полученной последовательностей. Показатель представляет собой интегральное значение, полученное на основании всей обучающей выборки, что исключает «попадание» в локальный экстремум, как это часто происходит при использовании МНК – наиболее популярного метода, используемого сегодня при анализе

степени обучения ИНС. Эффективность предлагаемой модели основывается на широком применении метода сравнения энергетических характеристик сигналов в системах передачи данных. Таким образом, предложенная модель позволит решит задачу поиска глобального экстремума и повысить эффективность обучения ИНС.

Дальнейшими направлениями исследования являются: использование предложенного показателя для поиска скрытых взаимосвязей и корреляций признаков во входной информации; разработка эффективного алгоритма изменения весовых показателей для обучения ИНС.

Список литературы

[1]. Колмогоров А.Н. О представлении непрерывных функций нескольких переменных в виде суперпозиций непрерывных функций одного переменного и сложения. Доклады Академии наук, Российская академия наук, том 114, № 5, 1957 г., стр. 953-956.
[2]. Арнольд В.И. О представлении функций нескольких переменных в виде суперпозиции функций меньшего числа переменных. Математическое просвещение, вып. 3, 1958 г., стр. 41—61.
[3]. Hecht-Nielsen R. Neurocomputing: picking the human brain. IEEE spectrum, vol. 25, no. 3, 1988, pp. 36-41
[4]. Дзядык В.К. Введение в теорию равномерного приближения функций полиномами. Наука, 1977.
[5]. Hebb D. O. The organization of behavior. New York: Wiley, 1949.
[6]. Hinton G.E. Training products of experts by minimizing contrastive divergence. Neural computation, vol. 14, no. 8, 2002, pp. 1771-1800.
[7]. Sreenivasulu D., Krishna P.V. Deep Learning Based Efficient Channel Allocation Algorithm for Next Generation Cellular Networks. Programming and Computer Software, vol. 44, no. 6, 2018, 428-434.
[8]. Hinton,G.E. Learning multiple layers of representation. Trends in cognitive sciences, vol. 11, no. 10) 2007, pp. 428-434.
[9]. Николенко С.И., Кадурин А.А., Архангельская Е.О. Глубокое обучение. Питер, 2018, 480 с.
[10]. Шеннон К. Работы по теории информации и кибернетике. Издательство иностранной литературы, 1963.
[11]. Сикарев А.А., Лебедев О.Н. Микроэлектронные устройства формирования и обработки сложных сигналов. Радио и связь, 1983.
[12]. Widrow B. Adaptive sampled-data systems—a statistical theory of adaptation. IRE Wescon Convention Record, vol. 4, 1959, pp. 74-85.
[13]. Айфичер Э.С., Джервис Б.У. Цифровая обработка сигналов: практический подход, 2-е издание. Издательский дом «Вильямс», 2008 г., 992 с.
[14]. Dorogov A.Y. Implementation of spectral transformations in the class of fast neural networks. Programming and Computer Software, vol. 29, no. 4, 2003, pp.187-198.
[15]. Хайкин С. Нейронные сети: полный курс, 2-е издание. Издательский дом Вильямс, 2006 г., 1104 с.
[16]. Adjemov S.S., Klenov N.V., Tereshonok M.V., Chirov D.S. The use of artificial neural networks for classification of signal sources in cognitive radio systems. Programming and Computer Software, vol. 42, no. 3, 2016, pp 121–128.
[17]. Солодов А.В. Теория информации и ее применение к задачам автоматического управления и контроля. Наука, глав. ред. физико-математической литературы, 1967 г.
[18]. Линник Ю. В. Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений. Государственное изд-во физико-математической литературы, 1958 г.

References

[1]. Kolmogorov A.N. On the representation of continuous functions of several variables in the form of superpositions of continuous functions of one variable and addition. Doklady Akademii nauk, Rossijskaya akademiya nauk [Reports of the Academy of Sciences, Russian Academy of Sciences], vol. 114, № 5, 1957., pp. 953-956. (in Russian)

[2]. Arnol'd V.I. On the representation of functions of several variables as a superposition of functions of a smaller number of variables. Mat. Prosveshchenie [Math. education], vol. 3, 1958, pp. 41—61. (in Russian)
[3]. Hecht-Nielsen R. Neurocomputing: picking the human brain. IEEE spectrum, vol. 25, no. 3, 1988, pp. 36-41
[4]. Dzyadyk V.K. Introduction to the theory of uniform approximation of functions by polynomials. Nauka [Science], 1977. (in Russian)
[5]. Hebb D. O. The organization of behavior. New York: Wiley, 1949.
[6]. Hinton G.E. Training products of experts by minimizing contrastive divergence. Neural computation, vol. 14, no. 8, 2002, pp. 1771-1800.
[7]. Sreenivasulu D., Krishna P.V. Deep Learning Based Efficient Channel Allocation Algorithm for Next Generation Cellular Networks. Programming and Computer Software, vol. 44, no. 6, 2018, 428-434.
[8]. Hinton,G.E. Learning multiple layers of representation. Trends in cognitive sciences, vol. 11, no. 10) 2007, pp. 428-434.
[9]. Nikolenko S.I., Kadurin A.A., Arhangel'skaya E.O. Deep learning. Piter [Piter], 2018, 480 p. (in Russian)
[10]. Shennon K. Works on information theory and cybernetics. Izdatel'stvo inostrannoj literatury [Foreign Literature Publishing House], 1963. (in Russian)
[11]. Sikarev A.A., Lebedev O.N. Microelectronic devices for the formation and processing of complex signals. Radio i svyaz' [Radio and communication], 1983. (in Russian)
[12]. Widrow B. Adaptive sampled-data systems—a statistical theory of adaptation. IRE Wescon Convention Record, vol. 4, 1959, pp. 74-85.
[13]. Ajficher E.H.S., Dzhervis B.U. Digital Signal Processing: A Practical Approach, 2nd Edition. Izdatel'skij dom «Vil'yams» [Publishing House "Williams"], 2008, 992 p. (in Russian)
[14]. Dorogov A.Y. Implementation of spectral transformations in the class of fast neural networks. Programming and Computer Software, vol. 29, no. 4, 2003, pp.187-198.
[15]. Hajkin S. Neural Networks: Full Course, 2nd Edition. Izdatel'skij dom «Vil'yams» [Publishing House "Williams"], 2006, 1104 p. (in Russian)
[16]. Adjemov S.S., Klenov N.V., Tereshonok M.V., Chirov D.S. The use of artificial neural networks for classification of signal sources in cognitive radio systems. Programming and Computer Software, vol. 42, no. 3, 2016, pp 121–128.
[17]. Solodov A.V. Information theory and its application to the tasks of automatic control and monitoring. Izd-vo "Nauka", glav. red. fiziko-matematicheskoj lit-ry [Publishing house "Science"], 1967.
[18]. Linnik YU. V. The method of least squares and the basics of mathematical and statistical theory of processing observations. Gos. izd-vo fiziko-matematicheskoj lit-ry [State publishing house of physical and mathematical literature], 1958 (in Russian)

Информация об авторах / Information about authors

Николай Анатольевич ВЕРШКОВ, кандидат технических наук, старший научный сотрудник Ставропольского краевого института развития образования, повышения квалификации и переподготовки работников образования.

Nikolay Anatolievitch VERSHKOV – Candidate of Technical Sciences, Senior Researcher at the Stavropol Regional Institute for the Development of Education, Advanced Training and Retraining of Educators.

Виктор Андреевич КУЧУКОВ является специалистом отдела научно-технической информации, наукометрии и экспортного контроля Управления науки и технологий Северо-Кавказского федерального университета. Его научные интересы включают распознавание образов, системы остаточных классов.

Viktor Andreevich KUCHUKOV is a specialist of the department of scientific and technical information, scientometrics and export control of the Department of Science and Technology of the North Caucasus Federal University. His research interests include pattern recognition, residual class systems.

Наталья Николаевна КУЧУКОВА – ведущий специалист Центра перспективных исследований и разработок технологий Северо-Кавказского федерального университета.

Natalya Nikolaevna KUCHUKOVA – Leading Specialist, Center for Advanced Research and Technology Development, North Caucasus Federal University.

DOI: 10.15514/ISPRAS-2019-31(2)-5

Mitigating MAC Layer Performance Anomaly of Wi-Fi Networks through Adaptable Channelization

[1] *A. Hussain, ORCID: 0000-0001-6095-1260 <abid.hussain@seecs.edu.pk>*
[2] *M. Safyan, ORCID: 0000-0003-4501-9699 <msafyan@gcul.edu.pk*
[3] *S. Sarwar, ORCID: 0000-0001-9714-6580 <sohail.sarwar@seecs.edu.pk>*
[3] *Z. Ul Qayyum, ORCID: 0000-0003-4230-6895 <zia@aiou.edu.pk>*
[4,5] *M. Iqbal, ORCID: 0000-0002-8438-6726 <m.iqbal@lsbu.uk>*
[1] *N.A. Saqib, ORCID: 0000-0003-1976-0643 <nazrabbas@eme.edu.pk>*

[1] *School of Electrical Engineering and Computer Science, NUST, Pakistan*
[2] *Department of Computing, GC University Lahore, Pakistan*
[3] *Department of Computer Science, University of Gujrat, Pakistan*
[4] *School of Engineering London South Bank University, England*
[5] *School of Computer Science and Electronic Engineering University of Essex, England*

Abstract. 802.11 wireless local area networks (WLANs) can support multiple data rates at physical layer by using adaptive modulation and coding (AMC) scheme. However, this differential data rate capability introduces a serious performance anomaly in WLANs. In a network comprising of several nodes with varying transmission rates, nodes with lower data rate (slow nodes) degrade the throughput of nodes with higher transmission rates (fast nodes). The primary source of this anomaly is the channel access mechanism of WLANs which ensures long term equal channel access probability to all nodes irrespective of their transmission rates. In this work, we investigate the use of adaptable width channelization to minimize the effect of this absurdity in performance. It has been observed that surplus channel-width due to lower transmission rate of slow nodes can be assigned to fast nodes connected to other access points (APs), which can substantially increase the overall throughput of the whole network. We propose a medium access control (MAC) layer independent anomaly prevention (MIAP) algorithm that assigns channel-width to nodes connected with different APs based on their transmission rate. We have modeled the effect of adaptable channelization and provide lower and upper bounds for throughput in various network scenarios. Our empirical results indicate a possible increase in network throughput by more than 20% on employing the proposed MIAP algorithm.

Keywords: Transmission Rates; Channel Access; Adaptive Channel; Anomaly Prevention; Throughput

For citation: Hussain A., Safyan M., Ul Qayyum Z., Sarwar S., Iqbal M., Saqib N.A. Mitigating MAC Layer Performance Anomaly of Wi-Fi Networks through Adaptable Channelization. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 53-66. DOI: 10.15514/ISPRAS-2019-31(2)-5

Сглаживание аномалий производительности сетей Wi-Fi на уровне MAC путем адаптивного выделения каналов

[1] *А. Хуссейн, ORCID: 0000-0001-6095-1260 <abid.hussain@seecs.edu.pk>*
[2] *М. Сафьян, ORCID: 0000-0003-4501-9699 <msafyan@gcul.edu.pk*
[3] *С. Сарвар, ORCID: 0000-0001-9714-6580 <sohail.sarwar@seecs.edu.pk>*
[3] *З.Уль Кайум, ORCID: 0000-0003-4230-6895 <zia@aiou.edu.pk>*
[4,5] *М. Икбал, ORCID: 0000-0002-8438-6726 <m.iqbal@lsbu.uk>*
[1] *Н.А. Сакиб, ORCID: 0000-0003-1976-0643 <nazrabbas@eme.edu.pk>*

[1] *Школа электротехники и информатики,*
Национальный университет наук и технологий, Пакистан
[2] *Правительственный университет колледжа, Лахор, Пакистан*
[3] *Университет Гуджарата, Пакистан*
[4] *Лондонский университет Саут Бэнк, Великобритания*
[5] *Университет Эссекса, Великобритания*

Аннотация. Беспроводные локальные сети (WLAN) 802.11 могут поддерживать несколько скоростей передачи данных на физическом уровне с использованием схемы адаптивной модуляции и кодирования (AMC). Однако эта возможность поддержки разных скоростей передачи данных вызывает в WLAN серьезную аномалию производительности. В сети, состоящей из нескольких узлов с разными скоростями передачи, узлы с более низкой скоростью передачи данных (медленные узлы) ухудшают пропускную способность узлов с более высокими скоростями передачи (быстрые узлы). Основным источником этой аномалии является механизм доступа к каналу WLAN, который обеспечивает долгосрочную равную вероятность доступа к каналу для всех узлов независимо от их скоростей передачи. В этой работе мы исследуем использование адаптируемого разделения на каналы по ширине, чтобы минимизировать влияние этого явления на производительность. Отмечается, что ширина канала, избыточная из-за более низкой скорости передачи медленных узлов, может быть назначена быстрым узлам, подключенным к другим точкам доступа (AP), что может существенно увеличить общую пропускную способность всей сети. Мы предлагаем алгоритм предотвращения аномалий на уровне управления доступом к среде (MAC), который назначает ширину канала узлам, связанным с различными точками доступа, на основе их скорости передачи. Мы смоделировали эффект адаптивного разделения на каналы и установили нижнюю и верхнюю границы пропускной способности в различных сетевых сценариях. Наши эмпирические результаты указывают на возможное увеличение пропускной способности сети более чем на 20% при использовании предложенного алгоритма MIAP.

Ключевые слова: скорость передачи; доступ к каналу; адаптивный канал; предотвращение аномалий; пропускная способность

Для цитирования: Хуссейн А., Сафьян М., Сарвар С., Ул Кайум З., Икбал М., Сакиб Н.А. Сглаживание аномалий производительности сетей Wi-Fi на уровне MAC путем адаптивного выделения каналов. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 53-66 (на английском языке). DOI: 10.15514/ISPRAS-2019-31(2)-5

1. Introduction

The exponential increase in wireless enabled devices requires maximum capitalization of available resources in WLANs. This imminent requirement has triggered the re-evaluation of wireless protocols. Today's WLANs acclimatize several transmission parameters to achieve optimal network performance. However, some of the parameters like channel width and MAC layer functioning still remain static resulting in sub-optimal network performance.

Authors in [8] provide a detailed analysis of a performance anomaly at MAC layer of WLANs. If a wireless cell contains nodes with varying data rates, the throughput performance of fast nodes decreases substantially due to longer channel capturing of slow nodes. In [8] authors analytically modeled this anomalous behavior which is applicable to any multi- rate 802.11 network that uses

contention based channel access mechanism[1] at MAC layer. If X_s and X_f are throughputs of slow and fast nodes respectively, these can be measured as given in equation 1

$$X_s = X_f = \frac{S_d}{(N-1)T_f + T_s + P_c(N) \times t_{jam} \times N}, \quad (1)$$

where S_d is frame size, N is the number of wireless nodes, and T_f and T_s are transmission times of fast and slow nodes respectively. $P_c(N)$ is collision probability and t_{jam} is the time elapsed in collision.

Equation 1 is applicable only to single cell networks. However, rapid improvements in wireless technologies have shifted the paradigm of few users, single AP networks to several APs and numerous users per AP environments. We found that substantial increase in network wide performance is achievable if we divert network resources from a cell with limited need to another resource hungry cell. Adaptable width channelization [9] has been used to achieve this intelligent diversion of resources.

In this work, we propose MIAP algorithm that uses adaptable channelization to minimize the effect of MAC layer performance anomaly. The elementary concept of MIAP is to assign channels with high level of granularity thus maximizing the spectrum utilization. A node with low SNR values and subsequent low transmission rate transmit at narrow channel width and vice versa. In addition to this, use of adaptable channelization is independent of MAC layer and do not require any modification in channel access mechanism. It ensures that long term channel access probability of all the nodes remains equal and slow nodes do not suffer starvation. The channel width is adjusted by adding different number of sub-carriers. The use of narrower channels at nodes with lower SNR values adds several benefits to communication. Since narrower channels have higher spectral efficiency, it increases SNR of nodes. The performance of MIAP algorithm is measured on essential network parameters like network throughput, fairness index and frame size. The contributions of this research work can be outlined as follows.

1) Implementation of MAC layer independent channel width adaptation algorithm for minimizing the effect of MAC layer performance anomaly.
2) Analysis of proposed algorithm by measuring its effect on essential network parameters like throughput, fairness of channel access mechanism and frame size.
3) Implementation of proposed algorithm on real test-bed of USRP devices for accurate performance measurements.

The rest of this paper is organized as follows. Section 2 provides an overview of research work and proposed method for elimination of MAC layer performance anomaly. Section 3 presents the problem formulation and analytically models the solution. We have explained our proposed algorithm in Section 4. Section 5 explains the test-bed environment and experimentation methodology. Achieved results and discussion on these results are presented in section 6. Finally, we have concluded this work in Section 7.

2. Related Work

A substantive research on mitigating the effect of MAC layer performance anomaly in multi-rate WLANs has been presented in literature. The work proposed in [2][11][13][15] are of premier importance to this research study. In [13] authors have proposed an algorithm for performance anomaly reduction using open flow access points. The proposed model jointly reduces the effect of performance anomaly and number of hand offs, thus maximizing throughput by 26.7%. The research work given in [15] proposes a modification to control packets by embedding the data rate of two hops neighbors. In response to this control packet, the nodes adjust the initial value of contention window (CWmin) according to the data rate of neighboring nodes. In [11] authors claim that the performance anomaly model presented in [8] is only valid for networks having static channel characteristics. The nodes with better Signal-to-Noise (SNR) have higher channel access

rate as compared to nodes having lower SNR. This assertion ensures that the effect of MAC layer performance anomaly can be substantially reduced by using time-varying and time-correlated channels with Rayleigh fading effects.

The work presented in [2] mitigates the effect of MAC anomaly by controlling the value of back-off contention window based on signal strength of a node. Authors have concluded that, lower values of contention window for nodes having higher SNR considerably reduces the effect of MAC anomaly. In [12] an anomaly mitigation scheme for TCP friendly rate control (TFRC) protocol is presented. We named this approach as channel occupancy time based anomaly mitigation (COTAM). In this approach nodes estimate their share of leftover channel occupancy time and only make their communication in that slot. Majority of the techniques for mitigation of MAC layer anomaly restricts the channel access of nodes having lower transmission rate. This methodology adds further disadvantage to already poor performance of these nodes. This below par performance of slower nodes, in turns negatively affects the overall performance of complete network. The use of adaptable channelization has gained significant importance in recent studies [9][16].

The concept of adaptable channelization involves the granular use of available frequency spectrum. Research in [5][9][16] shows that a considerable increase in network capacity can be achieved if we use channels of adaptable widths. Since the advent of flexible channelization concept with the work presented on [5], the main focus of researchers remains on physical layer parameters, like transmission rate, interference, power consumption, delay spread and likewise. To best of our knowledge, to-date, no study for effect of flexible channelization on MAC layer is presented in literature.

3. Problem Formulation

802.11 networks use two spectrum blocks for their communication. These blocks consist of 2.4 GHz and 5 GHz frequency ranges. In this work, we are emphasizing only 2.4 GHz frequency spectrum used by 802.11 b/g/n networks for proof of concept purpose. The total available spectrum block in 802.11 b/g/n networks is divided into 14 channels of equal width of 22 MHz each [1]. To minimize the effect of co-channels interference (CCI), a guard band of 5 MHz is incorporated between any two consecutive channels. Each 22 MHz Wi-Fi channel is constituted of 52 sub-carriers. Out of these 4 sub-carriers are used for control signals while rest of 48 sub-carriers are used for data symbols [1]. The physical layer of Wi-Fi networks spread the data symbols on these 48 sub-carriers through orthogonal frequency division multiplexing (OFDM) or direct sequence spread spectrum (DSSS). The DSSS is only used to support legacy Wi-Fi devices like 802.11b.

3.1 Network Model

Consider a network of N_t nodes operating at transmission rate R. The set of N_t nodes is divided in two subsets of and N_f such that N_s, $N_f \subset N_t$ and $N_s \cup N_f = N_t$ where N_s consists of all the nodes transmitting below a threshold transmission rate R_s and referred as slow nodes. The other subset of N_f nodes transmit above the threshold transmission rate (R_s) and referred as fast nodes. The N_t nodes of network are associated with K_t access points with K_i denoting any *ith* AP. The set of nodes associated to any AP K_i is n_t such that $n_t = n_s \cup n_f$, $n_t \subset N_t$, $n_s \subset N_s$, and $n_f \subset N_f$ where n_s and n_s are the sets of slower and faster nodes attached to any single AP K_i. The K_t access points of network form K identifical circles in which their transmission can be received and decoded correctly. The association of nodes with an AP is independent of each other and follows Poisson distribution with probability density function as given by equation 2.

$$Pr\{n_t \to K_i\} = \frac{\lambda^{n_t} e^{-\lambda}}{n_t!} \qquad (2)$$

where $n_t \rightarrow K_i$ denotes the total number of nodes (n_t) associated to an access point K_i.

Consider the probability of a slow and a fast node connected to an AP K_i is ρ and $(1-\rho)$ respectively. Then the joint probability distribution of slower and faster nodes attached to any AP K_i is given by

$$Pr\{(n_s \wedge n_f) \rightarrow K_i\} = \rho^{n_s}(1-\rho)^{n_t-n_s} \qquad (3)$$

The probability that exactly s number of slow nodes are attached to any AP K_i at any given time t_i can be given as

$$Pr\{(n_s = s) \rightarrow K_i\} = \binom{n_s}{s} \rho^s(1-\rho)^{n_s-s} \qquad (4)$$

for $s = 0,1,2,\dots,n_s$ and $n_s = 0,1,2,\dots,n_t$.

The probability that maximum number of slow nodes attached to any AP K_i at any given time t_i is less than s can be given as

$$Pr\{(n_s < s) \rightarrow K_i\} = \sum_{s=0}^{n_s} \binom{n_s}{s} \rho^s(1-\rho)^{n_s-s} \qquad (5)$$

In a similar way, the probability that exactly (or less than) f number of fast nodes are attached to any AP K_i at any given time t_i will be

$$Pr\{(n_f = f) \rightarrow K_i\} = 1 - \binom{n_s}{s} \rho^s(1-\rho)^{n_s-s} \qquad (6)$$

$$Pr\{(n_f < f) \rightarrow K_i\} = 1 - \sum_{s=0}^{n_s} \binom{n_s}{s} \rho^s(1-\rho)^{n_s-s} \qquad (7)$$

for $f = 0,1,2,\dots,n_f$ and $n_f = 0,1,2,\dots,n_t$.

Similarly, the probability for slow and fast nodes operating in whole network at any given time t can be calculated by using equation 8 and 9 respectively.

$$Pr\{(N_s \leq S) \rightarrow K_i\} = \sum_{S=0}^{N_s} \binom{N_s}{S} \rho^S(1-\rho)^{N_s-S} \qquad (8)$$

for S = 0, 1, 2,…, N_s and N_s = 0, 1, 2,…, N_t

$$Pr\{(N_f \leq F) \rightarrow K_i\} = 1 - \sum_{S=0}^{N_s} \binom{N_s}{S} \rho^S(1-\rho)^{N_s-S} \qquad (9)$$

3.2 Throughput and Adaptable Channel

Let us assume that the network model given in subsection 3.1 uses L transmission channels $L_1, L_2 \dots, L_u$ for communication with L_i representing the *ith* channel. According to the throughput calculations given in [17], the channel capacity C (or maximum achievable throughput T) of a node operating on static width communication channel of bandwidth B in the presence of noise is $T = Blog_2(1 + SINR(dB))$ and $SINR(dB) = 10log_{10}SINR$. The achievable throughput of any node N_i (slower or faster) can be written as follows.

$$T(N_i) = Blog_2(1 + 10log_{10}SINR(N_i)) \qquad (10)$$

Authors in [4] have calculated signal to interference plus noise ratio ($SINR$) for static width channels. We can extend the same approach to get $SINR$ for varying channel widths as follows

$$SINR(N_i) = \frac{Pd(J_i, K_i)^{-\alpha}}{\delta + P\sum \varphi(L_i, L_j) d(K_i, K_j)^{-\alpha}} \qquad (11)$$

for L_i & $L_j \in L$; K_i & $K_j \in K$; L_i ! $\rightarrow$ K_i and $L_j \rightarrow K_j$; $i \neq j$. Here P is the transmission power, $d(N_i, K_i)$ is the distance between node N_i and access point K_i, δ is the path loss, which varies from 2 to 4 for a typical 802.11 network, α is the ambient noise, and $\varphi(L_i, L_j)$ is the partial overlapping

degree between channel L_i and L_j . This partial overlapping degree is given in [9]. The expression $L_i \not\rightarrow K_i$ shows that channel L_i is not associated to access point K_i, and the expression $L_i \rightarrow K_i$ shows that channel L_i is associated to access point K_i Equation 11 is true when the network operates in saturation mode, that is, all the APs have data to send or receive and not idle at any time. As this is not always true, it is generalized as shown in equation 12 below.

$$SINR(N_i) = \frac{Pd(J_i, K_i)^{-\alpha}}{\delta + P\beta(L_i)\sum \varphi(L_i, L_j) d(K_i, K_j)^{-\alpha}}, \qquad (12)$$

where $\beta(L_i)$ is the probability of channel occupation of any channel L_i. It is '1' when the network operates in saturation mode showing that all available channels have been occupied by the APs. By substituting the value of $SINR(N_i)$ in equation 10 from equation 12 we have

$$T(N_i) = Blog_2\left(1 + 10log_{10}\frac{Pd(J_i, K_i)^{-\alpha}}{\delta + P\beta(L_i)\sum \varphi(L_i, L_j) d(K_i, K_j)^{-\alpha}}\right) \qquad (13)$$

Equation 13 gives the throughput of a single node of network irrespective of its transmission rate. It is evident that throughput of any node is a function of available bandwidth (B). If a node is transmitting at a slower rate, it means that its bandwidth requirement is inherently less, which can be diverted to faster nodes.

$$T = B\sum_{i=1}^{N} log_2\left(1 + 10log_{10}\frac{Pd(J_i, K_i)^{-\alpha}}{\delta + P\beta(L_i)\sum \varphi(L_i, L_j) d(K_i, K_j)^{-\alpha}}\right) \qquad (14)$$

3.3 Mitigating the Effect of MAC Performance Anomaly

The bandwidth (B) of a channel is a sum of individual bandwidths of its sub-carriers. Using adaptable channelization we can increase or decrease the width of channel by varying the number of sub-carriers in that channel accordingly. In this work, we have varied the number of sub-carriers from 12 (5 MHz channel width) to 72 (30 MHz channel width).

Let us consider that N_t wireless nodes are distributed randomly across N_t APs. The transmission probability of a slower node is τ_s and transmission probability of faster node will then be $(1 - \tau_s)$. The probability that at any given time, only slow nodes are transmitting in each cell will be ${\tau_s}^{K_t}$. Similarly, the probability that only faster nodes are transmitting in a cell will be $(1 - \tau_s)^{K_t}$. The joint probability distribution that only fast or slower nodes will be transmitting at any time t_i will be given as

$$Pr\{\tau_s \vee \tau_f\} = \rho^{K_t} + (1 - \rho)^{K_t} \qquad (15)$$

This implies that both slower and faster nodes are transmitting in same or different cells will have the probability as given in equation 16.

$$Pr\{\tau_s \wedge \tau_f\} = 1 - (\rho^{K_t} + (1 - \rho)^{K_t}) \qquad (16)$$

Since contention base CSMA/CA protocol ensures equal long term probability of channel access to all nodes irrespective of their transmission rate, equation 14 implies that, the overall efficiency of a network is dependent on number of slower and faster nodes in that network. In this way, we have three possible scenarios.

1) Number of slower nodes is larger than number of faster nodes that result in $\tau_s > (1 - \tau_s)$.
2) Number of slower nodes is equal to the number of faster nodes that results in $\tau_s = (1 - \tau_s)$.
3) Number of slower nodes is less than number of faster nodes that results in $\tau_s < (1 - \tau_s)$.

$$T(n_s) = (B - B_l)log_2\left(1 + 10log_{10}\frac{Pd(J_i, K_i)^{-\alpha}}{\delta + P\beta(L_i)\sum \varphi(L_i, L_j) d(K_i, K_j)^{-\alpha}}\right) \qquad (17)$$

where $T(n_s)$ is the throughput of any slower node and B_l is the surplus bandwidth that is not required by slower node. Similarly the throughput of faster node will be,

$$T(n_f) = (B + B_l) log_2 \left(1 + 10 log_{10} \frac{P d(J_i, K_i)^{-\alpha}}{\delta + P\beta(L_i) \sum \varphi(L_i, L_j) d(K_i, K_j)^{-\alpha}}\right) \qquad (18)$$

4. The proposed channel width adaptation algorithm

In 802.11 networks the transmission rate of any node is a function of received signal strength (RSS) values. MIAP calculates the RSS and subsequent transmission rate of any node through channel reciprocity [14]. Based on these calculations, MIAP estimates the bandwidth requirement of a specific node and assigns channel of that width. At the initialization phase all the APs use standard non-overlapping channels. All APs are connected to a back-end management server through a wired link which controls all the activities like spectrum allocation, transmission rate determination etc. MIAP runs at this sever. The server calculates the optimal channel width and number of sub-carriers for the spectrum allocation to AP dynamically on the basis of transmission rate and RSS values.

If transmission rate changes at an AP, it is communicated to the management server. The AP releases or demands spectrum resource according to its current bandwidth status. If an AP needs more bandwidth, it notifies the server and the server check the status of available sub-carriers still not assigned to any AP. MIAP asks the server to check the demand considering the threshold values of RSS and transmission rate and decides if the increment in channel width is possible. Server then communicates the values of sub-carriers to the corresponding AP. After increasing the channel width AP starts spreading it signal by adding more frequencies to already in use sub-carriers.

On the other hand, if an AP has less bandwidth requirement it releases spectrum resource, which is added by the management server in its available pool of sub-carrier frequencies for its on demand dissemination to other APs on the network. If throughput requirement of an AP decreases at any given time it sends its new status to the management server. The management server checks the in-use sub-carriers and ask the AP to reduce its channel width by spreading its signal on lesser number of sub-carrier frequencies. Algorithm 1 explains the working of MIAP.

```
   Result: Required Channel Bandwidth (CB)
   Input: Transmission Rate (TR), RSS
   Output: Channel Bandwidth (CB), Transmission Parameters (TP)
 1 begin
 2         for N_i ∈ N_t do
 3           if RSS(N_i) ≤ RSS_(Max)
 4              then Calculate TR_(current) && TP ← TP for CB_(current)
 5              else
 6                 if TR < TR_(Max) && RSS ≥ RSS_(Max)
                      then
 7                       CB_(new) ← CB_current + 1.875 MHz;
                         while TR(N_i) = TR(N_i) do
 8                             Return CB_(new) && TP ← TP for CB_(new)
 9                       end
10                    else
11                       GoTo 7
12                    end
13             end
14           if TR ≥ TR_(Max)
15              then
16                    CB_(new) ← CB_current − 1.875 MHz;
17                    while TR(N_i) = TR(N_i) do
18                       Return CB_(new) && TP ← TP for CB_(new)
```

```
19                    end
20                 else
21                    GoTo 16
22              end
23           end
24 end
```

Algorithm 1: MAC layer Independent Anomaly Prevention Algorithm

5. Experimental setup and implementation

For empirical evaluation of MIAP, we have deployed an indoor network of three USRP kits connected to laptops running GNU radio software on Linux operating system (OS). Fig. 1 shows the layout of deployed network. As proof of concept, implementation of MIAP for 802.11g wireless networks has been made by significantly modifying transceiver implementation provided at CGRAN (Comprehensive GNU Radio Archive Network) website [3][10] and better explained in [6]. This implementation is extendable to any 802.11 standard, by modifying its parameters at physical layer accordingly.

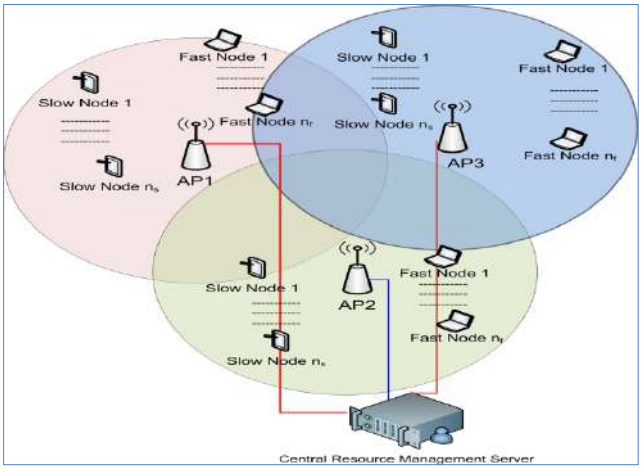


Fig 1: Topology of Experimental Network

A central management server constituted of Dell T-620 computer running MIAP on Linux OS has been placed for implementation of flexible channelization. Each USRP2 kit contained a 2400 RX/TX daughter card with omni-directional antennas. The specifications of USRP kit and daughter cards are available at website [7]. We have customized the physical layer of each AP in such a way that an AP can switch to any of narrower or wider channel widths at the end of current frame transmission. The wireless nodes detect the width of channels based on the preamble being transmitted by APs before the transmission of each frame.

6. Performance results and discussion

We performed a series of experiments to evaluate the effect of deploying MIAP on essential network performance parameters by using varying number of network nodes. We have deployed a network of 5, 10, 15, 20, 25, and 30 nodes in each cell with varying number of slow and fast nodes. The obtained results are averaged out by collecting traces of all APs for accurate efficiency measurement of MIAP.

We have evaluated our proposed algorithm for throughput gains for various ratio of slower and faster nodes. The slower nodes randomly choose their data rate from 6, 9, 12, 18. 24 and 36 (Mbps), while the faster nodes operate on maximum data rate they can achieve. The physical layer of faster nodes is modified to achieve maximum transmission rate. In some cases it is noted that

TR of faster nodes may reach to 128 Mbps. The achieved results are compared with standard 802.11g implementation, COTAM [12] and signal to noise ratio based contention window (SNR based CW) [2].

The comparison given in fig. 2 demonstrate that presented algorithm outperforms all its counterparts and shows a significant improvement in achieved throughput when compared with standard implementation of 802.11g physical layer. This improvement in achieved throughput becomes almost equal to 30% at some points. The reason behind this high throughput is the fact that, at any given time if a slower node in one cell is transmitting, the TR of faster node in other cell automatically increases. This increase in TR of faster cell diminishes the effect of slower node thus keeping the network wide average throughput on higher side.

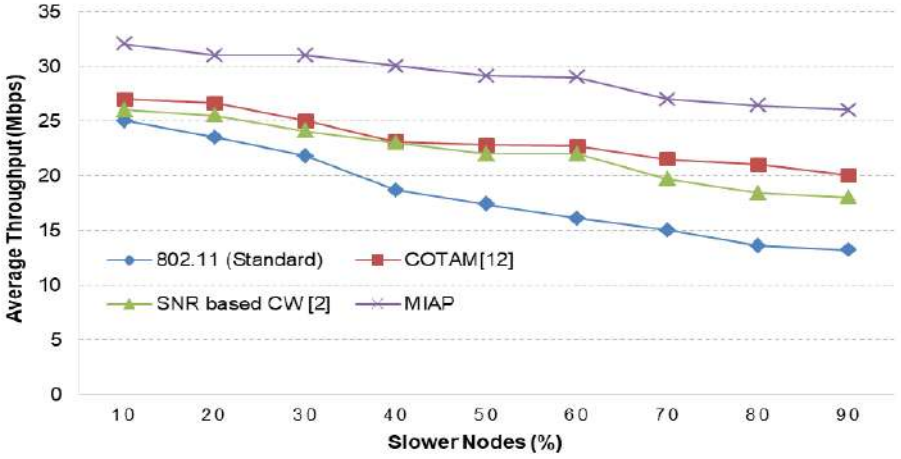


Fig 2: Average Network Wide Throughput Comparison

In fig 3, we evaluated the throughput performance of MIAP for slower and faster nodes and compared the results with standard 802.11 implementation. It is observed that MIAP significantly performs better than standard implementation due to better utilization of network resources. Since MIAP diverts surplus resources of slower cell to a faster cell which increases the efficiency of that cell without affecting the performance of slower cell. This efficient utilization of spectrum resources increases the average throughput of faster nodes. It is observed that for longer time intervals with nodes operating in saturation mode, the efficiency gains are significantly high.

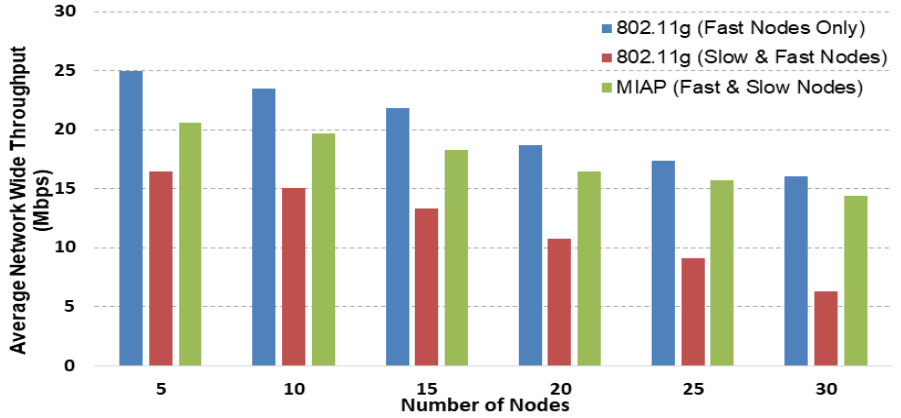


Fig 3: Average Network Wide Throughput Comparison

The results given in fig. 4 demonstrate the gain in average throughput of one cell with corresponding decrease of TR in adjacent cell. It is evident that if transmission rate of nodes in one cell decreases it automatically increases the TR of adjacent cell. It is noted that faster cell do not gain the exact throughput loss of slower cell. The reason behind this below par throughput gain is inefficiency of channel width detection mechanism. The rapid oscillation of channel width is not detected efficiently and some frames may loss in this process. This frame loss decreases the average throughput.

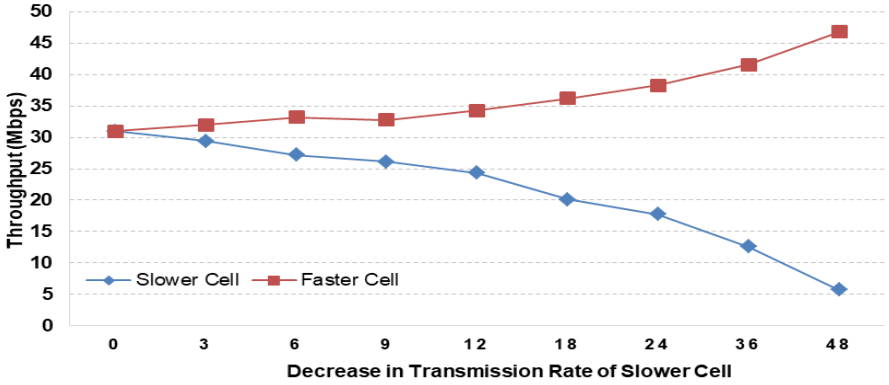


Fig 4: Average Network Wide Throughput Comparison

Fig 5 shows throughput of cell with faster node when TR of cell with slower nodes is fixed. The throughput comparison of MIAP for different MAC protocol data unit (MPDU) is given in Fig 6. The results show that longer the MAC fram higher will be the throughput. These results are self-explanatory considering that longer frames reduce the per unit time overhead of communication thus maximizing the throughput. The adaptable nature of MIAP further increases the throughput by maximum utilization of frequency spectrum.

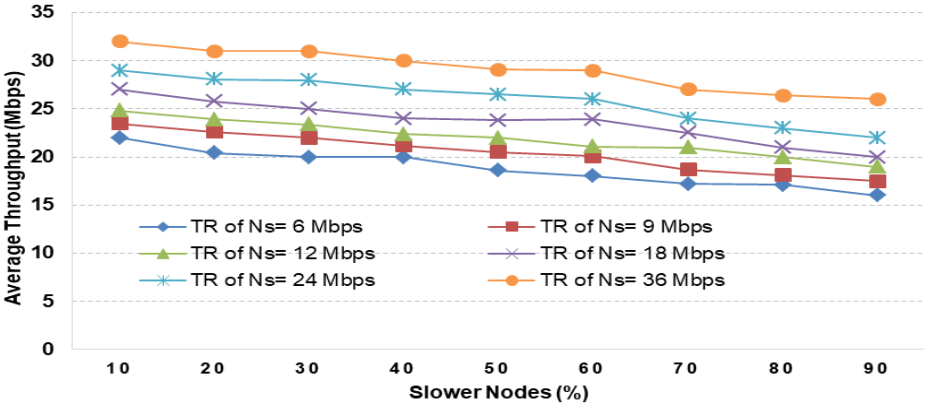


Fig 5: Throughput of Fast Nodes with Fixed TR of slower Nodes

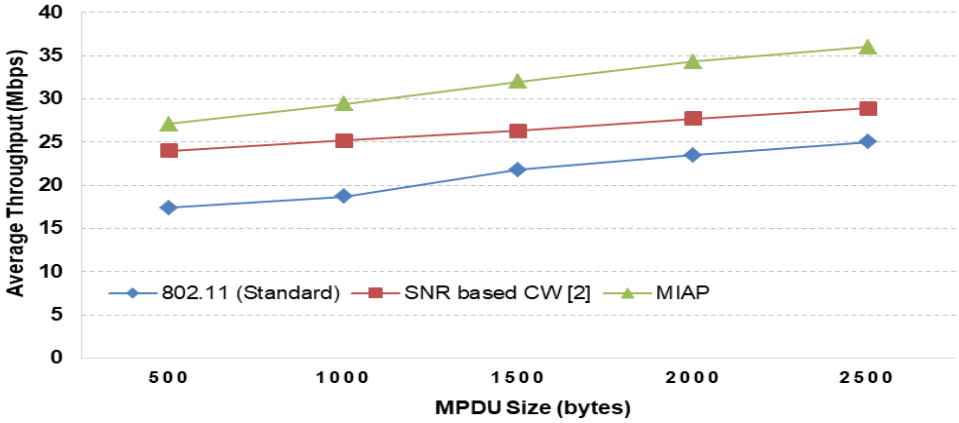


Fig 6: Average Throughput for Various MPDU sizes

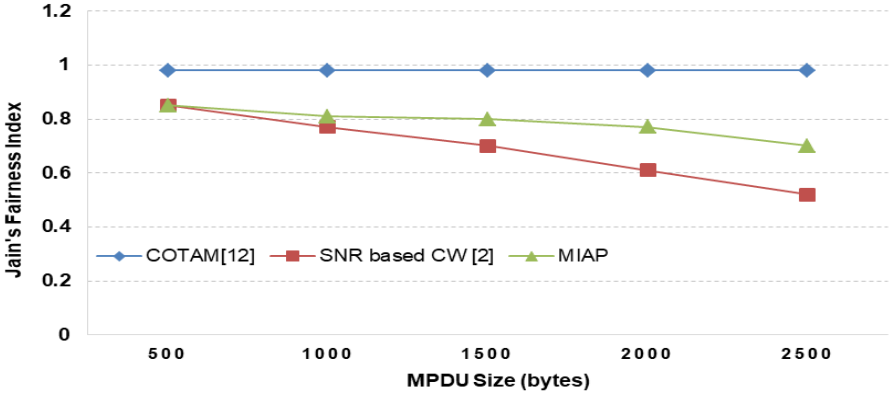


Fig 7: Channel Access Fairness for Various MPDU sizes

Finally, Fig 7 and Fig 8 show channel access fairness of MIAP for various sizes of MPDU and different number of nodes respectively. The achieved results depict that fairness of MIAP algorithm in granting channel access to various nodes is near to standard implementation. It is better than SNR based CW adaptation and below the performance of COTAM. Since MIAP is MAC layer independent mechanism and it does not change the channel access mechanism, therefore the fairness remains similar to standard implementation of 801.11 MAC. On the other hand SNR based CW adaptation performs poorly due to different sizes of contention window at different nodes.

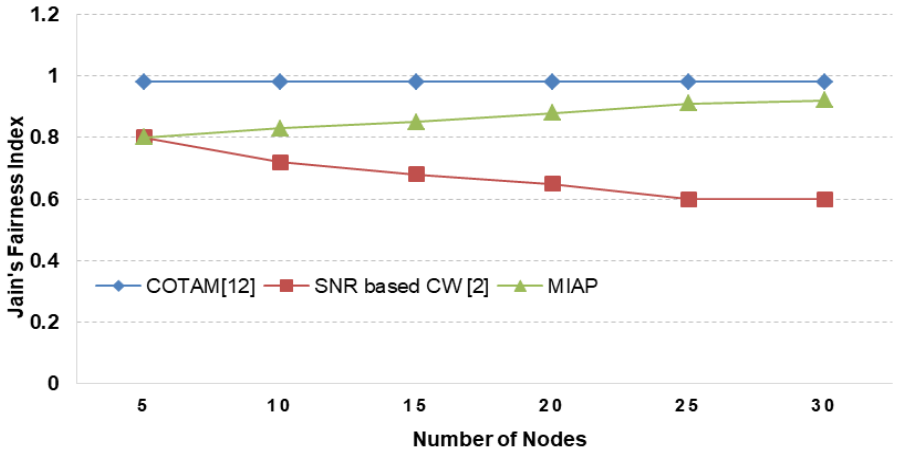


Fig 8: Channel Access Fairness for Different Number of Nodes

7. Conclusion

In this work, we propose an efficient mechanism to mitigate the effect of MAC layer performance anomaly by using adaptable width channelization in WLANs. The proposed algorithm assigns the channel widths based on transmission rate of nodes and divert the surplus frequency spectrum to resource hungry cells operating at higher transmission rates. We first probabilistically modeled the lower and upper bounds on number of slower and faster nodes in the network. In addition to this, we also analytically modeled the throughput and SINR of adaptable width channels. The evaluation of proposed algorithms is made based on throughput gains for different network settlements with varying number of slow and fast nodes. The throughput measurements show a significant improvement of more than 20% in achieved network capacity, with different combinations of slow and fast nodes. Moreover a detailed analysis on channel access fairness has also been presented. Since proposed algorithm is independent of channel access mechanism and do not require any change at MAC layer, thus long term channel access probability remains same for each network node.

Future work includes the implementation of adaptable channel widths in MIMO based wireless networks like 802.11n. In addition, development of a distributed channel adaptation algorithm that can assign spectrum resources locally on each AP is required. The effect of adaptable channelization on other essential network parameters like power consumption, transmission range, etc. is also needed to be explored.

References

[1]. 802.11-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), 2007.

[2]. O.C. Branquinho, N. Reggiani, and D.M. Ferreira. Mitigating 802.11 mac anomaly using snr to control back-off contention window. In Proc. of the International Conference Wireless and Mobile Communications, 2006,

[3]. The Comprehensive GNU Radio Archive Network (CGRAN). IEEE 802.11a/g/p ofdm transceiver. Available at: http://cgran.hopto.org/3000/, accessed 30.01.2019

[4]. Deepti Chafekar, V. S. Anil Kumar, Madhav V. Marathe, Srinivasan Parthasarathy, and Aravind Srinivasan. Capacity of wireless networks under sinr interference constraints. Wireless Network, vol. 17, no. 7, 2011 pp. 1605-1635.

[5]. Ranveer Chandra, Ratul Mahajan, Thomas Moscibroda, Ramya Raghavendra, and Paramvir Bahl. A case for adapting channel width in wireless networks. In Proc. of the ACM SIGCOMM 2008 Conference on Data Communication, 2008, pp. 135-146.
[6]. Andrea COSTANTINI. Implementation of an IEEE 802.11p transmitter in open-source Software Defined Radio. Master's thesis, Universit`a del Salento, Piazza Tancredi, 2009.
[7]. Ettus Research, Universal Software Radio Peripheral and Daughter Boards, Available at: http://www.ettus.com/product/details/UN210-KIT, accessed 30.01.2019.
[8]. M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In Proc. of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, vol. 2, 2003, pp. 836-843.
[9]. Abid Hussain and Nazar A. Saqib. Effects of implementing adaptable channelization in wifi networks. Mobile Information Systems, 2016, 15 p.
[10]. Abid Hussain, Nazar A. Saqib, Usman Qamar, Muhammad Zia, and Hassan Mahmood. Protocol-aware radio frequency jamming in wifi and commercial wireless networks. Journal of Communications and Networks, vol. 16, no. 4, 2014, pp. 397-406.
[11]. Seong il Hahm and Chong-Kwon Kim. Time-correlated fading can mitigate rate anomaly in ieee 802.11 wlans. In Proc. of the 9th International Symposium on Communications and Information Technology, 2009, pp. 560-561.
[12]. K. Kashibuchi, Y. Nemoto, and N. Kato. Mitigating performance anomaly of tfrc in multi-rate ieee 802.11 wireless lans. In Proc. of the Global Telecommunications Conference, 2009, pp. 1-6.
[13]. Won-Suk Kim, Sang-Hwa Chung, Chang-Woo Ahn, and Mi-Rim Do. Seamless handof and performance anomaly reduction schemes based on openow access points. In Proc. of the 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pages 316-321.
[14]. E. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta. Massive mimo for next generation wireless systems. IEEE Communications Magazine, vol. 52, no. 2, 2014, pp. 186-195.
[15]. Yumei Liu, Bo Lv, and Yan Li. A new mac mechanism to resolve 802.11b performance anomaly. In Proc. of the 2nd International Conference on Signal Processing Systems, vol. 3, 2010, pp. 134-138.
[16]. Shravan Rayanchu, Vivek Shrivastava, Suman Banerjee, and Ranveer Chandra. Fluid: Improving throughputs in enterprise wireless lans through exible channelization. IEEE Transactions on Mobile Computing, vol. 11, no. 9, 2012, pp. 1455-1469.
[17]. Herbert Taub and Donald L. Schilling. Principles of Communication Systems. McGraw-Hill Higher Education, 2nd edition, 1986.

Информация об авторах / Information about authors

Абид ХУССЕЙН получил степень доктора философии в Национальном университете наук и технологий, Исламабад, Пакистан. Его исследовательские интересы включают адаптацию полос беспроводного канала, физические атаки и атаки уровня MAC в беспроводных сетях и стохастическое моделирование поведения беспроводных сетей на физическом уровне и уровне MAC.

Abid HUSSAIN received a Ph.D. degree at National University of Sciences and Technology, Islamabad, Pakistan. His research interests include wireless channel band adaptation, physical and MAC layer attacks in wireless networks and stochastic modelling of physical and MAC layer behaviour of wireless networks.

Мухаммад САФЬЯН работает в Правительственном университете колледжа, Лахор, Пакистан. Он получил степень магистра в 2009 г. Национальном университете науки и технологии. Область его научных интересов включает отображение онтологий, электронное обучение, семантическое распознавание активностей.

Muhammad SAFYAN is in Government College University (GCU), Lahore. He received his MS degree from National University of Sciences and Technology in 2009. His area of interest is ontology alignment, e-learning and semantic activity recognition.

Сохаил САРВАР получил степень магистра в области информационных технологий в Национальном университете науки и технологии, Исламабад, Пакистан. В настоящее время он готовит диссертацию на соискание степени PhD на Компьютерном факультете

университета Гуджарата, Пакистан. Исследовательские интересы включают электронное обучение, семантические технологии и методы инженерии знаний.

Sohail SARWAR received the M.S. degrees in information technology from National University of Science and Technology. Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in the Department of Computing, University of Gujrat Pakistan. His research interests include e-learning, semantic technologies and knowledge engineering techniques.

Зия УЛЬ КАЙУМ в настоящее время является профессором в университете Гуджарата в Пакистане. Он получил степень PhD в области компьютерных наук в Университете Лидса, Великобритания, в 2005 году. В число научных интересов входят искусственный интеллект, инженерия знаний, интеллектуальный анализ знаний, семантический Web и электронное обучение.

Zia UL QAYYUM is currently a professor at University of Gujrat, Pakistan. He received his Ph.D. degree in computer science from Leeds University UK in 2005. His research interests include artificial intelligence, knowledge engineering, data mining, semantic web and e-learning.

Муддессар ИКБАЛ работает старшим преподавателем в Лондонском университете Саут Бэнк и в университете Эссекса, Великобритания. Он получил степень PhD в Кингстонском университете, Лондон, Великобритания. Его научные интересы включают сетевые технологии 5G, мультимедийные облачные вычисления, мобильные граничные вычисления, туманные вычисления, интернет вещей, программно-конфигурируемые сети, виртуализацию сетевых функций, качество восприятия, облачные инфраструктуры и службы.

Muddessar IQBAL is working as senior lecturer in London South Bank University and University of Essex, England. Dr. Iqbal completed his PhD from Kingston University in 2010. His research interests include 5G networking technologies, multimedia cloud computing, mobile edge computing, fog computing, Internet of Things, software-defined networking, network function virtualisation, quality of experience, and cloud infrastructures and services.

Назар Аббас САКИБ получил степень магистра наук в Университете Куэйд-и-Азам, Исламабад в 1993 году. Степень PhD в области электротехники получил в Центре исследований и перспективных исследований Национального политехнического института, Мексика. Его исследовательские интересы включают компьютерную и коммуникационную безопасность, криптографическое оборудование и проектирование систем на основе FPGA.

Nazar Abbas SAQIB recieved his master degree from Quaid-i-Azam University, Islamabad in 1993. He received his Ph.D. degree in Electrical Engineering from the Center for Research and Advanced Studies of the National Polytechnic Institute, Mexico. His research interests include computer and communication security, cryptographic hardware and FPGA based system design.

DOI: 10.15514/ISPRAS-2019-31(2)-6

Интеграция беспроводной связи для оптимизации распознавания окружения и расчёта траектории движения группы роботов

[1] *М.В. Иванов, ORCID: 0000-0002-5523-0343 <ivanovm@uabc.edu.mx>*
[1] *О.Ю. Сергиенко, ORCID: 0000-0003-4270-6872 <srgnk@uabc.edu.mx>*
[2] *В.В. Тырса, ORCID: 0000-0003-1623-5704 <vtyrsa@uabc.edu.mx>*
[1] *Л. Линднер, ORCID: 0000-0002-0623-6976 <lindner.lars@uabc.edu.mx>*
[2] *Х.С. Родригес-Киньонес, ORCID: 0000-0002-1830-0226 <julio.rodriguez81@uabc.edu.mx>*
[2] *В. Флорес-Фуэнтес, ORCID: 0000-0002-1477-7449 <flores.wendy@uabc.edu.mx>*
[1] *М. Ривас-Лопес, ORCID: 0000-0001-8751-4693 <mrivas@uabc.edu.mx>*
[2] *Д. Эрнандес-Бальбуэна, ORCID: 0000-0002-0055-4797 <dhernan@uabc.edu.mx>*
[3] *Х.И. Ньето Иполито, ORCID: 0000-0003-0105-6789 <jnieto@uabc.edu.mx>*

[1] *Автономный университет Нижней Калифорнии (UABC), Инженерный институт, Мехикали, Н.К., Мексика*
[2] *Автономный университет Нижней Калифорнии (UABC), Инженерный факультет, Мехикали, Н.К., Мексика*
[2] *Автономный университет Нижней Калифорнии (UABC), Факультет инженерии, архитектуры и дизайна, Енсенада, Н.К., Мексика*

Аннотация. В настоящее время искусственный интеллект и групповая робототехника становятся широко распространенными и используются в гражданских задачах. Основная цель статьи – показать возможность использования знаний о совместном окружении группы роботов при решении задачи навигации путем обеспечения передачи данных между роботами. В методике, представленной в статье, рассматривается комплекс задач, выполнение которых улучшает результаты роботизированной групповой навигации. Исследование затрагивает проблемы робототехнического зрения, планирования путей, хранения и обмена данными. В статье описывается структура лазерной системы технического зрения реального времени как основного инструмента взаимодействия роботов с окружающей. В системе зрения используется принцип динамической триангуляции. В статье приведены примеры полученных данных, методы сохранения разрешающей способности сканирования на расстоянии и контроля скорости. В соответствии с данными, полученными с помощью предоставленной системы зрения, было решено использовать матричный подход для планирования пути роботов, что позволяет решать задачи дискретизации окружения и аппроксимации траектории. Сравниваются два типа структуры сети для передачи данных. Авторы предлагают методологию формирования динамической сети на основе системы смены лидеров. Для апробации теории было разработано программное обеспечение для моделирования группы роботов. Полученные результаты показывают, что обмен знаниями внутри группы может значительно улучшить планирование траекторий движения роботов.

Ключевые слова: группа роботов; планирование путей; система зрения; 3D лазерный сканер; сети; передача данных.

Для цитирования: Иванов М.В, Сергиенко О.Ю., Тырса В.В, Линднер Л., Родригес-Киньонес Х.С., Флорес-Фуэнтес В., Ривас-Лопес М., Эрнандес-Бальбуэна Д., Нието Иполито Х.И. Интеграция беспроводной связи для оптимизации распознавания окружения и расчёта траектории движения

группы роботов. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 67-82. DOI: 10.15514/ISPRAS-2019-31(2)-6

Wireless integration to optimize environmental recognition and calculate the trajectory of a group of robots

[1] *M.V. Ivanov, ORCID: 0000-0002-5523-0343 <ivanovm@uabc.edu.mx>,*
[1] *O.Yu. Sergiyenko, ORCID: 0000-0003-4270-6872 <srgnk@uabc.edu.mx>*
[2] *V.V. Tyrsa, ORCID: 0000-0003-1623-5704 <vtyrsa@uabc.edu.mx>*
[1] *L. Lindner, ORCID: 0000-0002-0623-6976 <lindner.lars@uabc.edu.mx>*
[2] *J.C. Rodriguez-Quiñonez, ORCID: 0000-0002-1830-0226 <julio.rodriguez81@uabc.edu.mx>*
[2] *W. Flores-Fuentes, ORCID: 0000-0002-1477-7449 <flores.wendy@uabc.edu.mx>*
[1] *M. Rivas-Lopez, ORCID: 0000-0001-8751-4693 <mrivas@uabc.edu.mx>*
[2] *D. Hernández-Balbuena, ORCID: 0000-0002-0055-4797 <dhernan@uabc.edu.mx>*
[3] *J.I. Nieto Hipólito, ORCID: 0000-0003-0105-6789 <jnieto@uabc.edu.mx>*

[1] *Universidad Autonoma de Baja California (UABC), Instituto de Ingeniería, Mexicali, B.C., Mexico*
[1] *Universidad Autonoma de Baja California (UABC), Facultad de Ingeniería, Mexicali, B.C., Mexico*
[3] *Universidad Autonoma de Baja California (UABC), Facultad de Ingenieria, Arquitectura y Diseño, Ensenada, B.C., Mexico*

Abstract. Nowadays artificial intelligence and swarm robotics become wide spread and take their approach in civil tasks. The main purpose of the article is to show the influence of common knowledge about surroundings sharing in the robotic group navigation problem by implementing the data transferring within the group. Methodology provided in article reviews a set of tasks implementation of which improves the results of robotic group navigation. The main questions for the research are the problems of robotics vision, path planning, data storing and data exchange. Article describes the structure of real-time laser technical vision system as the main environment-sensing tool for robots. The vision system uses dynamic triangulation principle. Article provides examples of obtained data, distance-based methods for resolution and speed control. According to the data obtained by provided vision system were decided to use matrix-based approach for robots path planning, it inflows the tasks of surroundings discretization, and trajectory approximation. Two network structure types for data transferring are compared. Authors are proposing a methodology for dynamic network forming based on leader changing system. For the confirmation of theory were developed an application of robotic group modeling. Obtained results show that common knowledge sharing between robots in-group can significantly decrease individual trajectories length.

Keywords: robotic group; path planning; vision system; 3D laser scanner; network; data transferring

For citation: Ivanov M.V., Sergiyenko O.Yu., Tyrsa V.V., Lindner L., Rodriguez-Quiñonez J.C., Flores-Fuentes W., Rivas-Lopez M., Hernández-Balbuena D., Nieto Hipólito J.I. Wireless integration to optimize environmental recognition and calculate the trajectory of a group of robots. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 67-82 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-6

1. Введение

Успешное использование мобильных роботов в различных областях гражданской промышленности приводит исследователей к задаче эффективного контроля группы роботов. В качестве примеров можно упомянуть обнаружение объектов в различных видах окружающей среды, использование группы в качестве распределенной сенсорной системы для химического анализа и т. д.

Обобщая все задачи, мы можем сказать, что взаимодействие агентов в группе роботов на трудно проходимой местности является одной из основных проблем. В окружении такого типа группа обычно рассредоточивается по территории. Такое размещение дает роботам

возможность выполнять задачи обнаружения динамических событий в реальном времени в окружающей среде, поиска объектов и т. д. лучше, чем, например, сеть статических датчиков. Это достижимо, потому что каждый отдельный робот может покрывать большую часть площади, патрулируя, а не оставаясь в неподвижном состоянии. Это означает, что группа может выполнять мониторинг среды с меньшим количеством датчиков. Для достижения автоматизации внутри группы при выполнении таких задач роботы должны работать с предопределенными правилами коллективного поведения.

Каждый отдельный робот в группе – это устройство с определенным набором функций (восприятие, связь, движение и вычислительная обработка) и ограничивающими их факторами. В статье рассматривается возможность использования однородной группы роботов ([1], [2]), которые могут независимо выполнять различные простые задачи. Кроме того, роботы должны иметь возможность двигаться к своей цели в окружающей среде, не теряя при этом контакта с членами группы. Именно поэтому были выделены три типа задач, которые необходимо решать одновременно в режиме реального времени.

- Обнаружение и локализация препятствий. Успех мобильной группы роботов в неструктурированной среде возможен только в том случае, если они способны приспосабливаться к переменным факторам среды. Эти изменения, которые включают в себя наличие новых препятствий, могут быть обнаружены с использованием сенсорных систем, таких как лазерные системы технического зрения, камеры и т. д. Обнаружение препятствий служит начальным состоянием планирования движения для прогнозирования возможных маршрутов.
- Обмен данными в группе ([3], [4]). Необходимость в передаче данных может возникнуть в случае, когда группа роботов должна принять коллективное решение, при отсутствии данных для принятия индивидуального решения или также для информирования других роботов о возникновении резких изменений окружающей среды.
- Планирование траектории или коллективная навигация ([5], [6], [7], [8]). Для группы роботов в трудно проходимой местности реализуется задача планирования потенциальных траекторий через неизвестное поле препятствий из заданной начальной точки в искомую.

Таким образом, основной вклад статьи заключается в рассмотрении возможных решений этих проблем и их внедрении в модель, чтобы понять влияние обмена данными на взаимодействие роботизированной группы с окружающей средой во время задачи картографирования [9] и обнаружения цели.

2. Система технического зрения

Наиболее распространенные системы видения используют подходы, основанные на CCD или CMOS ([10], [11], [12], [13]), более дорогое оборудование, например, камеры Time-of-Flight [14] или на лазерной основе [15]. Большинство из них хороши для распознавания объектов, планирования пути и других задач. Однако в случае более сложных условий, таких как слабое освещение или резкое изменение ландшафта система зрения должна удовлетворять этим обстоятельствам. Рассматриваемый подход основан на лазерной системе технического зрения (СТЗ) [16] (рис. 1). Эта система по сравнению с другими имеет широкий угол обзора (до 160°) и идеально подходит для работы в совершенно темных условиях, что совершенно невозможно для систем с камерами.

В системе используется метод, называемый динамической триангуляцией [17] . Система рассчитывает декартовы координаты по двум обнаруженным углам B_{ij} и C_{ij} (в данном конкретном случае ij – шаги горизонтального и вертикального сканирования) лазера подсвеченной точки и фиксирует расстояние между проектором и приемником. В

полученном треугольнике (рис. 2) угол B_{ij} рассчитывается как простое соотношение двух счетчиков: количества тактовых импульсов между двумя исходными импульсами на интервале ‘home pulse – spot pulse’ (1).

$$B_{ij} = \frac{2\pi N_A}{N_{2\pi}}, \qquad (1)$$

где N_A – количество опорных импульсов, когда лазерные лучи обнаруживаются датчиком остановки, а $N_{2\pi}$ – количество тактовых опорных импульсов, когда зеркало в 45° завершает поворот на 360°, обнаруженный датчиком нуля.

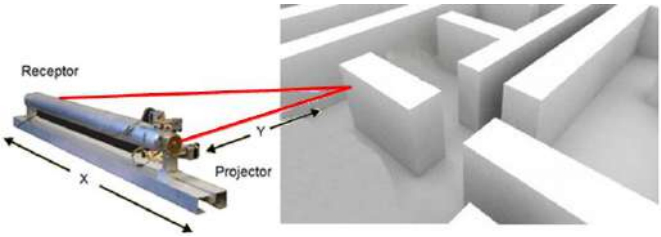


Рис. 1. Система технического зрения
Fig. 1. Technical Vision System

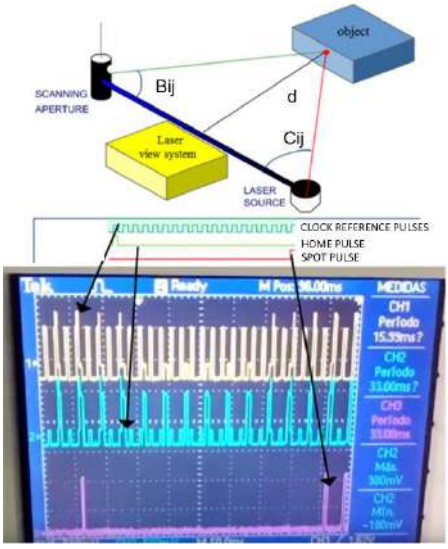


Рис. 2. Принцип динамической триангуляции СТЗ
Fig. 2. The principle of dynamic triangulation

Для вычисления координат *x*, *y* и *z* используются следующие уравнения (2-5):

$$x_{ij} = a\frac{\sin B_{ij} \cdot \sin C_{ij} \cdot \cos\sum_{j=1}^{j}\beta_j}{\sin\left[180° - \left(B_{ij} + C_{ij}\right)\right]} \qquad (2)$$

$$y_{ij} = a\left(\frac{1}{2} - \frac{\sin B_{ij} \cdot \sin C_{ij}}{\sin\left[180° - \left(B_{ij} + C_{ij}\right)\right]}\right) at\ B_{ij} \le 90° \qquad (3)$$

$$y_{ij} = -a\left(\frac{1}{2} - \frac{\sin B_{ij} \cdot \sin C_{ij}}{\sin\left[180° - \left(B_{ij} + C_{ij}\right)\right]}\right) at\ B_{ij} \ge 90° \qquad (4)$$

$$z_{ij} = a\frac{\sin B_{ij} \cdot \sin C_{ij} \cdot \cos\sum_{j=1}^{j}\beta_j}{\sin\left[180° - \left(B_{ij} + C_{ij}\right)\right]} \quad (5)$$

СТЗ может дать очень подробную информацию об обнаруженном препятствии. В задаче распознавания и классификации образов это можно рассматривается как выгоду. Но во время планирования движения робота, чтобы избежать столкновения, информация о препятствии должна содержать общие данные (ширина, глубина, высота и большие выпуклости его поверхности, которые могут препятствовать движению). Другими словами, препятствие для робота должно быть представлено в виде простой трехмерной фигуры с низким разрешением. Это делается путем вычисления эквивалентов углов раскрытия, на разных расстояниях сканирования, чтобы поддерживать одинаковое разрешение используемой изображения СТЗ.

Авторы в [18] рекомендует три различных угла 14.5636^o, 5.5455^o, 1.9091^o. Они представляют три типа разрешения, в виде лингвистических переменных: «Low», «Medium» и «High».

Поле зрения СТЗ может быть представлено в виде дуги. Разницу между горизонтальными шагами мы будем называть «Угол раскрытия», а радиус дуги – «Расстояние сканирования» (расстояние до обнаруженного объекта).

В соответствии с этими допущениями будут рассчитаны углы раскрытия, необходимые для достижения определенного разрешения (количества точек на дуге) для разных расстояний сканирования. Диапазон расстояний сканирования разделяется на три сектора: «Эффективный», когда роботу не нужно снижать свою скорость, чтобы избежать столкновения; «Оптимальный» реакция зависит от маневра, который необходимо выполнить; «Критический» робот должен замедляться или даже останавливаться.

Как видно, средний угол для «Critical» диапазона в конце расстояния даст низкое разрешение, которого недостаточно для обнаружения критических препятствий. В этом случае необходимо увеличить разрешение. Поэтому берется предельное значение угла для данного диапазона. Набор углов становится следующим: 5.209°, 2.474°, 1.247°.

С использованием полученных данных может быть выполнен набор правил для контроля скорости роботов и стабилизации разрешения во время движения (табл. 1).

Табл. 1. Правила разрешения и контроля скорости
Tab. 1. Rules for resolution and speed control

Расстояние сканирования (SD) (м)	Тип радиуса (лингвистическая переменная)	Углы раскрытия (Град.)	Разрешение (лингвистическая переменная)
SD ≤1	Critical	5.209	Low
1< SD ≤3	Optimal	2.474	Medium
3< SD ≤5	Effective	1.247	High

Использование представленных правил изменение углов раскрытия поможет сохранить условно равный уровень детализации препятствий в памяти одного робота. Кроме того, этот процесс дискретизации позволяет осуществлять обмен данными внутри группы для обновления общей базы знаний чаще, чем с необработанными данными из СТЗ. На этом этапе возникает необходимость формирования сети обмена данными для группы.

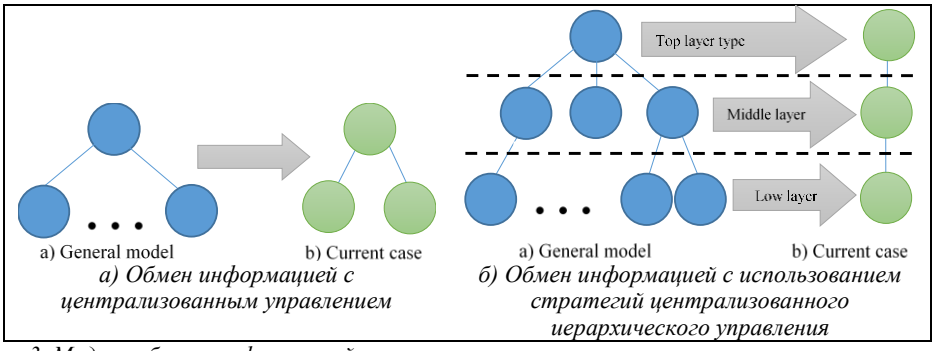
3. Динамические сети передачи данных

В статье будут рассмотрены две модели передачи данных: обмен информацией с централизованным управлением (рис. 3а) и стратегия централизованного иерархического управления (рис. 3б).

3.1 Формирование сети для роя роботов

Рассматривая общий случай роя, можно предложить метод формирования сети, основанный на создании связующего дерева. Алгоритм состоит из семи этапов и включает использование классических подходов:

1. построить полносвязную топологию сети;
2. используя алгоритм Крускала для построения минимального остовного дерева;
3. в полученном дереве используя алгоритм Флойда-Уоршелла, чтобы получить список всех возможных маршрутов в сети;
4. рассчитать среднюю длину маршрута для каждого узла;
5. выбрать узел с наименьшей средней длиной установить его как узел высокого уровня;
6. узлы с односторонним подключением устанавливаются как узлы низкого уровня;
7. другие узлы конфигурируются как узлы среднего уровня;



а) Обмен информацией с централизованным управлением

б) Обмен информацией с использованием стратегий централизованного иерархического управления

Рис. 3. Модели обмена информацией с централизованным и централизованным иерархическим решением для общего случая и группы из трех роботов

Fig. 3. Models of information exchange with a centralized and centralized hierarchical solution for the general case and a group of three robots

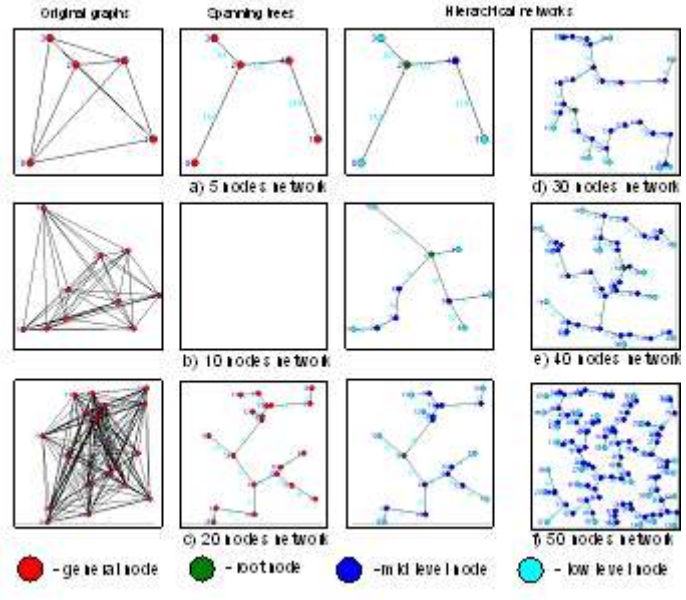


Рис. 4. Рассчитанные сети

Fig. 4. Calculated networks

Применяя этот метод, можно автоматически получить оба типа сетей (зависит от размещения роботов, их количества и качества сигнала сети). В частных случаях (рис. 4) в расчетах рассматривается открытое пространство без препятствий, поэтому использовались расстояния между узлами. В более сложных сценариях расстояния должны быть заменены уровнями сигнала беспроводной сети.

3.2 Метод формирования сети передачи данных на основе смены лидера

В соответствии со сложностью алгоритмов Крускала и Флойда-Варшалла в группе с небольшим количеством роботов более рационально использовать методологию распределения ролей. Именно поэтому будет рассмотрен метод распределения ролей, основанный на задаче выбора лидера.

Под термином «Лидер» мы будем понимать центральный узел обмена данными (робот на короткий срок станет точкой для хранения, слияния и оценки данных). Для выбора лидера роботы будут использовать процесс голосования.

Каждый робот может быть описан как набор параметров

$$R = (I, L, E, N), \qquad (6)$$

где I – идентификатор робота, L – идентификатор агента для голосования, E – оценка лидера L (количество голосов, которое необходимо отдать за лидера), N – список соединений, доступных для робота (его соседей).

Процесс голосования на начальном этапе проходит следующим образом: каждый робот оценивает своих соседей на роль лидера в соответствии с набором ранее определенных его характеристик; каждая из этих характеристик имеет свой вес; с помощью функции членства робот выбирает соседа с наибольшим значением.

Для значения голоса будет реализована лингвистическая переменная e = «оценка робота». Его значение основано на шкале M = {“very low”, “low”, “medium”, “high”, “very high”} или может иметь цифровой эквивалент M = {1, 2, 3, 4 , 5}. После процесса голосования будет создано много альтернатив для E, поэтому он будет иметь следующую форму:

$$E = \{e_1, e_2, \dots, e_n\}, \qquad (7)$$

где e_i – альтернативный «кандидат» ($i = 1..n$) и n это количество видимых соседей.

Оценка i-го соседа использует следующую формулу:

$$e_i = \sum_{j=1}^{k} w_j \, c_{ij} \qquad (8)$$

Робот оцениват всех своих видимых соседей по набору характеристик:

$$C_i = \{c_{i1}, c_{i2}, \dots, c_{ik}\}, \qquad (9)$$

где c_j – характерное значение i-го “кандидата” при $j = 1..k$.

Каждая из характеристик имеет свой вес:

$$W = \{w_1, w_2, \dots, w_k\}, \qquad (10)$$

где w_j – вес j-той характеристики, $\sum w_i = 1$.

Для определения значения лингвистической переменной мы используем три типа функций принадлежности, представленных на рис. 5.

Для получения результатов мы рассмотрим реализацию метода смены лидера в сети централизованного иерархического управления с пятью узлами (роботами). Первоначально

роботизированная группа работает на основе централизованной модели управления. На рис. 6 представлено общее количество запросов на обработку и количество запросов, которые были обработаны (показывает сумму от всех доступных роботов). Потеря данных и дубликаты запросов объясняют разницу между сериями графиков.

Потеря данных в таких задачах вызывает дополнительную нагрузку на модули планирования пути (неизвестные участки местности вызывают дополнительные пересчеты маршрута), что также увеличивает время, необходимое для решения основных задач (картирование местности, поиск объектов и т.д.). В соответствии с этим должны быть реализованы структурные изменения в сети передачи данных.

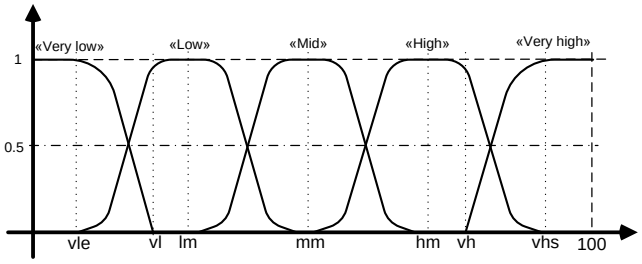


Рис. 5. Функции принадлежности
Fig. 5. Membership Functions

Внедрение системы смены лидеров позволяет роботам, потерявшим связь с центральным узлом, отправлять полученные данные с помощью соседей, компенсируя этим все потери (рис. 7).

На рис. 8 сравниваются обработанные запросы до и после использования системы смены лидеров. Представленные результаты нашего подхода помогают увидеть, что для каждого отдельного робота в группе общие данные (знания) становятся доступными более часто.

Рассмотрим влияние такого обмена данными и формирования общей базы знаний на группу роботов в трудно проходимой местности.

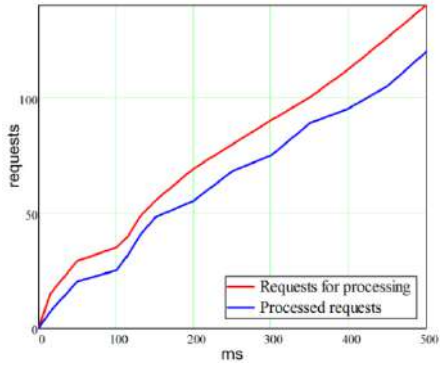


Рис. 6. Общий объем отправленных и обработанных запросов
Fig. 6. Total amount of sent and processed requests

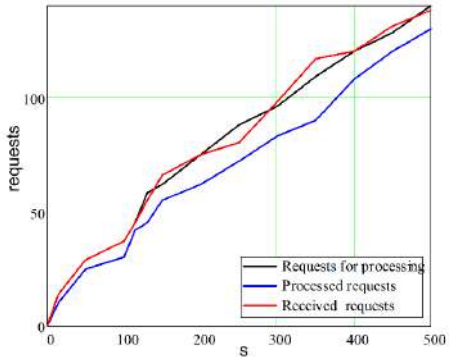


Рис. 7. Общий объем отправленных, полученных и обработанных запросов с потерей сигнала с использованием централизованного иерархического управления
Fig. 7. Total amount of sent, received and processed requests with signal loss using centralized hierarchical control

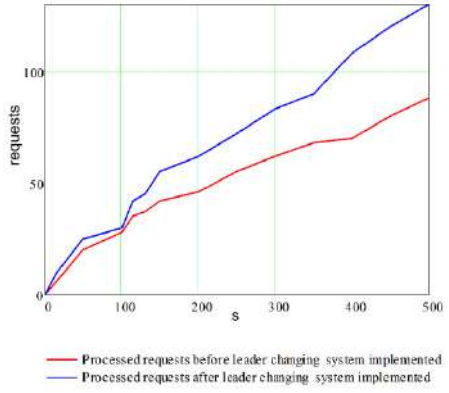


Рис. 8. Сравнение количества обработанных запросов до и после внедрения смены лидера
Fig. 8. Comparison of the number of processed requests before and after introducing a change of leader

4. Планирование маршрутов движения

Для формирования плавной траектории используются алгоритм A* и метод Безье на основе полигона из четырех точек ([18], [19], [20]). После каждого нового предупреждения СТЗ (обнаружение препятствий) текущий маршрут просчитывается заново.

Вышеупомянутый СТЗ представляет окружение в виде облака точек. Следовательно, для планирования пути можно разделить рельеф местности на небольшие участки (ячейки), чтобы уменьшить количество узлов, необходимых для более быстрого расчета бездействия (рис. 9).

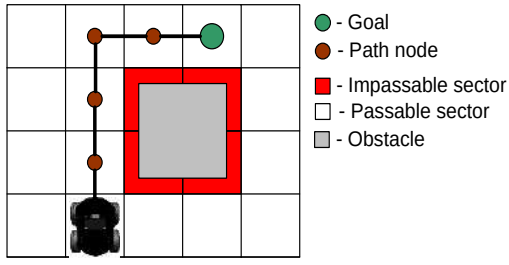


Рис. 9. Дискретизация окружающего пространства
Fig. 9. Discretization of the surrounding space

Экспериментальные результаты включают моделирование трех сцен (рис. 10). Каждая из них рассматривает группу из трех роботов (n = 3) с возможностью коммуникации и СТЗ. В экспериментах рассматривается следующий сценарий: для группы из трех роботов задана неизвестная местность, каждый из роботов имеет одинаковую общую цель для достижения и одну дополнительную (индивидуальную); роботы начинают двигаться к своим индивидуальным целям, после достижения роботы продолжают движение к общей цели; когда все роботы достигают общей цели, сценарий останавливается.

Рис. 10. Примеры использованных в моделировании сцен
Fig. 10. Examples of scenes used in modeling

Полученные результаты показаны на рис. 11 –13. На рисунках используется следующая маркировки WxGRx или WxSRx, здесь Wx – номеру сцены, G - для группового движения (с обменом знаниями), если S – движение без обмена данными, Rx – номер робота.

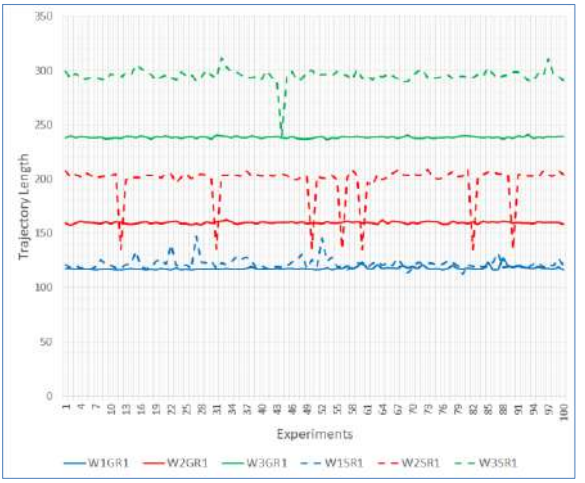


Fig. 11. Trajectories length for scene# 1
Рис. 11. Длина траекторий для сцены 1

Fig. 12. Trajectories length for scene# 2
Рис. 12. Длина траекторий для сцены 2

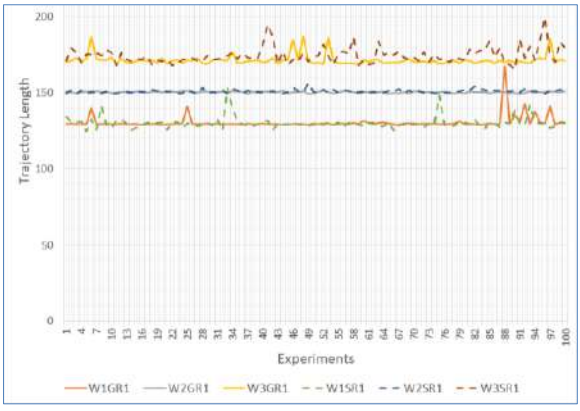


Fig. 13. Trajectories length for scene# 3
Рис. 13. Длина траекторий для сцены 3

В табл. 3 приведены результаты усредненных расстояний для каждого робота в случае обмена данных по сравнению с движением без обмена. В результате показано, что реализация планирования пути с помощью общей базы знаний может сократить маршрут роботов до 21,3%.

Табл. 3. Сравнение результатов планирования движения
Table 3. Motion planning comparing results

	Scene #1	Scene #2	Scene #3
Robot 1	0.035	0.213	0.19
Robot 2	0.002	0.0042	0.012
Robot 3	0.13	0.0025	0.018
Total	0.066	0.098	0.1

5. Заключение

Эта статья предлагает оригинальное решение, которое улучшает групповую маршрутизацию в неизвестной местности и взаимодействие между роботами в группе. Предложены модели формирования динамической сети передачи данных для роботизированного роя показывает улучшения в процессе обмена данными.

По результатам моделирования внедрение системы смены лидеров, основанной на процессе голосования и общей базе знаний, повышается эффективность планирования пути. Реализованный подход создает непрерывные траектории во время движения. Метод стабилизации разрешения дает дополнительную возможность настройки детализации в соответствии со спецификой среды или текущей задачей. Использование нечеткой логики в различных подзадачах делает поведение роботов более изменчивым и обеспечивает стабильное функционирование группы при меньших энергозатратах. Согласно полученным результатам, длина отдельных траекторий улучшилась до 21,3%.

Список литературы/References

[1] B. Eskridge, E. Valle, I. Schlupp. Emergence of Leadership within a Homogeneous Group. PLoS ONE, vol. 10, № 7, 2015

[2] V. Pshikhopov, M. Medvedev, A. Kolesnikov, R. Fedorenko, G. Boris. Decentralized Control of a Group of Homogeneous Vehicles in Obstructed Environment. Journal of Control Science and Engineering, 2016, 8 p.

[3] O. Sergiyenko, M. Ivanov, V. Tyrsa, M. Rivas-López, D. Hernández-Balbuena, W. Flores-Fuentes, J. C. Rodríguez-Quiñonez, J. I. Nieto-Hipólito, W. Hernandez, A. Tchernykh. Data transferring model determination in robotic group. Robotics and Autonomous Systems, vol. 83, 2016, pp. 251-260.

[4] O.Yu. Sergiyenko, M.V. Ivanov, V.M. Kartashov, V.V. Tyrsa, D. Hernández-Balbuena and J.I. Nieto-Hipólito. Transferring model in robotic group. In Proc. of the 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE), 2016, pp. 946-952.

[5] David J. Grymin, Charles B. Neas and Mazen Farhood. A hierarchical approach for primitive-based motion planning and control of autonomous vehicles. Robotics and Autonomous Systems, vol. 62, no. 2, 2014, pp. 214-228.

[6] Bence Kovács, Géza Szayer, Ferenc Tajti, Mauricio Burdelis, Péter Korondi. A novel potential field method for path planning of mobile robots by adapting animal motion attributes. Robotics and Autonomous Systems, vol. 82, 2016, pp. 24-34.

[7] V.A. Bobkov, Y.I. Ron'shin, A.P. Kudryashov, V.Y. Mashentsev. 3D SLAM from stereoimages. Programming and Computer Software, vol. 40, № 4, 2014, pp. 159-165.

[8] V.A. Bobkov, A.P. Kudryashov, S.V. Mel'man. On the Recovery of Motion of Dynamic Objects from Stereo Images. Programming and Computer Software, vol. 44, № 3, 2018, pp. 148-158.

[9] N. Kamaev, V.A. Sukhenko, D.A. Karmanov. Constructing and visualizing three-dimensional sea bottom models to test AUV machine vision systems. Programming and Computer Software, vol. 43, № 3, 2017, pp. 184-195.

[10] O. Vilão, D.H. Perico, I.J. Silva, T.P.D. Homem, F. Tonidandel, R.A.C. Bianchi. A Single Camera Vision System for a Humanoid Robot. In Proc. of the Joint Conference on Robotics: SBR-LARS Robotics Symposium and Robocontrol, vol. 1, 2014, pp. 181-186.

[11] N. Gryaznov и A. Lopota. Computer Vision for Mobile On-Ground Robotics. Procedia Engineering, vol. 100, 2015, pp. 1376-1380.

[12] M.C. Achtelik и D. Scaramuzza.Vision-Controlled Micro Flying Robots: From System Design to Autonomous Navigation and Mapping in GPS-Denied Environments. IEEE Robotics & Automation Magazine, vol. 21, № 3, 2014, pp. 26-40.

[13] N.F. Pashchenko, K.S. Zipa, A.V. Ignatenko. An algorithm for the visualization of stereo images simultaneously captured with different exposures. Programming and Computer Software, vol. 43, № 4, 2017, pp. 250-257.

[14] G. Alenyà Ribas, S. Foix Salmerón, C. Torras Genís.ToF cameras for active vision in robotics. Sensors and Actuators A: Physical, vol. 218, 2014, pp. 10-22.

[15] A. Mikhaylichenko и A.B. Kleshchenkov. Approach to Non-Contact Measurement of Geometric Parameters of Large-Sized Objects. Programming and Computer Software, vol. 44, № 4, 2018, pp. 271-277.

[16] L.C. Básaca-Preciado, O.Y. Sergiyenko, J.C. Rodríguez-Quinonez, X. García, V.V. Tyrsa, M. Rivas-Lopez, D. Hernandez-Balbuena, P. Mercorelli, M. Podrygalo, A. Gurko, I. Tabakova, O. Starostenko. Optical 3D laser measurement system for navigation of autonomous mobile robot. Optics and Lasers in Engineering, vol. 54, 2014, pp. 159-169.

[17] O. Sergiyenko, W. Hernandez, V. Tyrsa, L.D. Cruz, O. Starostenko, M. Pena-Cabrera. Remote Sensor for Spatial Measurements by Using Optical Scanning. Sensors (Basel), vol. 9, № 7, 2009, pp. 5477-5492.

[18] P.E. Bezier. How Renault Uses Numerical Control for Car Body Design and Tooling. Society of Automotive Engineers, Detroit, MI, USA, 1968.

[19] L. Han, H. Yashiro, T. Nejad, Q. Do, S. Mita. Bezier curve based path planning for autonomous vehicle in urban environment. In Proc. of the IEEE Intelligent Vehicles Symposium, 2010, pp. 1036-1042.

[20] Kuniaki Kawabata, Liang Ma, Jianru Xue, Chengwei Zhu, Nanning Zheng. A path generation for automated vehicle based on Bezier curve and via-points, Robotics and Autonomous Systems, vol. 74, № A, 2015, pp. 243-252.

[21] J. Hocking, Unity in Action: Multiplatform Game Development in C# with Unity 5. Shelter Island, New York, Manning Publications, 2015, 352 p.

[22] X. Garcia, O. Sergiyenko, V. Tyrsa, M. Rivas-Lopez, D. Hernandez-Balbuena, J. C. Rodriguez-Quiñonez, L. C. Basaca-Preciado, P. Mercorelli. Optimization of 3D laser scanning speed by use of combined variable step. Optics and Lasers in Engineering, vol. 54, 2014, pp. 141-151.

[23] R. Vincent, B. Morisset, A. Agno, M. Eriksen, C. Ortiz. Centibots: Large-scale autonomous robotic search and rescue experiment. In Proc. of the 2nd International Joint Topical Meeting on Emergency Preparedness & Response and Robotics & Remote Systems, 2008.

[24] Abduladhem A. Ali, Abdulmuttalib T. Rashid, Mattia Frasca, Luigi Fortuna. An algorithm for multi-robot collision-free navigation based on shortest distance. Robotics and Autonomous Systems, vol. 75, 2016, pp. 119-128.

[25] P. Muñoz, R.-M. D. María, D.F. Barrero. Unified framework for path-planning and task-planning for autonomous robots. Robotics and Autonomous Systems, vol. 82, 2016, pp. 1-14.

[26] V. Trianni, E. Tuci, C. Ampatzis, M. Dorigo. Evolutionary swarm robotics: A theoretical and methodological itinerary from individual neuro-controllers to collective behaviors. In The horizons of evolutionary robotics, Cambridge [MA], MIT Press, 2014, pp. 153–178.

Информация об авторах / Information about authors

Михаил Валерьевич ИВАНОВ получил степень магистра в 2012 г. в Национальном аэрокосмическом университете им. Н. Е. Жуковского «Харьковский Авиационный Институт», Харьков, Украина. В настоящее время работает исследователем в Инженерном институте Автономного университета Нижней Калифорнии, Мексика. В число научных интересов входят робототехника, лазерные системы технического зрения, навигационные системы, модели передачи данных, динамически образуемые сети.

Mikhail Valerievitch IVANOV received the M.S. degree in Kharkov National Aerospace University «KhAI», Kharkiv, Ukraine, in 2012. Currently he is a researcher in the Institute of Engineering of the Autonomous University of Baja California, Mexico. His research interests include robotics, laser technical vision systems, navigation systems, data transferring models, dynamical network forming.

Олег Юрьевич СЕРГИЕНКО защитил кандидатскую диссертацию в 1997 г. в Национальном техническом университете «Харьковский политехнический институт», Украина. В настоящее время возглавляет отдел прикладной физики в Инженерном институте Автономного университета Нижней Калифорнии, Мексика. Научные интересы включают автоматизированную метрологию, интеллектуальные сенсоры, управляющие системы, навигацию роботов и трехмерные лазерные сканеры.

Oleg Yurievitch SERGIYENKO received the Ph.D. degree in Kharkiv National Technical University in 1997. He is currently Head of Applied Physics Department of Engineering Institute of Baja California Autonomous University, Mexico. His current research interests include automated metrology & smart sensors, control systems, robot navigation, измерение трехмерных координат.

Вера Валентиновна ТЫРСА защитила кандидатскую диссертацию в 1996 г. в Национальном техническом университете «Харьковский политехнический институт», Украина. В настоящее время работает на Инженерном факультете Автономного университета Нижней Калифорнии, Мексика. Научные интересы: автоматизированная метрология, системы машинного зрения, быстрые электрические измерения, управляющие системы, навигация роботов и трехмерные лазерные сканеры.

Vera Valentinovna TYRSA received the Ph.D. degree in Kharkiv National Polytechnic University in 1996. Currently she is working at the Engineering Faculty of the Baja California Autonomous University, Mexico. Her current research interests include automated metrology, machine vision systems, fast electrical measurements, control systems, robot navigation, and 3D laser scanners.

Ларс ЛИНДНЕР получил степень магистра в Дрезденском техническом университете, Германия в 2009 г., а степень доктора философии – в Инженерном институте Автономного университета Нижней Калифорнии, Мексика в 2017 г. С 2009 г. преподает на Инженерном факультете Автономного университета Нижней Калифорнии. Основные научные интересы – управляющие системы и компьютерная оптика.

Lars LINDNER received his master's degree from the Technical University of Dresden in January 2009, and degree of PhD from the Institute of Engineering of the Baja California Autonomous University, Mexico. He currently teaches at the Faculty of Engineering of the Autonomous University of Baja California Mexicali campus. Main research interests include control systems and computer optics.

Хулио Сезар РОДРИГЕС-КИНЬОНЕС получил степень PhD в Автономном университете Нижней Калифорнии, Мексика в 2013 г. В настоящее время он работает профессором на Инженерном факультете Автономного университета Нижней Калифорнии. В число его текущих научных интересов входят автоматизированная метрология, системы стереозрения, управляющие системы, навигация роботов и трехмерные лазерные сканеры.

Julio Cesar RODRÍGUEZ-QUIÑONEZ received the Ph.D. degree from Baja California Autonomous University, México, in 2013. He is currently Professor of Electronic Topics with the Engineering Faculty, Autonomous University of Baja California. His current research interests include automated metrology, stereo vision systems, control systems, robot navigation, and 3D laser scanners.

Венди ФЛОРЕС-ФУЭНТЕС получила получил степень PhD в Автономном университете Нижней Калифорнии, Мексика в 2014 г. В настоящее время она является профессором-исследователем на Инженерном факультете Автономного университета Нижней Калифорнии. Научные интересы: робототехника, машинное зрение, навигация, управляющие системы.

Wendy FLORES-FUENTES received the Ph.D. degree from Autonomous University of Baja California in June 2014. Currently, she is a full-time professor-researcher at Universidad Autónoma de Baja California, at the Faculty of Engineering. Her research interests include robotics, machine vision, navigation, control systems.

Мойзес РИВАС-ЛОПЕС получил степень PhD в Автономном университете Нижней Калифорнии, Мексика в 2010 г. В настоящее время работает в отделе прикладной физики Инженерного института Автономного университета Нижней Калифорнии.

Moises RIVAS-LOPEZ received the Ph.D. degree from Autonomous University of Baja California in 2010. He is currently a Full Researcher with the Applied Physics Department, Engineering Institute, Baja California Autonomous University, Mexico.

Даниэль ЭРНАНДЕС-БАЛЬБУЭНА получил степень PhD в Автономном университете Нижней Калифорнии, Мексика в 2007 г. В настоящее время он является профессором Инженерного факультета Автономного университета Нижней Калифорнии. Его научные интересы связаны с метрологией времени и частоты и радиочастотными измерениями.

Daniel HERNÁNDEZ-BALBUENA received the Ph.D. degree from Autonomous University of Baja California in 2007. He is currently a Full Professor at the Engineering Faculty of Baja California Autonomous University, Mexico. His research interests are in the areas of time and frequency metrology and RF measurements.

Хуан Иван НЬЕТО ИПОЛИТО получил степень PhD в Политехническом университете Каталонии, Испания в 2005 г. В настоящее время он является профессором Автономного университета Нижней Калифорнии. Его научные интересы затрагивают компьютерную инженерию, компьютерные сети, мобильные вычисления.

Juan Iván NIETO HIPÓLITO received the Ph.D degree from Polytechnic University of Catalonia,Spain. He is currently a Full Professor of Baja California Autonomous University, Mexico. His research interests are in the areas computer engineering, computer networks, mobile computing.

DOI: 10.15514/ISPRAS-2019-31(2)-7

Непрерывная интеграция функционального наполнения распределенных пакетов прикладных программ в Orlando Tools

А.Г. Феоктистов, ORCID: 0000-0002-9127-6162 <agf65@icc.ru>
С.А. Горский, ORCID: 0000-0003-0177-9741 <gorsky@icc.ru>
И.А. Сидоров, ORCID: 0000-0002-2398-5426 <ivan.sidorov@icc.ru>
Р.О. Костромин, ORCID: 0000-0001-8406-8106 <kostromin@icc.ru>
Е.С. Фереферов, ORCID: 0000-0002-7316-444X <fereferov@icc.ru>
И.В. Бычков, Scopus ID: 56308077400 <bychkov@icc.ru>

Институт динамики систем и теории управления им. В.М. Матросова СО РАН, 663033, Россия, г. Иркутск, ул. Лермонтова, д. 134

Аннотация. В статье представлен новый подход к решению важных практических проблем комплексной отладки, совместного тестирования и анализа времени выполнения версий программных модулей в распределенной вычислительной среде. Эти проблемы возникают в процессе поддержки непрерывной интеграции функционального наполнения (прикладного программного обеспечения) распределенных пакетов прикладных программ (научных приложений). Исследование ориентировано на пакеты, которые используются для проведения крупномасштабных экспериментов, осуществляемых в рамках междисциплинарных исследований, в гетерогенных распределенных вычислительных средах, интегрирующих Grid и облачные вычисления. Научная новизна предложенного подхода заключается в объединении методологии создания распределенных пакетов прикладных программ с современной практикой разработки программного обеспечения на основе его непрерывной интеграции с использованием знаний о специфике решаемых задач. Средства непрерывной интеграции, разрабатываемые в рамках предложенного подхода, существенно расширяют спектр ее возможностей применительно к процессам создания и использования таких пакетов в сравнении с известными инструментами. Фундаментальной основой их функционирования является концептуальная модель, в рамках которой осуществляется спецификация, планирование и выполнение процессов непрерывной интеграции прикладного программного обеспечения с привязкой к конкретным предметным данным и решаемым задачам. Использование разрабатываемых средств на практике ведет к снижению числа ошибок и сбоев прикладного программного обеспечения при разработке и применении пакетов, что, в свою очередь, существенно сокращает время проведения крупномасштабных вычислительных экспериментов и повышает эффективность использования ресурсов гетерогенной распределенной вычислительной среды. Результаты практических экспериментов по применению прототипа системы непрерывной интеграции прикладного программного обеспечения показывают его высокую эффективность.

Ключевые слова: распределенная вычислительная среда; пакеты прикладных программ; программное обеспечение; непрерывная интеграция

Для цитирования: Феоктистов А.Г., Горский С.А., Сидоров И.А., Костромин Р.О., Фереферов Е.С., Бычков И.В. Непрерывная интеграция функционального наполнения распределенных пакетов прикладных программ. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 83-96. DOI: 10.15514/ISPRAS-2019-31(2)-7

Благодарности. Исследования выполнены при поддержке РФФИ, проект № 19-07-00097-а.

Continuous integrating modules of distributed applied software packages in Orlando Tools

A.G. Feoktistov, ORCID: 0000-0002-9127-6162 <agf@icc.ru>
S.A. Gorsky, ORCID: 0000-0003-0177-9741 <gorsky@icc.ru>
I.A. Sidorov, ORCID: 0000-0002-2398-5426 <ivan.sidorov@icc.ru>
R.O. Kostromin, ORCID: 0000-0001-8406-8106 <kostromin@icc.ru>
E.S. Fereferov, ORCID: 0000-0002-7316-444X <fereferov@icc.ru>
I.V. Bychkov, Scopus ID: 56308077400 <bychkov@icc.ru>
Matrosov Institute for System Dynamics and Control Theory of SB RAS,
134, Lermontov st., Irkutsk, 664033, Russia.

Abstract. We propose a new approach to solving important practical problems of complex debugging, joint testing, and analysis of the execution time of software module versions in a heterogeneous distributed computing environment that integrating Grid and cloud computing. These problems arise in the process of supporting the continuous integration of modules of distributed applied software packages. The study focuses on the packages that are used to conduct large-scale computational experiments. The scientific novelty of the proposed approach is to combine the methodology for creating the packages with modern software development practices based on its continuous integration using knowledge about the specifics of the problems being solved. Our contribution is multifold. We expanded the capabilities of continuous integration tools by developing new additional tools for the markup and transformation of data from poorly structured sources and predicting modules execution time. In addition, we developed a technological scheme of the joint applying our developed tools and external systems for continuous integration. Therefore, we provide a more large range of capabilities of continuous integration in relation to the processes of creating and using the packages in comparison with the well-known tools. The fundamental basis of their functioning is a new conceptual model of the packages. This model supports the specification, planning, and execution of software continuous integration processes taking into account the specific subject data and problems being solved. Applying the developed tools in practice leads to a decrease in the number of errors and failures of applied software in the development and use of the packages. In turn, such decrease significantly reduces the time for large-scale computational experiments and increases the efficiency of using resources of the environment. The results of practical experiments on the use of system prototype for continuous integration of applied software show their high efficiency.

Keywords: distributed computing environment; applied software packages; software; continuous integration

For citation: Feoktistov A.G., Gorsky S.A., Sidorov I.A., Kostromin R.O., Fereferov E.S., Bychkov I.V. Continuous integrating modules of distributed applied software packages in Orlando Tools. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 83-96 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-7

Acknowlwdgement. The studies were supported by the Russian Foundation for Basic Research, project No. 19-07-00097-a.

1. Введение

В настоящее время применение высокопроизводительных вычислений стало неотъемлемой составляющей процесса поддержки проведения крупномасштабных экспериментов по решению больших научных и прикладных задач в различных сферах человеческой деятельности. В зависимости от масштабности решаемых задач в вычислительную инфраструктуру могут быть включены персональные компьютеры (ПК), серверы, кластеры, ресурсы центров коллективного пользования, Grid-системы и облачные платформы. В общем случае, организуется гетерогенная распределенная вычислительная среда (ГРВС), в которой выполняются приложения, характеризующиеся разной степенью масштабируемости вычислений, чувствительности к неоднородности ресурсов, потребности в виртуализации ресурсов среды, а также необходимости интеграции модели своей предметной области с информацией о программно-аппаратной инфраструктуре среды и административных политиках, определенных для ее ресурсов. Приложения, чувствительные

к неоднородности ресурсов, выполняются, как правило, в однородных узлах кластера или в виртуальной среде. Потребность в ней возникает также и у приложений, использующих программное обеспечение (ПО), отличное от установленного в узлах среды. Применение высокопроизводительных вычислений связано с отображением алгоритмов решения задач на архитектуру вычислительной среды [1, 2].

Можно выделить отдельный класс приложений – распределенные пакеты прикладных программ (РППП), которые характеризуются применением модульного подхода, высокой степенью масштабируемости и возможностью их выполнения на разнородных ресурсах среды. Пользователи РППП заинтересованы в максимальном использовании вычислительных мощностей ГРВС. В модели предметной области РППП вычислительный процесс представляется в виде схемы решения задачи, которая тесно коррелирует с понятием рабочего процесса (workflow). Системы разработки и применения workflow можно рассматривать как частный случай РППП.

Как правило, ГРВС характеризуется постоянным изменением своих программно-аппаратных и информационных ресурсов. Это влечет за собой необходимость решения проблем реконфигурации вычислительных сред РППП, модификации их библиотек программных модулей и/или разработки нового ПО, поддержки корректности взаимодействия различных версий программных модулей в рамках единой схемы решения задачи, учета условий применения этих версий, комплексирования изменяющихся источников предметной информации со структурами данных РППП, прогнозирования времени выполнения модулей разных версий с целью оптимизации показателей функционирования выделяемых им ресурсов и эффективности решения задач. Для решения вышеперечисленных проблем могут быть использованы в той или иной мере средства непрерывной интеграции ПО.

Однако поддержка такой интеграции по-прежнему является нетривиальной проблемой для инструментальных средств организации РППП, включая системы создания и применения workflow [3]. Данные средства зачастую не готовы в полной мере поддерживать сложный процесс непрерывной интеграции в сочетании с концептуальным моделированием, традиционно применяемым в таких пакетах, а также использованием предметно-ориентированных знаний в сочетании со специализированными знаниями о программно-аппаратной инфраструктуре среды и административных политиках, установленных в ее узлах.

В этой связи в статье предложен новый подход к обеспечению непрерывной интеграции функционального наполнения РППП, базирующийся на слиянии методологии построения таких пакетов с современной практикой разработки ПО на основе его непрерывной интеграции с использованием предметно-ориентированных знаний. В рамках этого подхода расширены возможности средств непрерывной интеграции за счет разработки новых дополнительных инструментов для разметки и преобразования данных из слабоструктурированных источников, а также прогнозирования времени выполнения модулей РППП. Разработана технологическая схема совместного использования разработанных инструментов и внешних систем для непрерывной интеграции.

Оставшаяся часть статьи структурирована следующим образом: во втором разделе статьи приведен краткий обзор средств и обсужден ряд важных проблем непрерывной интеграции ПО. В третьем разделе рассмотрены вопросы, связанные с разработкой РППП в Orlando Tools. В четвертом разделе предложена технологическая схема непрерывной интеграции функционального наполнения пакетов. В следующих двух разделах особое внимание уделено используемому подходу к разметке и трансформации данных из слабоструктурированных источников, а также разработанной модели оценки времени выполнения модулей. Результаты практического применения разработанного прототипа подсистемы непрерывной интеграции в Orlando Tools приведены в седьмом разделе. Заключительный раздел обобщает результаты исследования.

2. Обзор средств непрерывной интеграции программного обеспечения

В процессе разработки сложных программных комплексов перед их разработчиками возникает необходимость организации взаимодействия между функциональными подсистемами таких комплексов. Подсистемы могут создаваться различными разработчиками с использованием широкого спектра языков программирования и в ориентации на функционирование под управлением разнообразных программно-аппаратных платформ. Основным назначением непрерывной интеграции является выявление и устранение проблем взаимодействия отдельных подсистем программного комплекса между собой путем автоматизации их сборки, отладки и совместного тестирования [4].

На сегодняшний день разработан широкий набор средств, обеспечивающих автоматизацию процессов непрерывной интеграции в ходе разработки сложных программных комплексов. В их числе системы CircleCI [5], Jenkins [6], TeamCity [7], Travis [8], GitLab [9] и многие другие средства [10, 11]. Каждая система имеет свои специфические особенности с точки зрения обеспечения функциональных возможностей, последовательности выполнения действий пользователями данной системы и ее администрирования. Все они обладают определенными преимуществами и недостатками.

Некоторые их них (например, CruiseControl.NET [12] или Apache Gump [13]) жестко привязаны к языку программирования, на котором осуществляется разработка ПО, с целью максимального использования возможностей данного языка в связке со специализированными средствами управления библиотеками программ. В качестве примера такого средства можно привести систему Conan [14] для языка C++. Другие средства предоставляют доступ только в режиме работы облачного сервиса (например, CircleCI или TeamCity) и не позволяют разместить весь необходимый набор средств непрерывной интеграции на своих ресурсах. Возникают определенные сложности с интеграцией таких средств, как BuildMaster [15] и Travis [16], со средами разработки из-за использования разных форматов представления данных и рабочих процессов.

Как показывает сравнительный анализ средств непрерывной интеграции, GitLab является одной из наиболее перспективных систем подобного назначения. Она обеспечивает тесную интеграцию процессов автоматического тестирования ПО и хранения его исходного кода с помощью репозитория Git [17], а также запуск тестов на серверах сборки программного обеспечения с применением таких средств, как сетевой протокол безопасного доступа SSH [18], скрипты на языке программирования Shell [19], программный комплекс VirtualBox [20] для виртуализации различных операционных систем (Microsoft Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других систем), программные продукты виртуализации компании Parallels [21], программные комплексы для автоматизации развертывания и управления приложениями в среде виртуализации Docker [22] и Kubernetes [23]. Возможность установки GitLab разработчиком ПО на собственных вычислительных ресурсах позволяет обеспечить необходимый уровень безопасности и гибкости всей системы непрерывной интеграции в целом. В табл. 1 приведен сравнительный анализ обеспечения важных функциональных возможностей наиболее популярными средствами непрерывной интеграции.

Табл.1. Результаты сравнительного анализа
Table 1. Results of the comparative analysis

Функциональная возможность	Travis CI	TeamCity	Jenkins	CircleCI	GitLab
Установка системы на ресурсах разработчика	–	+	+	–	+
Поддержка тестирования ПО для ОС Linux	+	+	+	+	+

Поддержка тестирования ПО для ОС Windows	–	+	+	–	+
Мониторинг ПО	–	–	–	–	+
Наличие репозитория образов контейнеров	–	–	–	–	+
Проверка качества программного кода	–	–	+	–	+

Информация, извлекаемая из источников предметных данных (например, веб-страниц [24]), и результаты решения задач, получаемые в результате выполнения РППП, зачастую являются сложно структурированными, неоднородными и подверженными частым изменениям. В этой связи в процессе непрерывной интеграции требуется применение гибкой, основанной на знаниях модели, позволяющей определять взаимосвязи между первичной информацией и структурами данных, используемыми такими пакетами. Известные средства непрерывной интеграции не поддерживают такой возможности.

Отладка и тестирование ПО на разных программно-аппаратных платформах потенциально позволяют в то же время выполнять и оценку времени выполнения этого ПО с учетом различий характеристик используемых ресурсов. Для решения этой задачи (нетривиальной для существующих средств непрерывной интеграции) необходима разработка новых методов и средств прогнозирования времени выполнения программ.

3. Orlando Tools: разработка и применение распределенных пакетов прикладных программ

Разработка приложений для проведения научных и прикладных исследований осуществляется с помощью инструментального комплекса Orlando Tools [24]. Этот комплекс обеспечивает построение предметно-ориентированных вычислительных сред, в которых интегрируются различные вычислительные инфраструктуры, поддерживающие, как Grid, так и облачные вычисления.

В описании модели предметной области РППП выделяются три концептуально обособленных слоя знаний – вычислительный, схемный и продукционный, над которыми формируются постановки задач и строятся схемы их решения. Вычислительный слой знаний реализуется программными модулями пакета, которые представляют его функциональное наполнение. Параметры и операции пакета отражают схемные знания. Параметры отражают значимые характеристики и свойства предметной области. Операции выступают в качестве отношений вычислимости между двумя подмножествами параметров предметной области. Такое отношение обуславливает возможность вычисления искомых значений параметров первого подмножества, когда известны значения параметров второго подмножества. Модули пакета представляют собой программную реализацию операций. Спецификация каждого модуля включает информацию об исполняемой прикладной программе (наименовании, версии, входных и выходных параметрах, процессах сборки и компиляции, инструкциях по запуску, допустимых классах ресурсов для выполнения). Возможность выполнения операций в процессе решения задачи в зависимости от текущего хода вычислений и состояния ресурсов ГРВС определяется продукциями, которые формируют продукционный слой знаний.

На вычислительной модели пакета формулируются постановки задач (формализованные описания условий задач в терминах параметров и операций). В общем случае постановка задачи определяет:

- входные параметры (данные, необходимые для решения задачи);
- выходные параметры (результаты решения задачи);
- операции, которые могут или должны быть выполнены в процессе решения задачи над полем параметров;

- ограничения, определяющие возможность выполнения операций.

По сформулированной постановке задачи строится ее схема решения, отражающая информационно-логические связи между операциями пакета.

4. Общая схема непрерывной интеграции

Архитектура Orlando Tools [25] расширена функционирующим прототипом системы непрерывной интеграции. Общая схема взаимодействия Orlando Tools с подсистемами непрерывной интеграции приведена на рис. 1. Запуск процессов непрерывной интеграции осуществляется на следующих четырех этапах, связанных с разработкой РППП:

- внесение изменений в исходный код модулей;
- добавление новой версии модуля;
- создание новых образов виртуальных машин для выполнения модулей;
- разработка новых спецификаций баз данных.

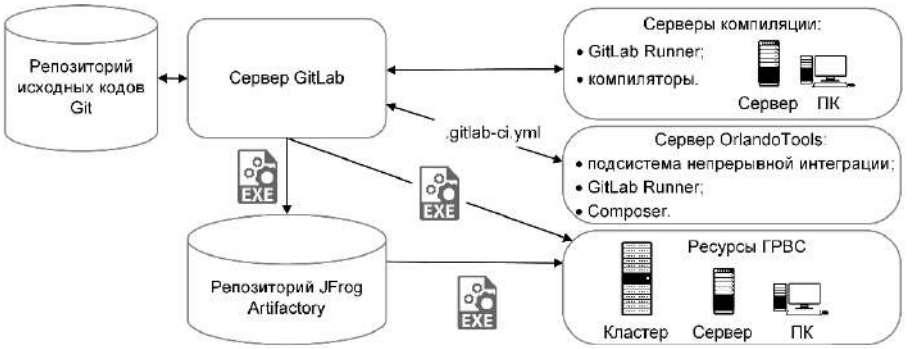


Рис. 1. Схема поддержки непрерывной интеграции
Fig. 1. Scheme of supporting the continuous integration

В Orlando Tools в качестве системы управления версиями исходного кода модулей используется репозиторий Git, доступ к которому обеспечивается средой GitLab. При внесении в эту систему изменений, связанных с разработкой нового или модификацией уже существующего ПО, автоматически осуществляется его компиляция на специализированных серверах или узлах ГРВС с помощью предустановленного агента Gitlab Runner.

В случае успешной компиляции, осуществляется тестирование модуля. Тестовые данные должны быть подобраны разработчиком пакета таким образом, чтобы время тестирования не превышало предельных значений (по умолчанию до 1 минуты), установленных администратором ГРВС. Тестирование модуля также осуществляется с помощью GitLab Runner.

Второй этап связан с добавлением новой версии модуля в РППП. В случае ее успешного тестирования на предыдущем этапе статус модуля помечается как «стабильный» и его бинарная версия добавляется в репозиторий JFrog Artifactory [26]. Данный репозиторий служит в качестве хранилища бинарных версий модулей и предоставляет интерфейсы для взаимодействия с различными пакетными менеджерами (например, Advanced Packaging Tool [27] или Yum Package Manager [28]). При включении новой версии модуля в репозиторий осуществляется автоматический запуск тестирования схем решения задач, операции которых реализуются данным модулем.

Создание новых образов виртуальных машин, с помощью которых в дальнейшем будут выполняться модули в узлах ГРВС, осуществляется в рамках третьего этапа. В случае добавления нового образа виртуальной машины с характеристиками, совпадающими с характеристиками требований к среде выполнения в спецификациях стабильных модулей,

производится запуск таких модулей для тестирования их корректного выполнения в новом образе виртуальной машины.

Последний этап связан с подготовкой спецификаций предметных баз данных для модулей, которые характеризуются обработкой больших объемов данных (BigData), которые не могут быть переданы в виде файлов для входных и выходных параметров этих модулей в узел ГРВС. Организация передачи и обработки таких объемов данных требует использования дополнительных предметных баз данных и веб-сервисов, предоставляющих возможности выборки данных по определенным критериям. В Orlando Tools такие базы данных специфицируются в формате JSON. В случае разработки новой спецификации предметной базы данных осуществляется запуск модулей, использующих эти базы, с целью тестирования процессов обмена данными.

5. Инструментальное средство разметки и трансформации данных из слабоструктурированных источников

Необходимость получения значений предметных данных, содержащихся в слабоструктурированных источниках (базах данных или отдельных файлах разных форматов, созданных ранее субъектами различных видов деятельности в рамках предметной области и содержащих результаты экспериментов или статистические показатели) часто возникает в процессе создания и применения РППП. Такие данные требуются для задания исходных параметров задач пакета. В связи с этим, его разработчики вынуждены осуществлять нетривиальное преобразование извлекаемых предметных данных к определенной форме их представления в пакете.

Рис. 2. Схема работы средства разметки и трансформации данных из слабоструктурированных источников

Fig. 2. Tool operation scheme of the markup and transformation of data from semi-structured sources

В системе непрерывной интеграции разработана схема разметки и трансформации данных из слабоструктурированных источников в виде файлов электронных таблиц (CSV, MS Excel) к структурированной форме представления значений параметров РППП в виде баз данных или XML-, JSON- файлов. В рамках данной схемы разработчику пакета предоставляется возможность визуальной настройки и спецификации процесса трансформации данных, необходимых для решения задач конкретного класса. На этапе разметки разработчик формирует дерево сущностей, указывая в каких диапазонах слабоструктурированных документов эти сущности находятся. Отдельным атрибутам могут быть заданы правила трансформации, например, разделение на несколько атрибутов или удаление частей значений. Дерево сущностей может быть дополнено классами для обеспечения формирования сложных целевых структур. Знания разработчика о разметке и правилах трансформации сохраняются в виде структурной спецификации, которые могут

быть применены многократно при решении типовых задач извлечения и трансформации данных (например, по использованию статистической информации за разные периоды). Кроме того, сформированные структурные спецификации могут быть использованы для автоматизации создания прикладных программных систем для работы с данными целевых структур. Общая схема разметки и трансформации представлена на рис. 2.

6. Оценка времени выполнения модулей

Разработана специальная модель оценки времени выполнения модулей схемы решения задачи. Модуль в процессе его тестирования запускается на эталонном узле в программной среде для профилирования программ. В процессе выполнения модуля определяются его временные затраты на работу с различными компонентами узла с учетом его вычислительных характеристик. Путем сравнения характеристик эталонного и целевого узлов прогнозируется время выполнения модуля на целевом узле с некоторой погрешностью.

В рамках разработанной модели формируются наборы $CR = \{cr_1, cr_2, \dots, cr_m\}$ и $CT = \{ct_1, ct_2, \dots, ct_m\}$ характеристик эталонного и целевого узлов и определяются их значения. Между cr_i и ct_i устанавливается взаимно однозначное соответствие, $i = \overline{1,m}$. Затем формируется множество $P = \{p_1(d), p_2(d), \dots, p_n(d)\}$. Элемент $p_j(d)$, $j = \overline{1,n}$ отражает вычислительную нагрузку узла при выполнении модуля (число выполненных целочисленных операций, число операций с плавающей точкой, число обращений к оперативной памяти и кэш-памяти разных уровней, число промахов таких обращений, число сессий чтения с диска и записи на диск и другие показатели) в зависимости от объема d обрабатываемых данных этим модулем. Далее определяются функции $f_l(CR, P)$, вычисляющие время работы l-го компонента узла при обработке вычислительной нагрузки, $l = \overline{1,k}$. Время выполнения модуля в эталонном узле оценивается выражением

$$\hat{T}_r(d) = \sum_{l=1}^{k} f_l\big(CR, P, g(d)\big),$$

где $g(d)$ – это интерполяционная функция, определяющая зависимость от объема данных d экспериментальным путем. Погрешность ε данной оценки определяется из разности реального времени $T_r(d)$ выполнения модуля и $\hat{T}_r(d)$:

$$\varepsilon = T_r(d) - \hat{T}_r(d).$$

Время $\hat{T}'_t(x)$ выполнения модуля в целевом узле оценивается выражением

$$\hat{T}'_t(x) = \hat{T}_t(d) + \varepsilon \frac{\hat{T}_r(d)}{\hat{T}_t(d)}, \hat{T}_t(d) = \sum_{l=1}^{k} f_l\big(CT, P, g(d)\big).$$

Оценка времени выполнения модуля, получаемая с помощью предложенной модели, является достаточно грубой. Кроме того, автоматический выбор интерполяционной функции $g(d)$ для некоторых классов модулей является трудно реализуемым. Тем не менее, как показано в следующем разделе, такая оценка позволяет в ряде случаев существенно улучшить пользовательские оценки, а также оценки, определяемые на основе вычислительной истории.

7. Применение непрерывной интеграции в Orlando Tools

В качестве примера применения непрерывной интеграции рассматривается разработка модулей РППП, предназначенного для тестирования модификаций алгоритма мультистарта на задачах поиска глобального минимума многоэкстремальных функций. Модель схемы решения подобных задач приведена на рис. 3, где $z_1 - z_{13}$ и $o_1 - o_4$ – это соответственно параметры и операции вычислительной модели. Назначение параметров и операций, а также особенности процесса решения задач детально рассмотрены в [29]. В данной модели схемы z_9 является составным параметром, а z_3 и z_{12} представляют параллельные списки данных, элементы которых обрабатываются q экземплярами операции o_3. В пакете

разработан набор модулей, реализующих операции $o_1 - o_4$ и представляющих этапы тестируемых модификаций алгоритма применительно к различным многоэкстремальным функциям. Процесс решения таких задач требует многократного обновления модулей.

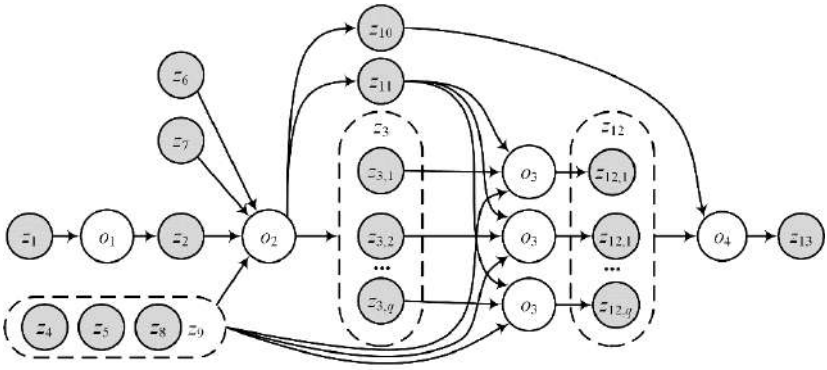


Рис. 3. Модель схемы решения задачи
Fig. 3. Problem-solving scheme model

Спецификация объектов вычислительной модели. На рис. 4 приведены спецификации основных объектов вычислительной модели в Orlando Tools, используемые в процессе тестирования модулей.

```
<module>
  <name>Имя_модуля</name>
  <parameters>Входные_параметры>
              Выходные_параметры
  </parameters>
  <signature>Команда_запуска
  </signature>
  <cores>Число_ядер</cores>
  <walltime>Время_останова</walltime>
  <run_mode>Режим_запуска</run_mode>
  <repository>описание_модуля
  </repository>
</module>
```

a)

```
<operation>
  <name>Имя_операции</name>
  <parameters>Входные_параметры>
              Выходные_параметры
  </parameters>
  <run_condition>Условие_запуска
  </run_condition>
  <while_flag>Признак_повторения
  </while_flag>
  <module_name>Имя_модуля</module_name>
  <split_condition>Условие_расщепления
  </split_condition>
  <task_name>Имя_задачи</task_name>
</operation>
```

b)

```
<parameter>
  <name>Имя_параметра</name>
  <extention>Расширение</extention>
  <list>Число_элементов</list>
</parameter>
```

c)

```
<task>
  <name>Имя задачи</name>
  <parametrs>Входные_параметры>
             Выходные_параметры</parametrs>
  <operations>Список_операций</operations>
  <modules>Список_версий_модулей</modules>
  <test>описание_данных</test>
</task>
```

d)

Рис. 4. Спецификации объектов вычислительной модели: модуль (a), операция (b), параметр (c) и схема решения задачи (d)
Fig. 4. Object specifications in the computational model: module (a), operation (b), parameter (c), and problem-solving scheme (d)

Новые элементы спецификации, необходимые для поддержки процесса непрерывной интеграции, выделены полужирным шрифтом. В спецификации модуля элемент <repository> содержит информацию о размещении этого модуля в репозитории и его зависимости от других модулей. Элемент <test> спецификации задачи включает информацию о тестовых данных. Информация в обоих элементах представлена в формате JSON, требуемом для их дальнейшей обработки с помощью пакетного менеджера Composer. Обе спецификации расширены дополнительными элементами необходимыми для работы Orlando Tools, помещенными в элемент "orlando". Они игнорируются пакетным менеджером Composer и позволяют связать модули пакета программ с их реализациями в

репозиториях, а также задать наборы входных и выходных данных для тестирования схемы решения задачи. Элемент <modules> является необязательным. Он указывает версии модулей для данной схемы решения задачи. Примеры описаний в формате JSON приведены на рис. 5.

```
{"orlando": {
  "Имя_модуля": {
        "dir": "директория_модуля",
    "exe": "исполняемый_файл"}},
  "repositories": [Репозитории],
  "require": {Список модулей с
              указанием версий}}
```

a)

```
{"orlando": {
  "fileio": "Входные_файлы>
             выходные_файлы"},
  "repositories": [Репозитории],
  "require": {Пакет_с_тестовыми
              _данными}}
```

b)

Рис. 5. Пример описания информации о модуле (a) и тестовых данных (b)
Fig. 5. An example of the description of information about the module (a) and test data (b)

Разработка модулей пакета. На рис. 6 показаны результаты оценки среднего времени работы разработчика пакета, затрачиваемого им на добавление или модификацию одного модуля с использованием автоматизации непрерывной интеграции в Orlando Tools (а) и путем неавтоматизированного применения сторонних систем поддержки такого процесса в системах управления workflow, таких как Condor DAGMan [30] (н/а). Данные результаты показывают существенное сокращение времени (с/в), затрачиваемого разработчиком в первом случае, когда этапы компиляции исполняемого кода модуля, тестирования его скомпилированной версии, ее размещение в репозитории и тестирование модуля в составе схемы решения задачи выполняются в Orlando Tools автоматически, без его прямого участия. Сокращение времени во многом обусловлено исключением накладных расходов, связанных с запуском и завершением работы сторонних систем непрерывной интеграции, преобразованием и передачей данных между ними.

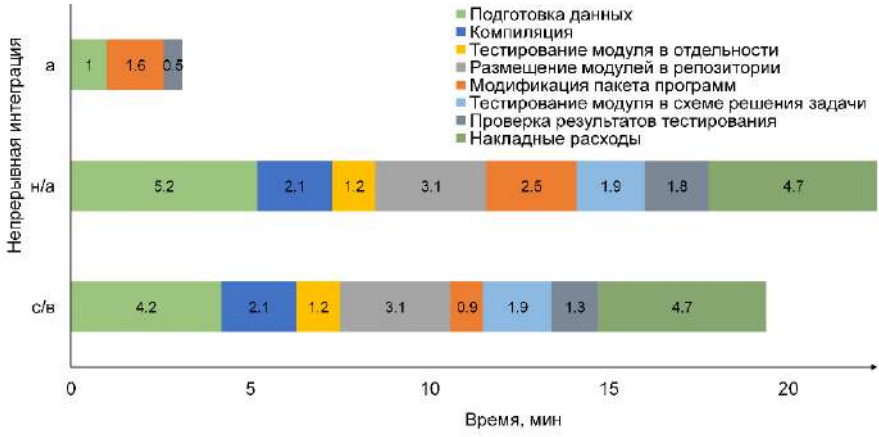


Рис. 6. Время выполнения непрерывной интеграции
Fig. 6. Continuous integration runtime

Прогнозирование времени выполнения схемы решения задачи. Схема решения задачи (рис. 3) выполнялась на десяти узлах двух вычислительных кластеров по двум сценариям: с оценкой времени выполнения ее модулей в узлах с помощью рассмотренной выше модели (о) и без такой оценки (б/о). Оценка времени выполнения модулей применялась для пропорционального распределения вычислительной нагрузки между узлами с учетом отличий их характеристик (узел кластера 1: 2 процессора AMD Opteron 6276, 16 ядер, 2.3 GHz, 64 GB оперативной памяти; узел кластера 2: 2 процессора Intel Xeon CPU X5670, 18 ядер, 2.1 GHz, 128 GB оперативной памяти). Числа узлов кластера 1 (кластера 2) в процессе эксперимента изменялось от 0/10 (10/0) до 10/0 (0/10). На рис. 7 представлены время

решения задачи, средняя загрузка процессоров, ускорение и эффективность вычислений при соотношении числа m узлов кластера 1 к числу n узлов кластера 2. Ускорение и эффективность вычислены относительно времени решения задач на 1 узле кластера 2.

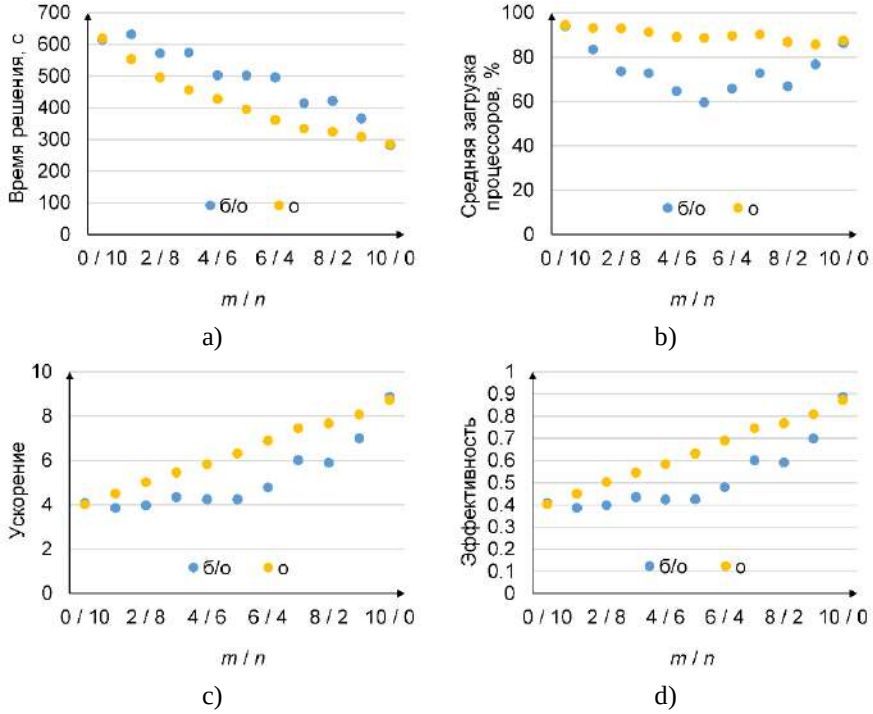


Рис. 7. Экспериментальные данные: время решения задачи (a), средняя загрузка процессоров (b), ускорение (c) и эффективность (d)

Fig. 7. Experimental data: problem-solving time (a), average processor load (b), speedup (c), efficiency (d)

Прогнозные оценки времени решения задачи, использованные в процессе распределения вычислительной нагрузки при разном соотношении узлов кластеров 1 и 2, показаны на рис. 8 в сравнении оценками пользователя, оценками, полученными на основе вычислительной истории и реальным временем решения задачи. Оценка пользователя, как правило, существенно завышена и основана на его практическом опыте решения задачи в однородной среде. Усредненная оценка, полученная на основе вычислительной истории, так же дает значительную погрешность, так как на основе такой истории сложно учесть различия в характеристиках узлов. Таким образом, наименьшую погрешность в большинстве случаев обеспечивает прогнозная оценка.

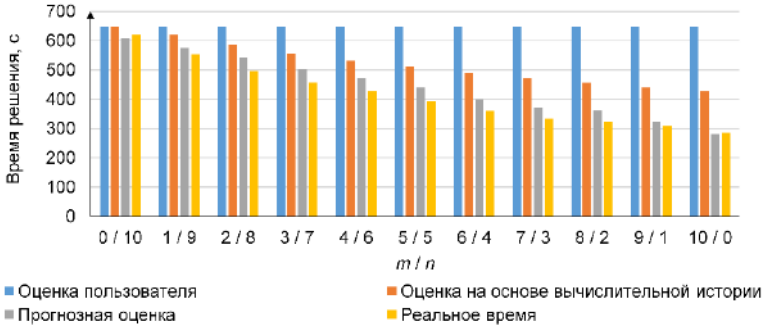


Рис. 8. Время решения задачи

Fig. 8. Problem-solving time

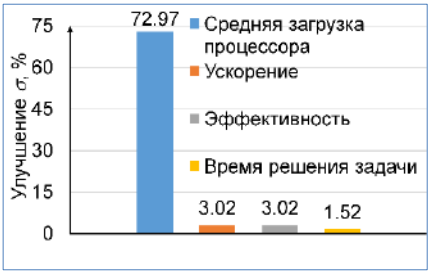


Рис. 9. Улучшение среднеквадратического отклонения критериев
Fig. 9. Improving the standard deviation of criteria

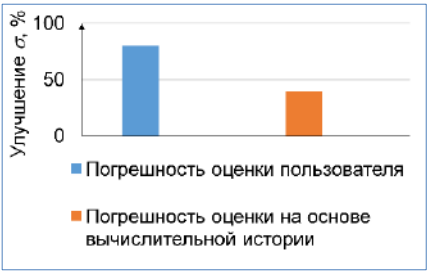


Рис. 10. Улучшение среднеквадратического отклонения погрешностей оценок
Fig. 10. Improving the standard deviation of evaluation errors

На рис. 9 приведено улучшение среднеквадратического отклонения σ критериев решения задачи при распределении нагрузки в ГРВС с учетом прогнозных оценок. Улучшение касается как эффективности использования ресурсов, так и процесса решения задачи. Рис. 10 показывает улучшение среднеквадратического отклонения σ погрешностей оценок времени решения задачи, полученных от пользователя и на основе вычислительной истории, в процентах. Расчеты выполнены в ИСКЦ СО РАН [31].

8. Заключение

В рамках предложенной системы непрерывной интеграции модулей РППП, в отличие от известных средств подобного назначения, реализуются как традиционные функции управления версиями программ, автоматизации их сборки и тестирования, так и новые функции извлечения и структуризации предметных знаний, унификации процессов сборки модулей как на выделенных серверах, так и на машинах разработчиков РППП путем использования специализированных виртуальных машин, синтеза тестовых схем решения задач на концептуальной модели и исследования свойств выполнения модулей относительно характеристик ГРВС. Результаты практического использования прототипа системы непрерывной интеграции показывают существенное улучшение различных показателей процесса выполнения вычислений в ГРВС.

Список литературы/References

[1] Il'in V.P., Skopin I.N. About performance and intellectuality of supercomputer modeling. Programming and Computer Software, vol. 42, no. 1, 2016, pp. 5-16.
[2] Massobrio R., Nesmachnow S., Tchernykh A., Avetisyan A., Radchenko G. Towards a Cloud Computing Paradigm for Big Data Analysis in Smart Cities. Programming and Computer Software, vol. 44, no. 3, 2018, pp. 181-189.
[3] Deelman E., Peterka T., Altintas I., Carothers C.D., van Dam K.K., Moreland K., Parashar M., Ramakrishnan L., Taufer M., Vetter J. The future of scientific workflows. The International Journal of High Performance Computing Applications, vol. 32, no. 1, 2018, pp. 159-175.
[4] Krol M., Rene S., Ascigil O., Psaras I. ChainSoft: Collaborative Software Development using Smart Contracts. In Proc. of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, 2018, pp. 1-6.
[5] Sochat V. Containershare: Open Source Registry to build, test, deploy with CircleCI. The Journal of Open Source Software, vol. 3, no. 28, 2018, pp. 1-3.
[6] Soni M., Berg A.M. Jenkins 2.x Continuous Integration Cookbook. Packt Publishing, 2017, 438 p.
[7] Machiraju S., Gaurav S. Deployment via TeamCity and Octopus Deploy. In S. Machiraju, S. Gaurav. DevOps for Azure Applications. Apress, 2018, pp. 11-38.
[8] Beller M., Gousios G., Zaidman A. Oops, My Tests Broke the Build: An Explorative Analysis of Travis

CI with GitHub. In Proc, of the 14th International Conference on Mining Software Repositories, 2017, pp. 356-367.
[9] Gruver G. Start and Scaling Devops in the Enterprise. BookBaby, 2016, 100 p.
[10] Shahin M., Babar M.A., Zhu L. Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. IEEE Access, 2017, pp. 3909-3943.
[11] Wolff E. A Practical Guide to Continuous Delivery. Addison-Wesley, 2017, 265 p.
[12] CruiseControl.NET (online). Available at: http://sourceforge.net/projects/ccnet, accessed 10.12.2018.
[13] Apache Gump (online). Available at: https://gump.apache.org, accessed 10.12.2018.
[14] Conan C/C++ package manager (online). Available at: https://www.conan.io, accessed 10.12.2018.
[15] BuildMaster (online). Available at: https://inedo.com/buildmaster, accessed 10.12.2018.
[16] Heckel T. (2015) Meet Travis CI: Open Source Continuous Integration, InfoQ (online). Available at: https://www.infoq.com/news/2013/02/travis-ci, accessed 10.12.2018.
[17] Chacon S., Straub B. Pro git. Apress, 2014, 419 p.
[18] Barrett D., Silverman R., Byrnes R. SSH: The Secure Shell. O'Reilly, 2005, 672 p.
[19] Blum R. Linux Command Line and Shell Scripting Bible, Wiley, 2017, 816 p.
[20] Colvin H. VirtualBox: An Ultimate Guide Book on Virtualization with VirtualBox. CreateSpace Independent Publishing Platform, 2015, 70 p.
[21] Крупин А. Обзор пакета Parallels Remote Application Server для виртуализации рабочих мест: все включено. 3DNews – Daily Digital Digest (online). Доступно по ссылке: https://3dnews.ru/931400, дата обращения 10.12.2018 / Krupin A. Overview of the Package Parallels Remote Application Server for Workplace Virtualization: All-inclusive, 3DNews – Daily Digital Digest, 2016. Available at: https://3dnews.ru/931400, accessed 10.12.2018 (In Russian).
[22] Smith R. Docker Orchestration. Packt Publishing – ebooks Account, 2017, 284 p.
[23] Luksa M. Kubernetes in Action. Manning Publications, 2018, 624 p.
[24] Varlamov M.I., Turdakov D.Y. A survey of methods for the extraction of information from Web resources. Programming and Computer Software, vol. 42, no. 5, 2016, pp. 279-291.
[25] Feoktistov A., Kostromin R., Sidorov I.A., Gorsky S.A. Development of Distributed Subject-Oriented Applications for Cloud Computing through the Integration of Conceptual and Modular Programming. In Proc. of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, 2018, pp. 256-261.
[26] JFrog Artifactory (online). Available at: https://jfrog.com/artifactory, accessed 10.12.2018.
[27] Debian Package Tracking System – Advanced Packaging Tool (online). Available at: https://packages.qa.debian.org/a/apt.html, accessed 10.12.2018.
[28] Yum Package Manager (online). Available at: http://yum.baseurl.org, accessed 10.12.2018.
[29] Bychkov I.V., Oparin G.A., Tchernykh A.N., Feoktistov A.G., Gorsky S.A., Rivera-Rodriguez R. Scalable Application for Searching Global Minimum of Multiextremal Functions. Optoelectronics, Instrumentation and Data Processing, vol. 54, no. 1, 2018, pp. 83-89.
[30] Tannenbaum T., Wright D., Miller K., Livny M. Condor – A Distributed Job Scheduler. In Beowulf Cluster Computing with Linux, The MIT Press, 2002, pp. 307-350.
[31] Иркутский суперкомпьютерный центр СО РАН (online). Доступно по ссылке: http://hpc.icc.ru, дата обращения 10.12.2018 / Irkutsk Supercomputer center of SB RAS. Available at: http://hpc.icc.ru, accessed 10.12.2018.

Информация об авторах / Information about authors

Александр Геннадьевич ФЕОКТИСТОВ – кандидат технических наук, доцент, ведущий научный сотрудник лаборатории параллельных и распределенных вычислительных систем Института динамики систем и теории управления им. В.М. Матросова СО РАН. Основное направление исследований – теория и практика разработки методов и инструментальных программных средств организации распределенных вычислений для решения фундаментальных и прикладных ресурсоемких задач.

Alexander Gennadievitch FEOKTISTOV – Candidate of Technical Sciences, Associate Professor, Leading Researcher of the Laboratory of Parallel and Distributed Computing Systems of the Matrosov Institute of System Dynamics and Control Theory of SB RAS. The main line of his

research is the theory and practice of developing methods and tool software for organizing distributed computing for solving fundamental and applied resource-intensive tasks.

Сергей Алексеевич ГОРСКИЙ – кандидат технических наук, научный сотрудник Института динамики систем и теории управления им. В.М. Матросова СО РАН. В число его научных интересов входят многоагентные системы, облачные вычисления, виртуализация, параллельная обработка, теория графов, булева алгебра, булевы функции.

Sergey Alekseevich GORSKY - Candidate of Technical Sciences, Researcher at the Matrosov Institute of System Dynamics and Control Theory of SB RAS. His research interests include multi-agent systems, cloud computing, virtualization, parallel processing, graph theory, Boolean algebra, Boolean functions.

Иван Александрович СИДОРОВ – кандидат технических наук, научный сотрудник Института динамики систем и теории управления им. В.М. Матросова СО РАН. Его научные интересы включают параллельное и распределенное программирование, облачные вычисления, виртуализацию.

Ivan Sergeevitch SIDOROV – Candidate of Technical Sciences, Researcher at the Matrosov Institute of System Dynamics and Control Theory of SB RAS. His research interests include parallel and distributed processing, cloud computing, virtualization.

Роман Олегович КОСТРОМИН – аспирант Института динамики систем и теории управления им. В.М. Матросова СО РАН. Его научные интересы включают распределенные прикладные программные пакеты, схемы решения проблем, многоагентное управление, отказоустойчивость.

Roman Olegovich KOSTROMIN – PhD student of the the Matrosov Institute of System Dynamics and Control Theory of SB RAS. His research interests include distributed application software packages, problem solving schemes, multi-agent management, and fault tolerance.

Евгений Сергеевич ФЕРЕФЕРОВ – кандидат технических наук с 2014 года, учёный секретарь Института динамики систем и теории управления им. В.М. Матросова СО РАН. В число его научных интересов входят распределенные вычислительные среды, имитационное моделирование, автоматизация разработки, информационные системы, приложения баз данных.

Evgeny Sergeevich FEREFEROV – Candidate of Technical Sciences since 2014, academic secretary of the the Matrosov Institute of System Dynamics and Control Theory of SB RAS. His research interests include distributed computing environments, simulation, development automation, information systems, database applications.

Игорь Вячеславович БЫЧКОВ – доктор наук, профессор, академик РАН, директор Института динамики систем и теории управления им. В.М. Матросова СО РАН. Основные научные интересы: интеллектуальная технология обработки пространственно-распределенных данных, технология автоматизации создания программных систем на основе метаописаний.

Igor Vyacheslavovich BYCHKOV – Doctor of Science, Professor, Academician of the Russian Academy of Sciences, Director of the Matrosov Institute of System Dynamics and Control Theory of SB RAS. His research interests include intellectual technology for processing spatially distributed data, technology for automating the creation of software systems based on meta descriptions.

DOI: 10.15514/ISPRAS-2019-31(2)-8

Полуавтоматический подход к параллельному решению задач с использованием модели Multi-BSP

М.О. Алениз, ORCID: 0000-0001-9984-2248 <marcelo.alaniz@fing.edu.uy>
С.Е. Несмачнов Кановас, ORCID: 0000-0002-8146-4012 <sergion@fing.edu.uy>
Республиканский университет,
Уругвай, г. Монтевидео, ул. Эрреры-и-Рейсига, д. 565

Аннотация. Модель Multi-Bulk Synchronous Parallel (Multi-BSP) – это модель параллельного программирования для многоядерных машин, которая расширяет классическую модель Bulk Synchronous Parallel. Multi-BSP направлена на поддержку разработки алгоритмов и оценки времени их работы. Эта модель в значительной степени опирается на правильное вычисление параметров, которые характеризуют оборудование. Конечно, использование оборудования также зависит и от особенностей задач и алгоритмов, применяемых для их решения. В этой статье представлен полуавтоматический подход к решению задач с применением параллельных алгоритмов на основе модели Multi-BSP. Во-первых, характеристики конкретного многоядерного компьютера определяются путем применения автоматической процедуры. После этого аппаратная архитектура, обнаруженная на предыдущем этапе, применяется для разработки переносимого параллельного алгоритма. Наконец, выполняется точная настройка параметров для повышения общей эффективности. Мы предлагаем бенчмарк для измерения параметров, которые характеризуют расходы на коммуникации и синхронизацию в конкретном оборудовании. Наш подход обнаруживает иерархическую структуру многоядерной архитектуры и вычисляет параметры для каждого уровня. Вторым вкладом нашего исследования является предложение системы поддержки Multi-BSP. Она позволяет разрабатывать алгоритмы, применяя рекурсивную методологию к иерархическому дереву, уже построенному с помощью бенчмарка, уделяя особое внимание трем элементарным функциям и основываясь на стратегии «разделяй и властвуй». Валидация предлагаемого метода производилась путем изучения алгоритма, реализованного в прототипе механизма Multi-BSP, тестирования различных конфигураций параметров, которые лучше всего подходят для каждой задачи, и использования трех различных высокопроизводительных многоядерных компьютеров.

Ключевые слова: высокопроизводительные исчисления; бенчмарк; многоядерное программирование; модель BSP

Для цитирования: Алениз М.О., Несмачнов Кановас С.Е. Полуавтоматический подход к параллельному решению задач с использованием модели Multi-BSP. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 97-120. DOI: 10.15514/ISPRAS-2019-31(2)-8

A semi-automatic approach for parallel problem solving using the Multi-BSP model

M.O. Alaniz, ORCID: 0000-0001-9984-2248 <marcelo.alaniz@fing.edu.uy>
S.E. Nesmachnow Cánovas, ORCID: 0000-0002-8146-4012 <sergion@fing.edu.uy>
Universidad de la República,
Herrera y Reissig 565, Montevideo, Uruguay

Abstract. The Multi-Bulk Synchronous Parallel (Multi-BSP) model is a recently proposed parallel programming model for multicore machines that extends the classic Bulk Synchronous Parallel model. Multi-BSP aims to be a useful model to design algorithms and estimate their running time. This model heavily relies on the right computation of parameters that characterize the hardware. Of course, the hardware utilization also depends on the specific features of the problems and the algorithms applied to solve them. This article introduces a semi-automatic approach for solving problems applying parallel algorithms using the Multi-BSP model. First, the specific multicore computer to use is characterized by applying an automatic procedure. After that, the hardware architecture discovered in the previous step is considered in order to design a portable parallel algorithm. Finally, a fine tuning of parameters is performed to improve the overall efficiency. We propose a specific benchmark for measuring the parameters that characterize the communication and synchronization costs in a particular hardware. Our approach discovers the hierarchical structure of the multicore architecture and compute both parameters for each level that can share data and make synchronizations between computing units. A second contribution of our research is a proposal for a Multi-BSP engine. It allows designing algorithms by applying a recursive methodology over the hierarchical tree already built by the benchmark, focusing on three atomic functions based in a divide-and-conquer strategy. The validation of the proposed method is reported, by studying an algorithm implemented in a prototype of the Multi-BSP engine, testing different parameter configurations that best fit to each problem and using three different high-performance multicore computers.

Keywords: High Performance Computing; Benchmark; Multicore Programming; BSP Model

For citation: Alaniz M.O., Nesmachnow Cánovas S.E. A semi-automatic approach for parallel problem solving using the Multi-BSP model. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 97-120 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-8

1. Введение

Модель BSP была представлена в конце 1980-ых гг. как модель программирования для распределенных вычислительных систем в предположении, что у каждого вычислительного узла имеется только одно ядро [9]. Хотя модель успешно использовалась в 1990-ых гг., постепенно ее популярность уменьшилась по причине возникновения в течении последних десяти лет новых многоядерных архитектур. Поскольку оценка возможностей компьютеров приобрела новое значение, модель BSP была расширена до Multi-BSP [10]. Multi-BSP расширяет BSP в двух направлениях:

- это иерархическая модель с произвольным числом компонентов, учитывающая физическую структуру многочисленных уровней памяти и кэша как одном чипе, так и в многокристальных архитектурах;
- в модели Multi-BSP, в отличие от исходной модели BSP, в качестве дополнительного параметра учитывается размер памяти на каждом уровне.

Учитывая характерные черты, присущие современным параллельным архитектурам, Multi-BSP обеспечивает более полную модель, позволяющую конструировать эффективные параллельные алгоритмы. Исследование, которому посвящена эта статья, состоит в разработке комплексного подхода к проектированию и реализации параллельных приложений на основе модели Multi-BSP с использованием самых современных инструментов и учетом требований не только производительности, но и переносимости

алгоритмов. Комплексная разработка предполагает наличие описанной аппаратной архитектуры, шаблона для разработки алгоритма, функции оценки стоимости алгоритма, а также конкретной методологии для реализации алгоритма на параллельной аппаратуре.

Основными результатами описываемого исследования являются:

a) предложение конкретной методологии для обнаружения иерархических структур многоядерной архитектуры и определение параметров, характеризующих расходы на коммуникации и синхронизацию в данной параллельной аппаратуре;
b) разработка системы поддержки Multi-BSP (Multi-BSP Engine), позволяющей разрабатывать алгоритмы при помощи применения рекурсивного шаблона «разделяй и властвуй» к иерархическому дереву, ранее построенному на основе применения бенчмарка;
c) валидация предложенного подхода, включающая разработку алгоритма с применением системы поддержки Multi-BSP, оценку различных конфигурационных параметров, которые лучше всего подходят для решения данной задачи, и реализацию алгоритма для трех разных высокопроизводительных многоядерных компьютеров, включая сопроцессор Xeon Phi, который не использовался в предыдущих аналогичных исследованиях.

Часть исследований, представленных в данной статье, была выполнена в рамках проекта «Scheduling evaluation in heterogeneous computing systems with hwloc» (SEHLOC). Основная цель проекта (SEHLOC) заключалась в разработке подсистем поддержки времени выполнения, которые позволяют комбинировать характеристики программного кода приложений и информацию о топологии вычислительных платформ для обеспечения планирования выполнения задач, позволяющего получить выигрыш от соответствия программных и аппаратных средств и обеспечить способ эффективного выполнения реалистичных приложений.

Эта статья расширяет нашу предыдущую работу [1], в которой были представлены первые идеи о применении Multi-BSP. В данной статье представлен более полный подход и представлена система Multi-BSP, поддерживающая весь процесс разработки параллельных алгоритмов.

Статья устроена следующим образом. В разд. 2 представлены модели BSP и Multi-BSP, а также автоматическое инструментальное средство, позволяющее обнаруживать особенности архитектуры и содействующее обеспечению переносимости приложений. В разд. 3 описаны родственные работы, относящиеся к разработке и использованию бенчмарков BSP, а также разработка и реализация бенчмарка MBSPDiscover. В разд. 4 описываются преимущества разработки алгоритмов с использованием Multi-BSP и разработанной системы поддержки, причем основное внимание уделяется рекурсивному построению шаблонов параллельных приложений для обеспечения переносимости. Функция стоимости разработана на основе модели затрат Multi-BSP. Система поддержки проверена на примере разработки простого алгоритма и реализации этого алгоритмы для трех параллельных машинах, характеристики которых были получены с использованием предложенного бенчмарка (разд. 5). Наконец, в разд. 6 представлены выводы и сформулированы основные направления будущих исследований.

2. Модели BSP и Multi-BSP

Чтобы установить контекст этой статьи, в этом разделе мы описываем модели BSP и Multi-BSP. Представлено краткое описание традиционной модели BSP и того, как модель доросла до включения концепции многоядерности, что привело к приданию особого значения иерархии компонентов. Далее описываются аналитические методы прогнозирования, что требуется для понимания основ обеих моделей. После этого описывается стоимостная функция Multi-BSP. В конце этого раздела мы рассуждаем о необходимости автоматического процесса обнаружения особенностей архитектуры для

обеспечения переносимости, а также описываем применение для этих целей конкретного пакета программ.

2.1 Оригинальная модель BSP

Модель BSP основана на понятии абстрактного параллельного компьютера, который полностью моделируется набором параметров: *количеством доступных процессоров (p)*, *скоростью процессора (s)*, *стоимостью коммуникаций (g)* и *стоимостью синхронизации (l)*. На основе этих можно точно вычислить время выполнения любого BSP-алгоритма.

В модели BSP вычисления организуются в виде последовательности глобальных супершагов, каждый из которых состоит из трех фаз:

a) каждый участвующий процессор выполняет локальные вычисления, во время которых его процессы могут использовать только значения, хранящиеся в локальной памяти данного процессора;
b) процессы обмениваются данными, чтобы обеспечить возможность доступа к удаленным данным;
c) каждый участвующий процесс должен достичь следующего барьера синхронизации.

После этого можно начать следующий супершаг.

Фактически, эта модель программирования соответствует парадигме «одна программа – много данных» (Single Program Multiple Data, SPMD): несколько копий программ на C/C ++, работают на p процессорах; обмен данными между копиями и их синхронизация производятся с использованием специальных библиотек, таких как BSPlib [5] или PUB [3]. Помимо определения абстрактной машины и наложения структуры на параллельные программы, модель BSP предоставляет функцию стоимости, опирающуюся на параметры архитектуры.

Общее время выполнения программы BSP может быть вычислено как накопленная сумма стоимости ее супершагов, где стоимость каждого супершага является суммой трех значений:

d) w – максимальный объем вычислений, выполняемых каждым процессором;
e) $h \times g$, где h – максимальное число сообщений, отправленных/полученных каждым процессором, причем каждое сообщение занимает g единиц времени и
f) l – временн*ая* стоимость барьера, синхронизирующего процессоры.

Влияние компьютерной архитектуры учитывается параметрами g и l. Эти значения, наряду со скоростью процессора s, могут быть определены эмпирически для каждого параллельного компьютера путем выполнения бенчмарков во время развертывания.

2.2 Модель Multi-BSP

Современные суперкомпьютеры состоят из высокопараллельных многоядерных узлов. Для обеспечения эффективности этих узлов потребовалось усовершенствование подсистемы основной памяти путем добавления нескольких иерархических уровней кэшей, а также обеспечения удаленного доступа к основной памяти, что приводит к архитектуре с неоднородным доступом к памяти (Non-Uniform Memory Access, NUMA).

В 2010 году Лесли Вэлиант (Leslie G. Valiant) обновил модель BSP, чтобы учесть эту ситуацию, что привело к появлению модели Multi-BSP [10]. Те же абстракции и архитектура шлюза, которые использовались в исходной BSP, в Multi-BSP были адаптированы для многоядерных машин, и экземпляр модели стали описывать в виде древовидной структуры вложенных компонентов, где листья – это процессоры, а каждый внутренний узел – компьютер BSP с локальной основной памятью или некоторым устройством хранения данных.

Формально машина Multi-BSP определяется списком уровней. Каждый уровень описывается четырьмя параметрами p_i, g_i, L_i, m_i.

- p_i – это число компонентов уровня $(i – 1)$ в компоненте уровня i. Для $i = 1$ компонентами первого уровня являются p_1 реальных процессоров, которые можно считать компонентами уровня 0. Продолжительность одного вычислительного шага такого процессора над словом основной памяти на уровне 1 принимается в качестве базовой единицы времени.
- g_i – это параметр стоимости коммуникаций, определяемый как частное от деления числа операций, которые процессор может выполнить за одну секунду на количество слов, которые могут быть переданы за одну секунду между памятью компонента уровня i и его родительским компонентом на уровне $(i + 1)$. Слово определяется как фрагмент данных, над которыми выполняются операции процессора. В модели предполагается, что основная память на уровне 1 привязана к процессорам, следовательно, скорость передачи данных (соответствующая значению g_0) также имеет значение 1.
- Li – это стоимость барьерной синхронизации для супершага на уровне i. Это определение предполагает требование барьерной синхронизации для подкомпонентов каждого компонента, но не предполагает синхронизацию подкомпонентов вышестоящих ветвей в иерархии компонентов.
- m_i – это число слов в основной памяти внутри компонента на уровне i, которая не находится ни в одном из компонентов уровня $(i − 1)$.

Рис. 1 демонстрирует компонент уровня i в модели Multi-BSP. Супершаг уровня i представляет собой набор инструкций, выполняемых в компоненте уровня i, что позволяет каждому из p_i компонентов на уровне $(i − 1)$ действовать независимо, включая все супершаги уровня $(i − 1)$. Как только все p_i компоненты закончат свои вычисления, они могут обменяться информацией с памятью m_i компонента уровня i. Стоимость коммуникаций этой операции определяется $g_i − 1$. Полная стоимость будет равна $m \times g_i − 1$, где m – это максимальное число слов, передаваемых между памятью компонента уровня i и любым его подкомпонентом уровня $(i – 1)$. После прохождения синхронизационного барьера всеми p_i компонентами может начаться следующий супершаг.

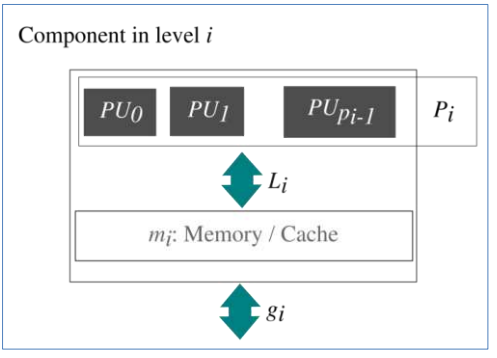


Рис. 1: Схематическое изображение компонента на уровне i в модели Multi-BSP
Fig. 1: Schematic view of a component on level i of the Multi-BSP model

На рис. 2 показана диаграмма компьютера, архитектура которого может быть определена тремя компонентами Multi-BSP (level0, level1 и level2): (1, 0, 0, 0), (4, g_1, L_1, 5118KB) и (8, g_2, L_2, 64 GB). Можно игнорировать level0, поскольку он содержит всего один процессор, и, таким образом, в нем отсутствуют внутренние коммуникации или синхронизация. Соответственно, в этой машине имеются два компонента, которые соответствуют двум уровням иерархии архитектуры.

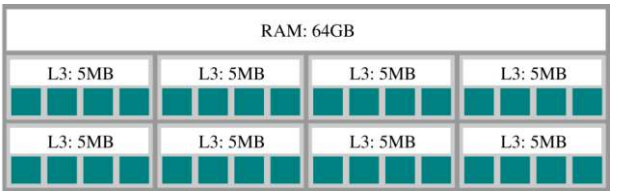


Рис. 2: Модель Multi-BSP: (4, g1, L1, 5118KB), (8, g2, L2, 64 GB)
Fig. 2: Multi-BSP model: (4, g1, L1, 5118KB),(8, g2, L2, 64 GB)

2.3 Прогнозирование затрат для модели Multi-BSP

Так же, как и у других абстрактных вычислительных моделей, одной из главных задач модели Multi-BSP является предоставление четкого представления о времени выполнения компьютерной программы. В этом подразделе представлена математическая формулировка модели стоимости исполнения, основанная на полном определении операционной семантики Альберта-Яна Изельмана (Albert-Jan Yzelman) [11]. Позже в подразделе 4.3 мы представляем упрощенную формулировку и подробно описываем систему поддержки Multi-BSP, рассматриваемую нами, как основной вклад данной работы.

Прогноз затрат на конкретном компьютере выражается в терминах объема вычислений, объема перемещаемых данных и задержки в соответствии с формулой (1), где L соответствует числу уровней в дереве Multi-BSP, N_k – число супершагов на k-м уровне, $h_{k,i}$ – максимум всех h-отношений в i-м супершаге на уровне k, а $w_{k,i}$ – максимум объема всех работ в i-м супершаге на уровне k.

$$T = \sum_{k=0}^{L-1} \left(\sum_{i=0}^{N_k-1} w_{k,i} + h_{k,i} \times g_k + l_k \right) \qquad (1)$$

Формула (1) соответствует сумме стоимостей супершагов каждого k-го компонента Multi-BSP. Стоимость отдельного супершага состоит из двух независимых слагаемых: стоимость вычислений и стоимость коммуникаций. Стоимость коммуникаций включают в себя стоимость синхронизации (l_k, всегда одно значение на один супершаг), а слагаемое $h_{k,i} \times g_k$, зависящее от числа операций put/get между потоками, формально определяется на основе понятия h-отношения (h-отношением (*h-relation*) называется максимальное число сообщений, получаемых или посылаемых процессором). Выполнение супершага внутри каждого компонента происходит последовательно, а внутри супершага каждый поток работает параллельно. Таким образом, величины $h_{k,i}$ и $w_{k,i}$ соответствуют максимумам всех h-отношений на супершаге i на уровне k и максимуму объемов всех работ на супершаге i на уровне k соответственно.

Для обеспечения переносимости при комплексной разработке с использованием Multi-BSP требуется использовать процедуру для обнаружения свойств используемой компьютерной архитектуры. В бенчмарке Multi-BSP используется переносимый инструмент HardWare LOCality (hwloc) [4], обнаруживающий характеристики используемой аппаратуры. hwloc позволяет получать информацию о компьютере во время выполнения. Мы используем hwloc версии 1.7.2, которая обеспечивает абстракцию (не зависящую от используемой операционной системы, архитектуры и т.д.) иерархической топологии современных архитектур, включая процессоры, узлы памяти NUMA, сокеты, общие кэши, ядра и расположение устройства ввода/вывода.

3. Механизм обнаружения и тестирования для Multi-BSP

Многоядерные архитектуры широко используются для разработки и выполнения высокопроизводительных приложений [6]. Количество ядер, как и уровней кэша в

многоядерной архитектуре за последние годы стабильно увеличивалось. Поэтому существует реальная потребность выявления и оценки различных параметров, которые характеризуют структуру процессорных ядер и основной памяти, не только для того, чтобы понимать и сравнивать различные архитектуры, но и для их разумного использования для более качественной разработки высокопроизводительных приложений. Это обосновывается тем, что возможность повышения производительности при использовании многоядерного процессора очень зависит от программных алгоритмов, их реализации и использования возможностей аппаратного обеспечения.

В модели Multi-BSP производительность параллельного алгоритма зависит от параметров, которые характеризуют многоядерную машину: расходы на коммуникации и синхронизацию, количество ядер и объем кэша. Составление аналитических уравнений для расчета этих параметров – сложная задача. По этой причине жизнеспособным методом оценки производительности и определения характеристик архитектуры является эталонное тестирование (*benchmarking*).

В этом разделе представлен обзор родственных работ по бенчмаркам моделей BSP и Multi-BSP, а также описана разработка и реализация инструмента обнаружения и эталонного тестирования (Multi-BSP-Disc-Bench), предназначенного для оценки параметров g и L, которые характеризуют машину Multi-BSP.

3.1 Родственные работы

Программа BSPbench из пакета BSPEupack [3] является основным инструментом для эталонного тестирования модели BSP. Этот бенчмарк измеряет полное h-отношение, когда каждый процессор отправляет и получает ровно h слов данных. Методология пытается выявить самое медленное коммуникационное взаимодействие, циклически перемещая одиночные слова в другие процессоры. Это показывает, действительно ли системное программное обеспечение комбинирует данные для одного и того же пункта назначения и может ли оно эффективно обрабатывать коммуникации «каждый с каждым». В этих случаях результирующее значение параметр g, полученное программой эталонного тестирования BSPbench, называются пессимистическим.

Пакет программ Oxford BSP [5] включает другую программу эталонного тестирования для BSP – bspprobe. Этот бенчмарк измеряет оптимистические значения g, используя не отдельные слова, а пакеты большего размера. Еще одним вариантом эталонного тестирования BSP является использование инструмента mpibench из пакета MPIedupack [5].

Эталонному тестированию вычислительной модели multi-BSP посвящена недавняя публикация Савади (Abdorreza Savadi) и Делдари (Hossein Deldari) [7], которые использовали подход, очень близкий к тому, который применяли мы. За основу берется эталонное тестирование BSP, однако экземпляр модели определяется по-другому. В отличии от методологии эталонного тестирования, использованной в нашей работе, авторы [7] принимают во внимание мельчайшие детали архитектуры, например, как поддерживается когерентность кэшей для распространения значений в иерархической структуре памяти. В их подходе анализ результатов основывается на сравнивании действительных значений g и L, полученных тестированием, и теоретических значений этих параметров, которые рассчитываются как оптимистические нижние границы, т.е. авторы предполагают, что все нужные данные всегда помещаются в кэше и все ядра работают на максимальной скорости. В этом наш подход отличается, поскольку мы не делаем никаких предположений о базовой аппаратной платформе, а скорее скрываем ее характеристики в результатах тестов. Мы считаем, что эта стратегия лучше подходит для современных архитектур, которые слишком сложны для точного моделирования из-за наличия расширенных, скрытых и/или плохо документированных возможностей.

С практической точки зрения, основной особенностью инструмента обнаружения и эталонного тестирования, который мы описываем в этой статье, является оценка реальных операций Multi-BSP, реализованных на основе библиотеки MulticoreBSP for C [12]. Кроме того, наши результаты проверяются с использованием набора реальных программ Multi-BSP, где реальное время выполнения на нескольких высокопроизводительных платформах сравнивается с прогнозируемым временем с использованием теоретической функции стоимости Multi-BSP.

3.2 Разработка инструментального средства Multicore-BSP-Disc-Bench

При разработке своего инструмента Multi-BSP-Disc-Bench мы использовали общие идеи бенчмарка BSPbench [3] для стандартной модели BSP и расширили его возможности с учетом отличий модели Multi-BSP. Основное отличие бенчмарка для BSP от бенчмарка для Multi-BSP заключается в необходимости получения пар значений параметров g и L для каждого уровня компонентов в модели Multi-BSP. Кроме того, в случае Multi-BSP обработка выполняется внутри многоядерных узлов, а не внешними узлами, соединенными сетью.

Важно подчеркнуть, что качество инструмента сравнения не должно зависеть от конкретной архитектуры. Это дополнительное требование решается путем автоматического обнаружения взаимосвязей различных ядер на каждом уровне кэша. Еще одна важная цель бенчмарка для Multi-BSP состоит в том, чтобы обнаруживать особенности архитектуры во время выполнения. Для этого мы используем инструмент hwloc.

Компоненты предлагаемого бенчмарка описываются в следующих подразделах.

3.2.1 Архитектура и модули программного обеспечения

На рис. 3 представлены архитектура и состав модулей инструментального средства Multi-BSP-Disc-Bench.

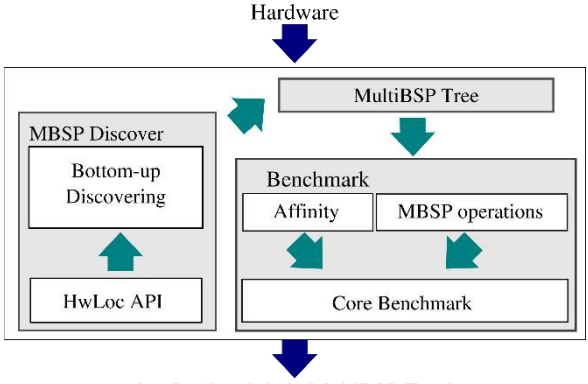


Рис. 3: Схематическое изображение архитектуры программного обеспечения Multi-BSP-Disc-Bench и процесса обнаружения и эталонного тестирования

Fig. 3: Schematic view of the software architecture of Multi-BSP-Disc-Bench, and the discovering and benchmarking process

Функциональные возможности модулей Multi-BSP-Disc-Bench состоят в следующем.

- Модуль обнаружения (*Multi-BSP Discover*). Этот модуль собирает данные об архитектуре и свойствах аппаратуры, используя hwloc, и загружает данные в дерево ресурсов (структура памяти, определенная внутри блока API hwloc).
- Интерфейс (*Multi-BSP Tree*). После построения структуры, содержащей информацию о ресурсах, набор функций интерфейсного модуля проходит по дереву, используя восходящий процесс для построения нового дерева с именем Multi-BSP Tree. Это новое дерево содержит всю информацию, необходимую для поддержки модели Multi-BSP.

- Модуль эталонного тестирования (*Multi-BSP Bench*). Этот модуль извлекает из дерева Multi-BSP информацию об индексах и объеме кэш-памяти ядер для каждого уровня. После этого он измеряет стоимость коммуникаций и стоимость синхронизации через подмодуль Multi-BSP и использует подмодуль нахождения соответствия для закрепления каждого уровня на правильном ядре. Наконец, этот модуль вычисляет результирующие параметры g и L.

Эти шаги процесса тестирования применяются в соответствии с псевдокодом, показанном в алгоритме 1.

```
1: Multi-BSP-Tree ← Multi-BSP-Discover ()
2: for each level in Multi-BSP-Tree do
3:   [g, L] ← coreBenchmark(level)
4: end for
```

Алгоритм 1. Псевдокод Multi-BSP Discover
Algorithm 1. Multi-BSP Discover pseudocode

Multi-BSP Tree выступает в качестве интерфейса между Multi-BSP Discover и модулем эталонного тестирования. В качестве примера на рис. 4 показана структура, соответствующая конкретной аппаратной архитектуре с 32 ядрами, сгенерированная Multi-BSP Discover.

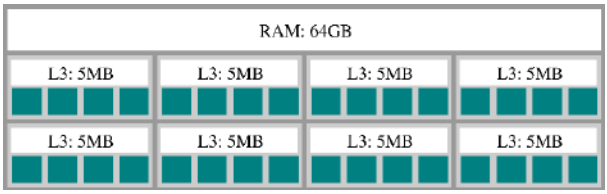


Рис. 4: Структура Multi-BSP Tree, сгенерированная Multi-BSP-Disc-Bench
Fig. 4: Multi-BSP Tree structure generated by Multi-BSP-Disc-Bench

3.2.2 Модуль coreBenchmark

Модуль coreBenchmark разработан для расчетов параметров gi и Li согласно псевдокоду, приведенному в Алгоритме 2.

```
01: setPinning(level.cores indexes)
02: begin(level.cores)
03: rate ← computingRate(level)
04: sync()
05: for h = 0 to HMAX do
06:   initCommunicationPattern(h)
07:   sync()
08:   t0 ← time()
09:   for i = 0 to NITERS do
10:     communication()
11:     sync()
12:   end for
13:   t ← time() − t0
14:   if master then
15:     times.append(t × rate/NITERS)
16:   end if
17: end for
18: level.g, level.L ← leastSquares(times)
19: return (level.g, level.L)
```

Алгоритм 2. Функция coreBenchmark
Algorithm 2. coreBenchmark function

Функция *coreBenchmark* принимает в качестве параметров информацию соответствующего уровня модели Multi-BSP, а данные, используемые для установления соответствия потоков (т.е. данные об индексах и объеме памяти кэша) хранятся в структуре Multi-BSP Tree. Сначала (строка 1 алгоритма 2) функция *setPinning* модуля установления соответствия (*affinity module*) используется для связи нитей, порожденных функцией begin (строка 2), с ядрами, соответствующими данному уровню. Функция порождает одну нить на каждое ядро данного уровня и рассчитывает скорость вычислений компонента Multi-BSP, используя функцию *computingRate* (строка 3). У каждого уровня имеется набор ядер с общей памятью; впоследствии при эталонном тестировании учитываются только эти ядра.

Функция *computingRate* (строка 3) измеряет время, требуемое для выполнения 2×*n*×DAXPY операций. Подпрограмма DAXPY выполняет векторную операцию $y = \alpha \times x + y$, складывая несколько векторов с двойной точностью с другим вектором двойной точности. DAXPY – это стандартная операция для оценки эффективности вычислительной платформы при выполнении операций с плавающей запятой, интенсивно использующих память, из набора Basic Linear Algebra Subprograms – Level 1 (BLAS1, http://www.netlib.org/blas). После этого выполняется синхронизация для текущего уровня (строка 4), чтобы гарантировать, что для всех потоков имеется правильное значение скорости вычислений.

Мы используем функцию *coreBenchmark* для измерения полной *h*-коммуникации. Это абстракция, которую мы определяем, как расширение абстракции *h*-отношения из стандартной модели BSP, но в этом случае понятие применяется к случаю наличия общей памятью внутри одного узла. *h*-коммуникация – это такая коммуникация, при которой каждое ядро записывает/считывает ровно *h* слов данных. Мы рассматриваем наихудший случай, измеряя самую медленную возможную коммуникацию путем циклического считывания отдельных слов данных из памяти других процессоров. Таким образом, значения g_i и l_i, вычисляемые с использованием нашего бенчмарка, являются пессимистическими значениями, и реальные значения всегда будут лучше. Переменная *h* представляет наибольшее количество слов, прочитанных или записанных в общей памяти данного уровня. *HMAX* – это максимальное значение для всех параметров (*h*), используемых в шаблонах связи для каждого уровня. Значения *HMAX* могут различаться для разных уровней иерархии; мы предлагаем находить подходящие значения с помощью эмпирического анализа.

Время коммуникаций (вычисляемое на основе шаблона *h*-коммуникации) инициализируется процедурой *initCommPattern* (строка 6). Этот процесс повторяется *NITERS* раз (строки 9–12), потому что каждая операция является слишком быстрой, чтобы ее можно было измерить с достаточной точностью. После этого главный поток на каждом уровне сохраняет время, потраченное на каждую *h*-коммуникацию (строка 15).

Наконец, параметры *g* и *L* вычисляются с использованием традиционного метода аппроксимации наименьших квадратов для подгонки данных к линейной модели (линия 18) в соответствии с результатами и аппроксимациями, найденными в родственных работах [1, 5].

Таким образом, метод обеспечивает точные приближения для g_i и L_i.

3.3 Эмпирический анализ h-коммуникаций

Методология, применяемая для измерения h-коммуникаций и затем определения значений параметров g и L, основана на измерении реализации операций Multi-BSP. Мы называем операциями Multi-BSP функции/процедуры, которые требуются для реализации алгоритма, разработанного с использованием вычислительной модели Multi-BSP. В нашей разработке операционный модуль Multi-BSP содержит реализацию этих функций, включая операции, предоставляемые библиотекой MulticoreBSP for C [12]. Эта библиотека устанавливает методологию программирования в соответствии с вычислительной моделью Multi-BSP.

Важно учитывать архитектуру инструмента Multi BSP-Disc-Bench, показанную на рис. 3: если алгоритмы Multi-BSP программируются с использованием других библиотек, можно реконфигурировать инструмент, изменяя операционный модуль Multi-BSP, и повторно выполнить процедуру обнаружения и эталонного тестирования с новой конфигурацией. Более подробная информация о методологии эмпирической оценки *h*-коммуникации представлена в нашей статье [1].

4. Предлагаемая система поддержки разработки и выполнения алгоритмов мульти-BSP

В этом разделе представлено наше предложение системы поддержки разработки и выполнения алгоритмов мульти-BSP. Предлагаемая система будет поддерживать разделение данных, управление потоками и выполнение, инкапсулируя всю базовую логику, которая будет скрыта для программиста. На самом деле, в предлагаемой системе рекурсивно применяется стратегию «разделяй и властвуй».

4.1 Основные идеи

Предлагаемая система задумана как базовый слой, скрывающий детали реализации, необходимые для работы с алгоритмами Multi-BSP. Основная цель системы состоит в том, чтобы предоставить простой и осмысленный способ разработки и реализации кода Multi-BSP, обращая внимание только на стратегии решения задач, а не фокусируясь на конкретных деталях модели Multi-BSP, таких как управление потоками, разделение данных и распределенное выполнение.

В предлагаемой системе используется процесс обнаружения для определения базовой архитектуры многоядерного компьютера и строится стратегия «разделяй и властвуй» для решения задачи. Стратегия «разделяй и властвуй» применяется рекурсивно на разных уровнях аппаратной архитектуры, которые представляются в виде дерева. Стратегия направлена на решение трех основных проблем: разделение данных, наращивание потоков и свертывание потоков для вычисления окончательных результатов.

Предлагаемая система сможет предоставить программистам несколько преимуществ, три из которых наиболее актуальны:

- у программиста будет иметься улучшенная спецификация его алгоритмов;
- один программный слой будет управлять общими вопросами, свойственными каждой реализации Multi-BSP и
- подход обеспечит переносимость алгоритмов Multi-BSP.

Полезная особенность любой реализации Multi-BSP заключается в том, что программисту требуется гарантия того, что применяемое разделение данных приведет к эффективному использованию кэш-памяти, то есть обеспечит большое число успешных обращений к кэш-памяти и минимизирует промахи. Это обеспечивается естественным образом, если в алгоритме применяется стратегии разделения данных на основе доступного оборудования, а потоки или процессы выполняются в процессорных блоках, ближайших к этой памяти единицах. Как правило, размер раздела данных никогда не должен превышать размер соответствующего размера кэша.

Другая проблема алгоритмов Multi-BSP заключается в необходимости их разработки в тесной связи с архитектурой аппаратуры. В этой ситуации нельзя гарантировать переносимость специально разработанного алгоритма, и, возможно, он будет правильно работать только на машинах того же типа (с теми же размерами кэшей каждого уровня, с тем же распределением процессорных блоков и т.д.). Чтобы решить эту проблему, в предлагаемой системе реализуется общий метод для сокрытия всех специфических деталей аппаратного обеспечения, и программисту нужно будет обеспечить только общие функции,

которые могут использоваться в различных архитектурах, не преодолевая трудности, связанные с особенностями конкретной аппаратуры, и обеспечивая таким образом переносимость. В следующем подразделе описываются особенности предлагаемой системы поддержки Multi-BSP.

4.2 Структура системы поддержки Multi-BSP

Как отмечалось выше, система поддержки Multi-BSP – это обобщенная рекурсивная процедура, которая обходит дерево, представляющее конкретную обобщенную архитектуру аппаратуры. Путь, которого придерживается система, определяет стратегию разделения данных, наращивания и свертывания потоков. В нашей реализации применен алгоритм прямого обхода, но это всего лишь одно из возможных простых решений, позволяющих получить полезные результаты. Алгоритм обхода можно кастомизировать, изменяя используемые пути прохода по дереву.

В системе используется тот же процесс автоматического обнаружения особенностей аппаратуры, который применяется в Multi-BSP-Disc-Bench для генерации Multi-BSPTree. После получения этой информации система обрабатывает дерево рекурсивным образом, причем каждый уровень рекурсии отображается на соответствующий уровень вычислительной модели Multi-BSP.

Псевдокод, показывающий общую схему функционирования системы поддержки Multi-BSP представлен в алгоритме 3. У системы имеются два входных параметра: i) текущий узел дерева, представляющий некоторый компонент Multi-BSP, ii) данные для работы. Вся информация, нужная для определения соответствия потоков, уже доступна в компоненте Multi-BSP. В структуре данных имеются указатели на подкомпоненты (*t.sons*), и у каждого подкомпонента имеются правильные индексы для работы.

У каждого потока имеется уникальный идентификация $p \in [0 \ldots n-1]$, где n – число потоков, полученное при помощи вызове функции *bsp_nprocs*. Идентификатор потока p определяется путем вызова функции *bsp pid* (строки 3 и 4 в алгоритме 3).

После этого, к данных применяется функция разделения с использованием в качестве параметров значений p и n (строка 5). До обработки дерева требуется барьерная синхронизация (функция *bsp_synch()*), чтобы гарантировать доступность соответствующего частного фрагмента данных в каждом из потоков (строка 5). Затем рекурсия начинает обрабатывать узлы дерева.

```
01: bsp_set_pin(t.sons){ Affinity using sons components }
02: bsp_begin()  { Spawn threads }
03: n ← bsp_nprocs() { Amount of threads in the current level }
04: p ← bsp_pid() { thread id / component number at level n }
05: dpi ← partition(|d|, p, n) { Data for thread p and level i }
06: bsp_synch()  { Sync to guarantee all threads have their partitions }
07: if n > 1 then { is not a leaf component / it has sons }
08:   foreach tson, i in t.sons do
09:     vr[i] ← mbspEngine(dpi, tson) { recursion down over sons}
10:   end for
11:   bsp synch() { Waiting to receive the result of every son }
12:   if master then
13:     r ← reduce(vr) { The master of the level executes reduce}
14:   end if
15: else
16:   r ← work(dij) { The leaf thread executes work function }
17: end if
18: bsp_synch() { Wait for master to have r or sons running work}
19: return r
```

Алгоритм 3. Система поддержки Multi-BSP
Algorithm 3. Multi-BSP engine

Обработке данных в тех компонентах, которые не являются листовыми узлами, соответствует код в строках 7–16. Выполняется рекурсивный вызов процедуры *mbspEngine* (строки 8–10) с использованием в качестве параметров текущего раздела данных и узла дерева для каждого подкомпонента. Каждый вызов возвращает результат, который сохраняется в векторе *vr*. Чтобы гарантировать, что все результаты хранятся в *vr*, необходима синхронизация (строка 11). Затем вызывающий поток (то есть главный поток) редуцирует значения, применяя к вектору *vr* функцию *reduce* (строки 12–14). Наконец, действия, выполняемые при достижении рекурсией листовых узлов Multi-BSPTree, показаны в строках 15–17, где выполняется функция *work* для вычисления частичных результатов.

На рис. 5 показано типичная работа системы при решении разделяемой задачи, где применяются функции, определенные пользователем: *partition*, *work* и *reduce*. Работа происходит на компьютере, архитектура которого содержит два уровня, каждый из которых имеет два подкомпонента. Каждый серый квадрат представляет экземпляр компонента Multi-BSP, а каждая стрелки представляют связи между компонентами.

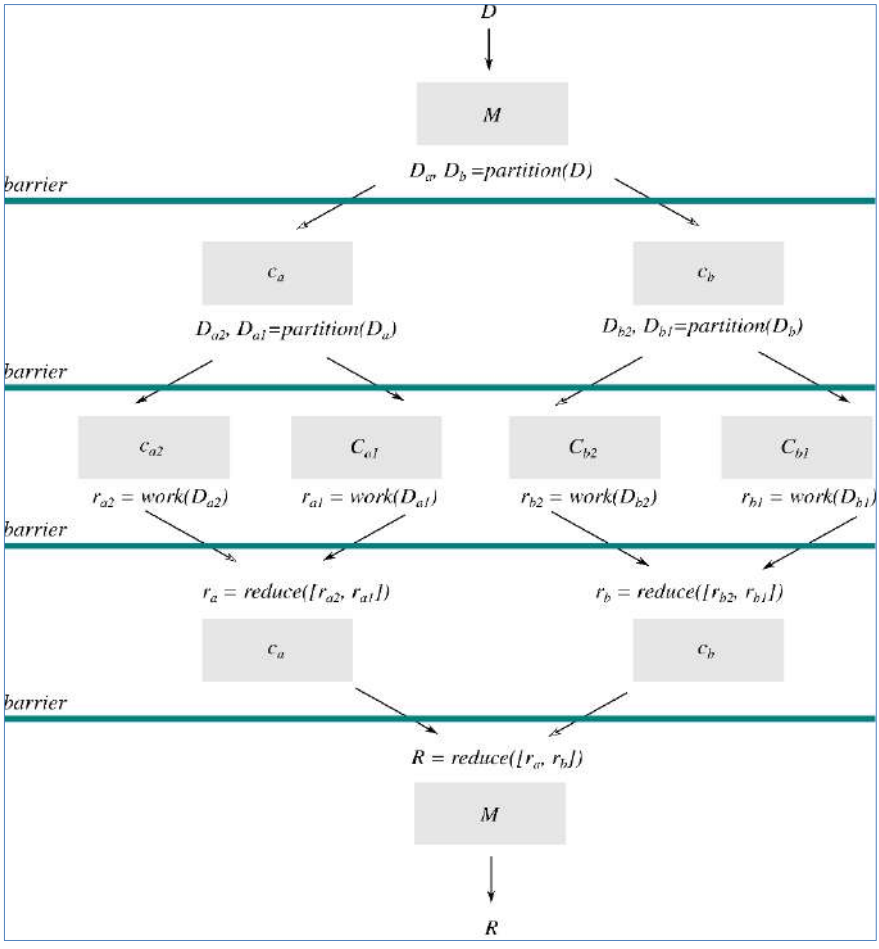


Рис. 5: Схематическое изображение работы MBSPEngine
Fig. 5: Schematic view of an MBSPEngine execution

4.3 Оценочная функция для предлагаемой системы

В системе имеются три последовательных этапа на каждом шаге *T*, выполняемых над деревом архитектуры: рекурсивный обход дерева сверху вниз (*CD*), вызов функции *work* на уровне листьев (*CW*) и возврат из рекурсии снизу вверх (*CU*). Каждый шаг *T* представляет собой работу, необходимую для обработки фрагмента данных *D*.

Стоимость выполнения системы представляет собой сумму значений стоимостных функций для каждого из трех последовательных шагов: *CT = CD + CW + CU*. Как показано ниже, значение стоимостной функции для каждого шага и компонента вычисляется на основе формулы (1).

Рекурсия сверху вниз. Декомпозиция данных фрагмента *D* выполняется с применением функции partition только один раз (то есть один супершаг) на уровень. Тогда соответствующее значение N_k в формуле (1) равно 1, и поскольку функция *partition* является последовательной и безопасной для потоков (т.е. не требует параллельных вычислений), для нее можно использовать стандартную нотацию «О большое», в результате чего получается формула (2).

$$C_D = \sum_{k=0}^{L-1} (O(partition_k) + h_k \times g_k + l_k) \qquad (2)$$

У компонента, работающего на этапе разделения, имеются *p* подкомпонентов, с каждым из которых он нуждается в коммуникации. Поэтому, значение h_k для каждого разделения максимально, что приводит к формуле (3).

$$C_D = \sum_{k=0}^{L-1} \left(O(partition_k) + \frac{D_k}{p_k} \times g_k + l_k \right) \qquad (3)$$

Work. Функция *work* еще проще, поскольку она выполняется только один раз на одном конкретном уровне: листьях дерева, соответствующих процессорным блокам каждого компонента. Тогда N_k и *L* равны 1, а стоимость определяется формулой (4).

$$C_w = O(work_{leaf}) + l_0 \qquad (4)$$

Рекурсия снизу вверх. Стоимость восходящей рекурсии складывается из стоимости функции *reduce* на каждом уровне. Важно, что каждое выполнение функции *reduce* зависит от количества непосредственных потомков этого уровня. После вызова функции *reduce* каждый непосредственный потомок вернет одно значение, что подразумевает наличие одой коммуникации снизу вверх для каждого подкомпонента. Если у компонента на уровне *k* имеется p_k подкомпонентов, выполняющих *reduce*, то количество сообщений (h_k) будет равно p_k, по одному на каждый подкомпонент. Тогда стоимость задается формулой (5).

$$C_D = \sum_{k=0}^{L-1} (O(reduction_k) + p_k \times g_k + l_k) \qquad (5)$$

Результирующая формула (6) дает время выполнения алгоритма, разработанного для системы поддержки Multi-BSP.

$$C_T = O(work_{leaf}) + l_0 + \sum_{k=0}^{L-1} \left(O(partition_k) + O(reduction_k) + p_k \times g_k + \frac{D_k}{p_k} \times g_k + 2l_k \right) \qquad (6)$$

Следующий подраздел представляет пример алгоритма, разработанного при помощи предлагаемой системы путем задания конкретных спецификаций функций partition, work и reduce

4.4 Пример применения MBSPEngine

В этом подразделе описывается простой пример применения предлагаемой системы для решения простой декомпозируемой задачи. Этот пример обеспечивает ориентир для разработки и реализации более сложных алгоритмов путем определения всего трех основных функций, включаемых в систему: *partition, work* и *reduce*.

Функция *partition* разбивает исходные данные по одному фрагменту на каждый подкомпонент. Обработка выполняется рекурсивно над деревом MBSP, и фрагмент данных компонента является источником для следующего вызова функции *partition* внутри его подкомпонентов. Когда рекурсия достигает фазы остановки, в компоненте на уровне 0 на процессорах выполняется функция *work*. Когда функция *work* возвращает результат, мастер-процесс объединяет результаты подкомпонентов путем вызова функции *reduce*. Результат функции *reduce* отправляется в родительский компонент. Процесс выполнения разделений, работы на процессорах и редукции результатов представлен на рис. 5.

Важно отметить, что не каждый параллельный алгоритм будет соответствовать общей схеме, поддерживаемой в нашей системе. Рекурсивная стратегия «разделяй и властвуй» обычно не наилучшим образом подходит для задач, данные которые не могут быть разделены произвольным образом. Чтобы можно было разрабатывать переносимые алгоритмы MultiBSP с применением нашей системы, нужно, чтобы допускалась возможность рекурсивного разделения данных по компонентам раскрываемой аппаратной архитектуры.

Кроме того, программист заранее не знает архитектуру компьютеров, для которых он разрабатывает конкретную программу. Программист может разработать конкретный алгоритм, тесно связанный с данным компьютером, но в этом случае весьма вероятно, что алгоритм не сможет эффективно использовать функции других аппаратных платформ (например, когда доступно большее количество вычислительных ресурсов/ядер). В некоторых случаях алгоритм вообще не сможет работать на другой архитектуре. Использование предложенной системы позволяет программисту разрабатывать и реализовывать переносимые алгоритмы. Такие алгоритмы обнаружат архитектуру компьютера, на котором они выполняются, и воспользуются возможностями доступных ресурсов и топологии. В соответствии с обнаруженной информацией задачи разделения данных будут выполняться на вводном этапе, затем на доступных ресурсах будет выполняться функция work, а результаты будут редуцироваться на этапе свертывания рекурсии. Таким образом, для любого алгоритма, который вписывается в общую схему, поддерживаемую системой (то есть, если его данные могут быть разделены произвольны произвольным образом), она предоставляет полезный способ прозрачного и эффективного использования преимуществ базовой аппаратной архитектуры.

Чтобы лучше проиллюстрировать преимущества предложенного движка, в этом подразделе в качестве примера мы представляем алгоритм вычисления скалярного произведения двух векторов. Очевидно, что он подходит для рекурсивной стратегии «разделяй и властвуй» (т.е. следуя подходу параллелизма по данным) и, следовательно, и для нашей системы. Алгоритм прост, но он очень полезен, чтобы показать, как можно работать с предлагаемый системой.

Начнем с определения трех функций, необходимых для двигателя. Функция *Partition* (Алгоритм 4) разделяет исходные данные на основе номера компонента и числа компонентов на данном уровне. Для представленного примера функция обеспечивает разделение, пригодное для алгоритма вычисления скалярного произведения: фрагмент общих данных, разделенный между заданным числом компонентов. Конкретный номер каждого номера компонента используется для определения фрагмента, который будет использоваться компонентом.

```
01 Partition(interval, componentNumber, n) {
02   sliceSize = interval.length / n
02   return interval.slice [
03       sliceSize * componentNumber,
04       sliceSize * (componentNumber+1)
05   ]
06 }
```

Алгоритм 4. Функция разделения для примера скалярного произведения
Algorithm 4. Partition function for dot product instance

Функция *Work* (алгоритм 5) получает фрагмент, или интервал исходных данных. В данном случае эта функция выполняется только для листовых компонентов. Это самые элементарные компоненты, то есть процессоры со своей ближайшей памятью. Как показано на рис. 5, каждый поток, работающий на этом уровне, напрямую соответствует процессору. Как показано ниже, возвращаемое значение будет использоваться функцией *Reduce*.

```
01 Work (slice) {
02     for value in slice {
03        result += value*value
04     }
05     return result
06 }
```

Алгоритм 5. Функция work для примера скалярного произведения
Algorithm 5. Work function for dot product instance

Наконец, функция Reduce (алгоритм 6) получает массив значений. Входные значения получаются либо в результате выполнения функции Work, либо в результате другого выполнения функции Reduce в непосредственно подчиненных подкомпонентах.

```
01 Reduce( arrayValues ) {
02    for v in arrayValues {
03       result += arrayValues[i]
04    }
05 }
```

Алгоритм 6. Функция reduce для примера скалярного произведения
Algorithm 6. Reduce function for dot product instance

5. Экспериментальный анализ

В этом разделе приводятся значения параметров g и L, полученные для разных архитектур с использованием предложенного бенчмарка. Эти значения будут использованы позже при валидации алгоритма, разработанного с использованием нашей системы, на основе сравнения реального времени выполнения и расчетного времени, сообщенного моделью.

5.1 Архитектуры, использованные в экспериментальном анализе

Для описанных экспериментов особенно важны иерархические уровни рассматриваемых архитектур. Основные цели экспериментального анализа состоят в том, чтобы проверить, соответствуют ли вычисленные значения параметров Multi-BSP теоретическим значениям.

Для экспериментального анализа были выбрано три реальных многоядерных инфраструктуры с достаточно большим числом ядер и интересными уровнями кэша.

- Первым образцом является dell32, архитектура которого показана на рис. 6 (диаграмма получена путем применения hwloc). В dell32 имеются четыре процессора AMD Opteron 6128 Magny-Cours всего с 32 ядрами, 64 Гб основной памяти и два уровня иерархии.

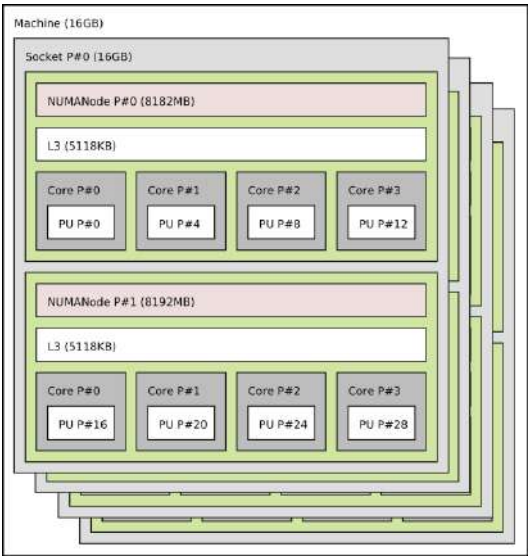


Рис. 6. Вывод hwloc, описывающий топологию многоядерного компьютера dell32
Fig. 6. hwloc output describing the topology of the dell32 multicore computer

- Образец #2 – jolly, архитектура которого показана на рис. 7 (диаграмма получена путем применения hwloc). В jolly имеются четыре процессора AMD Opteron 6272 Interlagos процессоры всего с 64 ядрами, 128 Гб основной памяти и три уровня иерархии.

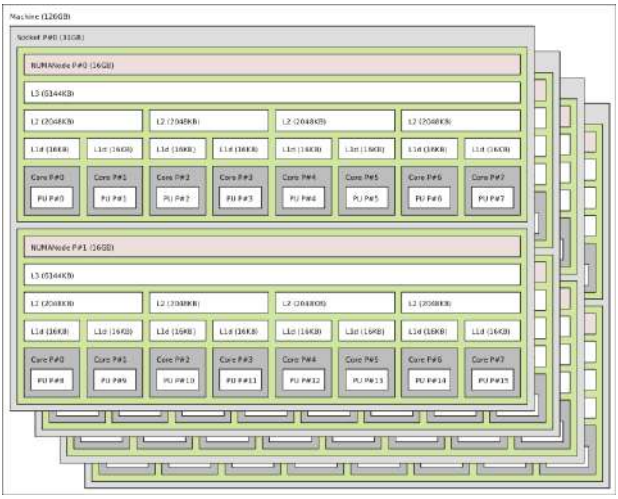


Рис. 7. Вывод hwloc, описывающий топологию многоядерного компьютера jolly
Fig. 7. hwloc output describing the topology of the jolly multicore computer

- Образец #3: узел XeonPhi в высокопроизводительной вычислительной платформе Cluster FING Республиканского университета [6]. У Xeon Phi 60 ядер, 8 Гб основной памяти, кэш L2 – 512 Кб и кэш L1 – 32 Кб. У каждого ядра имеются четыре процессорных блока для гиперпотоковой обработки, в результате чего общее число физических потоков составляет 240. Архитектура узла XeonPhi представлена на рис. 8

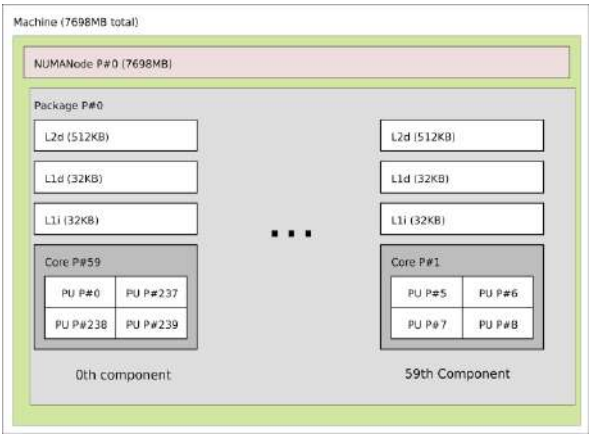


Рис. 8. Вывод hwloc, описывающий топологию сопроцессора XeonPhi
Fig. 8. hwloc output describing the topology of the XeonPhi co-processor

Для каждой целевой архитектуры на первом этапе необходимо определить соответствующие экземпляры в модели Multi-BSP. Для лучшего понимания состава Multi-BSP дальнейшее описание продвигается шаг за шагом в процессе построения спецификации.

Процедура создания спецификации для компьютера dell32 продвигается с нижнего уровня (ядра) к верхним уровням и создает кортежи компонентов, совместно использующих пространство памяти. Первый кортеж состоит из одного ядра на уровне 0. Это ядро не разделяет какую-либо память с каким-либо другим компонентом, поэтому объем его совместно используемой памяти равен 0, и оба параметра g и L равны нулю по определению: $\text{tuple}_0 = <p_0 = 1, g_0 = 0, L_0 = 0, m_0 = 0>$. Что касается следующего уровня, четыре базовых компонента уровня 0 совместно используют кэш-память L3 размером 5 МБ, образуя новый компонент Multi-BSP уровня 1. Этот новый компонент формально описывается кортежем $\text{tuple}_1 = <p_1 = 4, g_1, L_1, m_1 = 5$ МБ>. Наконец, все восемь компонентов уровня 1 совместно используют оперативную память объемом 64 ГБ, образуя следующий и последний уровень 2 в спецификации Multi-BSP. Этот формально описывается как $\text{tuple}_2 = <p_2 = 8, g_2, L_2, m_2 = 64$ ГБ>.

Заключительный шаг состоит в соединение всех кортежей в последовательность для получения полной спецификации машины Multi- BSP с отбрасыванием нулевого уровня, так как значения g_0 и L_0 известны по определению. Тогда архитектура образца #1 описывается соотношением (16).

$$M_1 = [< p_1 = 4, g_1, L_1, m_1 = 5\,Mb >, < p_2 = 8, g_2, L_2, m_2 = 64\,Gb >] \quad (16)$$

С использованием той же процедуры создается спецификация Multi-BSP для экземпляра #2. Опять же, уровень 0 описывается как $\text{tuple}_0 = <p_0 = 1, g_0 = 0, L_0 = 0, m_0 = 0>$. Уровень 0 имеет одинаковую спецификацию на всех машинах за исключением ядер, в которых используется технология гиперпоточности (в этом случае требуется дополнительный уровень для спецификации физических потоков).

Далее, имеются два компонента, разделяющие кэш L2 размером в 2 Мб. Первый уровень описывается кортежем $\text{tuple}_1 = <p_1 = 2, g_1, L_1, m_1 = 2$ МБ>. Компоненты первого уровня совместно используют четыре кэш-памяти L3 размером в 6 MB, образуя второй уровень, который описывается кортежем $\text{tuple}_2 = <p_2 = 4, g_2, L_2, m_2 = 6$ MB>. На последнем уровне группируются восемь компонентов второго уровня. Они разделяют основную память объемом в 128 GB. Третий уровень описывается кортежем $\text{tuple}_3 = <p_3 = 8, g_3, L_3, m_3 = 128$ GB>.

Подобно спецификации для dell32, окончательной спецификацией экземпляра MultiBSP для jolly является соотношение (17).

$$M_1 = [< p_1 = 2, g_1, L_1, m_1 = 2\ Mb >, < p_2 = 4, g_2, L_2, m_2 = 6\ Mb >, < p_3 = 8, g_3, L_3, m_3 = 128\ Gb >] \quad (17)$$

Третьей архитектурой является сопроцессор XeonPhi. С применением той же процедуры на нижнем уровне идентифицируются процессорные блоки, и они включаются в уровень 0. Как и в других архитектурах, процессорные блоки вообще не разделяют память, и определением этого уровня является $\text{tuple}_0 = <p_0 = 1, g_0 = 0, L_0 = 0, m_0 = 0>$. Затем, четыре компонента нулевого уровня разделяют кэш-память L2размером в 512 Kb. Так что первый уровень описывается как $\text{tuple}_1 = <p_1 = 4, g_1, L_1, m_1 = 512$ Kb>. Наконец, как показывает рис. 8, последнему уровню соответствует $\text{tuple}_2 = <p_2 = 60, g_2, L_2, m_2 = 7698$ Mb>.

Вышеупомянутые экземпляры модели Multi-BSP применяются в этой статье для прогнозирования времени работы алгоритма Multi-BSP, выполняемого на каждом компьютере. Параметры g_i и L_i в каждом кортеже должны быть предварительно рассчитаны с использованием процедуры эталонного тестирования, описанной в предыдущем разделе. В следующем подразделе приводятся значения g и L, полученные для всех архитектур на каждом уровне.

5.2. Результаты производительности исследованных архитектур

Эксперименты с производительностью ориентированы на определение времени выполнения простого алгоритма, разработанного и реализованного с использованием предложенной системы поддержки Multi-BSP. Таким образом, в этом подразделе приводится время выполнения *h*-коммуникаций на каждом уровне с увеличением числа *h* в соответствии с правилами функции *coreBenchmark*.

Полученные результаты представлены на рис. 9-11. Рис. 9 показывает *h*-коммуникации на каждом уровне для dell32 (уровни один и два). Рис. 10 демонстрирует аналогичные результаты для jolly (первый, второй и третий уровни). Рис. 11 показывает *h*-коммуникации на каждом уровне для Xeon Phi.

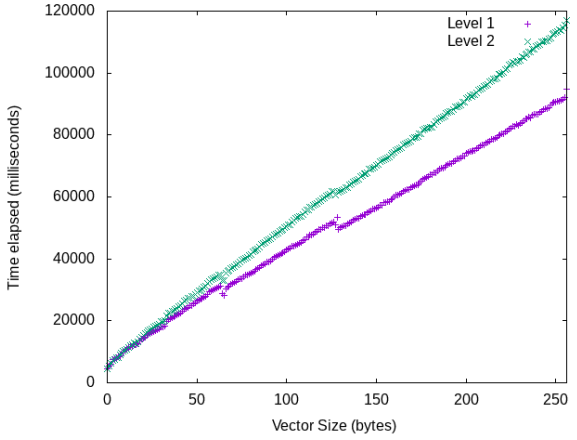


Рис. 9. Время h-коммуникаций в dell32
Fig. 9. Time for h-communications in dell32

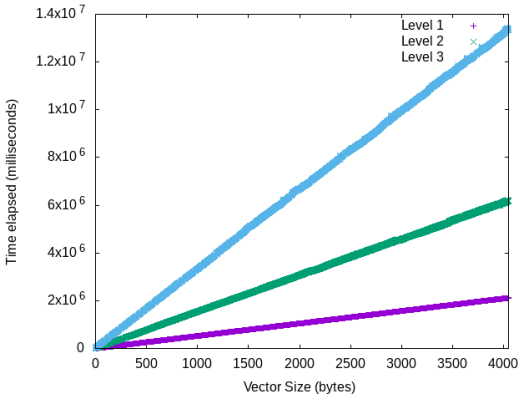


Рис. 10. Время h-коммуникаций в jolly
Fig. 10. Time for h-communications in jolly

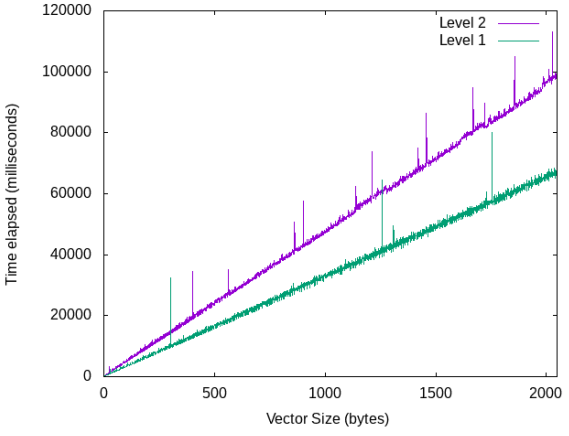


Рис. 11. Время h-коммуникаций в Xeon Phi
Fig. 11. Time for h-communications in Xeon Phi

В dell32 все коммуникации уровня 1 выполняются через общую память (кэш L3), поэтому они в два раза быстрее, чем на уровне 2, в котором используется основная память. В jolly коммуникации на уровне 1 выполняются через кеш L2, поэтому они в три раза быстрее, чем на уровне 2, где для этого используется кэш L3. В свою очередь, коммуникации на уровне 2 в 1,5 раза быстрее, чем на уровне 3, которые выполняются путем доступа к основной памяти.

Наконец, для определения значений g_i и L_i в *h*-коммуникациях для каждого уровня применяется метод наименьших квадратов. Окончательные значения для dell32, jolly и Xeon Phi представлены в табл. 1.

Табл. 1. Результирующие значения параметров g и L по уровням для dell32, jolly и Xeon Phi
Table 1. Results of g and L parameters per level for dell32, jolly and Xeon Phi

	dell 32		***jolly***			***Xeon phi***	
Level	***2***	***1***	***3***	***2***	***1***	***2***	***1***
g	977.5	334.9	1315.9	549.9	105.3	2470.1	1947.9
L	15550.2	7792.9	16184.4	7157.9	498.2	1380955.3	1322578.2

5.3 Анализ примера со скалярным произведением

Для проверки результатов, описанных в предыдущем подразделе, был проведен эксперимент с использованием алгоритма вычисления скалярного произведения, реализованного на основе системы поддержки MultiBSP. Процесс проверки включает в себя следующие этапы (применяются для разных размеров вектора):

1) оценить объем коммуникаций и синхронизации на каждом уровне, используя аппаратные счетчики;
2) вычислить значения параметров gi и Li, используя разработанный бенчмарк;
3) вычислить время исполнения алгоритма, используя теоретическую оценочную модель для мульти- BSP в виде, представленном в [10];
4) выполнить алгоритм вычисления скалярного произведения;
5) сравнить время выполнения алгоритма скалярного произведения с теоретическим предсказанным временем.

На рис. 12-14 показано сравнение теоретически оцененных затрат с реальными затратами на коммуникации и синхронизацию при выполнении алгоритма скалярного произведения, реализованного на основе системы поддержки MultiBSP. На рисунках показано время выполнения алгоритма скалярного произведения с использованием предложенного механизма MBSP в сравнении с временем, рассчитанным на основе теоретической модели, с учетом возрастающего размера входных данных.

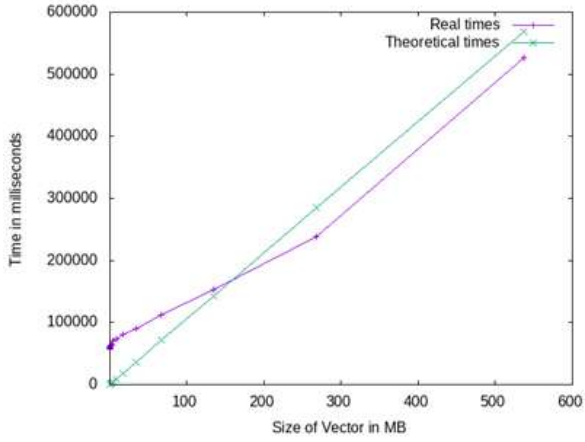


Рис. 12. Сравнение теоретически оцененных и реальных затрат для компьютера dell32
Fig. 12. Theoretical vs real cost for the dell32 computer

Результаты на рис. 12-14 показывают точность предсказанного времени по сравнению с реальным временем. Относительные погрешности составляют от 0% до 7%. В dell32 средняя ошибка составляет 6%, а максимальная ошибка – 9%. В jolly средняя ошибка составляет 7%, а максимальная ошибка прогнозируемого времени – 17%. Наилучшие результаты были получены для Xeon Phi, для которого средняя ошибка составляет всего 2%, а максимальная ошибка – 5%. Эти результаты показывают, что теоретическая оценка времени выполнения алгоритма скалярного произведения является достаточно точной по отношению к реальному времени для всех исследованных архитектур.

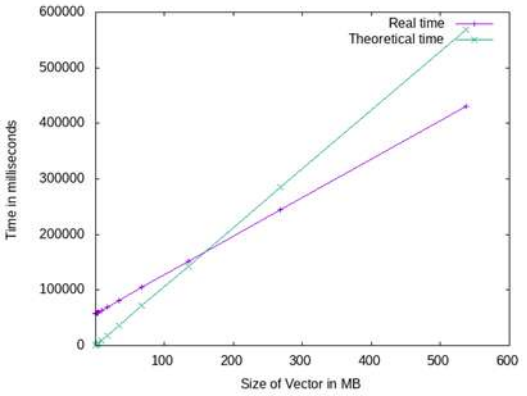


Рис. 13. Сравнение теоретически оцененных и реальных затрат для компьютера jolly
Fig. 12. Theoretical vs real cost for the dell32 computer

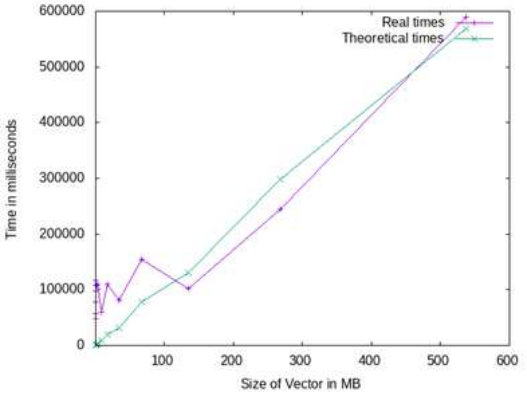


Рис. 14. Сравнение теоретически оцененных и реальных затрат для сопроцессора Xeon Phi
Fig. 14. Theoretical vs real cost for the Xeon Phi co-processor

6. Заключение и планы на будущее

В этой статье предложен упрощенный подход к разработке и реализации алгоритмов с использованием модели MultiBSP.

Предложенный подход включает методологию для автоматического обнаружения аппаратных особенностей данного компьютера и систему поддержки для разработки и реализации параллельных алгоритмов на основе обобщенной процедуры спецификации. Следуя этому подходу, при программировании не нужно сосредотачиваться на конкретных деталях реализации и эталонного тестирования MultiBSP, которое включены в предлагаемую систему. Программист стимулируется к разработке алгоритмов MultiBSP с использованием общей спецификации, основанной на рекурсивной стратегии «разделяй и властвуй», действующей над компонентами архитектуры (то есть над ядрами, кэшем и оперативной памятью).

Также представлена реализация бенчмарка MultiBSP для выявления характеристик используемых архитектур. Этот бенчмарк применяется в нашей системе, в который также используется процесс обнаружения для выполнения алгоритмов MultiBSP, позволяющий скрыть от программиста все детали разделения данных и закрепления потоков.

Валидация выполненных реализаций была произведена на трех современных высокопроизводительных архитектурах. Был построен и исследован частный случай

использования разработанной системы для решения декомпозируемой задачи – алгоритм вычисления скалярного произведения векторов.

Этот примерный алгоритм использовался для сравнения теоретического времени выполнения, оцененного с использованием модели стоимости MultiBSP, и реального времени выполнения реализации алгоритма скалярного произведения на основе разработанной системы. Результаты теоретической оценки оказались достаточно точными: средняя относительная погрешность составила от 2% до 7%. Наилучшие результаты были получены для Xeon Phi, для которого средняя ошибка составила всего 2%, а максимальная ошибка – 5%.

Предложенная методология обеспечивает основу для разработки пригодного для практического использования фреймворка, включающего набор инструментов для разработки, реализации и выполнения алгоритмов MultiBSP, а также точного прогнозирования времени их выполнения.

Основные направления будущих исследований связаны с расширением анализа предлагаемой методологии, например, путем изучения возможностей системы поддержки MultiBSP с использованием новых, более сложных алгоритмов. Систему можно расширить для решения недекомпозируемых задач, используя преимущества его модульной организации и учитывая знания о задачах, поставляемые пользователями (т.е. система может автоматически определять соответствие потоков, обеспечивать параллельное выполнение и локальность данных для функции разделения, задаваемой пользователем). Процесс обнаружения параметров аппаратного обеспечения может быть расширен дополнительными уровнями, включая обнаружение характеристик сети с использованием специальных программных библиотек и определение соответствия и локальности данных с учетом скорости и пропускной способности сети.

Список литературы / References

[1] Alaniz M., Nesmachnow S., Goglin B., Iturriaga S., Gil Costa V., Printista M. MBSPDiscover: An automatic benchmark for MultiBSP performance analysis. Communications in Computer and Information Science; vol. 485, 2014, pp, 158–172.

[2] Bisseling R. Parallel scientific computation: a structured approach using BSP and MPI. Oxford University Press, 2004, 334 p.

[3] Bonorden O., Juurlink B., von Otte I., Rieping I. The Paderborn University BSP (PUB) Library. Parallel Computing, vol. 29, no. 2, 2003, pp. 187–207.

[4] Broquedis F., Clet-Ortega J., Moreaud S., Furmento N., Goglin B., Mercier G., Thibault S., Namyst R. Hwloc: A generic framework for managing hardware affinities in HPC applications. In Proc. of the 18th Euromicro Conference on Parallel, Distributed and Network-based Processing, 2010, pp. 180–186.

[5] Hill J., McColl B., Stefanescu D., Goudreau M., Lang K., Rao S., Suel T., Tsantilas T., Bisseling R. BSPlib: The BSP programming library. Parallel Computing, vol. 24, no. 14, 1998, pp. 1947–1980.

[6] Nesmachnow S. Computación científica de alto desempeño en la Facultad de Ingeniería, Universidad de la República. Revista de la Asociación de Ingenieros del Uruguay, vol. 61, no. 1, 2010, pp. 12-15 (In Spanish).

[7] Savadi A., Deldari H. Measurement latency parameters of the MultiBSP model: A multicore benchmarking approach. Journal of Supercomputing, vol. 67, no. 2, 2014, pp. 565–584.

[8] Soudris D., Jantsch A. (eds.). Scalable Multi-core Architectures: Design Methodologies and Tools. Springer Publishing Company, 2011, 223 p.

[9] Valiant L. A bridging model for parallel computation. Communications of the ACM, vol. 33, no. 8, 1990, pp. 103–111.

[10] Valiant, L. A bridging model for multi-core computing. Journal of Computing and System Sciences, vol. 77, no. 1, 2011, pp. 154–166.

[11] Yzelman, A. Fast sparse matrix-vector multiplication by partitioning and reordering. Ph.D. thesis, Utrecht University, Utrecht, the Netherlands, 2011, 136 p.

[12] Yzelman A., Bisseling R., Roose D., and Meerbergen K. MulticoreBSP for C: A High-Performance Library for Shared-Memory Parallel Programming. International Journal of Parallel Programming, vol. 42, no. 4, 2014, pp. 619-642.

Информация об авторах / Information about authors

Марсело Аланис работает исследователем Вычислительном центре Института компьютерных наук Инженерного факультета Республиканского университета.

Marcelo Alaniz is a researcher at the Numerical Center (CeCal) at Computer Science Institute, Engineering Faculty.

Серджо Энрике НЕСМАЧНОВ КАНОВАС обладает степенью PhD в области компьютерных наук, полученной в Республиканском университете, Уругвай. В настоящее время он занимает должность профессора в Вычислительном центре Института компьютерных наук Инженерного факультета Республиканского университета. Основные научные интересы: параллельные и распределенные вычисления, научные вычисления, эволюционные алгоритмы и метаэвристика, а также численные методы.

Sergio Enrique NESMACHNOW CÁNOVAS has a Ph.D. degree in Computer Science from Universidad de la República, Uruguay. He currently holds an Aggregate Professor position in the Numerical Center (CeCal) at Computer Science Institute, Engineering Faculty. His main research interests are parallel and distributed computing, scientific computing, evolutionary algorithms and metaheuristics, and numerical methods.

DOI: 10.15514/ISPRAS-2019-31(2)-9

Ориентированное на данные планирование с применением отказоустойчивого метода динамической кластеризации для поддержки потоков научных работ в облаках

З. Ахмад, ORCID: 0000-0002-4787-1511 <zulfiqarahmad@hu.edu.pk>
А.И. Джехангири, ORCID: 0000-0001-5920-433X <ali_imran@hu.edu.pk>
М. Ифтихар, ORCID: 0000-0002-7053-2040 <mehreeniftikhar@hu.edu.pk>
А.И. Умар, ORCID: 0000-0002-4148-5062 <arifiqbalumar@yahoo.com>
И. Афзал, ORCID: 0000-0002-3565-1319 <ibrar@hu.edu.pk>

Факультет информационных технологий, Университет Хазары, Мансехра, Пакистан

Аннотация. Облачные вычисления – одна из наиболее распространенных парадигм параллельных и распределенных вычислений. Они используются для поддержки огромного количества научных и бизнес-приложений. В частности, на основе облачных вычислений могут выполняться крупномасштабные научные приложения, которые организованы как потоки научных работ. Потоки научных работ являются приложениями, интенсивно использующими данные, поскольку один поток научных работ может состоять из сотен тысяч задач. Дополнительные затруднения могут вызываться сбоями при выполнении задач, ограничениями по срокам, бюджетными ограничениями и неправильным управлением задачами. Поэтому обеспечение отказоустойчивых методов с использованием ориентированного на данные планирования является важным подходом для поддержки выполнения потоков научных работ в облачных средах. В этой статье мы представляем усовершенствованный механизм планирования, ориентированного на данные, с использованием отказоустойчивой техники динамической кластеризации (EDS-DC) подходом для поддержки выполнения потоков научных работ в облачных средах. Для оценки эффективности EDS-DC, мы сравниваем его результаты с тремя хорошо известными политиками эвристического планирования: (a) MCT-DC, (b) Max-min-DC и (c) Min-min-DC. В качестве примера мы рассматриваем поток научных работ CyberShake, потому что он обладает большинством характеристик потоков научных работ, таких как интеграция, дезинтеграция, параллелизм и конвейеризация. Результаты показывают, что EDS-DC позволил сократить время цикла обработки на 10,9% по сравнению с MCT-DC, на 13,7% по сравнению с Max-min-DC и на 6,4% по сравнению с политикой планирования Min-min-DC. Аналогично, EDS-DC позволил снизить стоимость на 4% по сравнению с MCT-DC, на 5,6% по сравнению с Max-min-DC и на 1,5% по сравнению с политиками планирования Min-min-DC. При использовании EDS-DC по отношению к временным и стоимостным ограничениям не нарушается SLA, в то время как оно нарушается несколько раз при применении политик планирования MCT-DC, Max-min-DC и Min-min-DC.

Ключевые слова: потоки научных работ; отказоустойчивость; планирование потоков работ; cybershake; ориентация на данные

Для цитирования: Ахмад З., Джехангири А.И., Ифтихар М., Умер А.И., Афзал И. Ориентированное на данные планирование с применением отказоустойчивого метода динамической кластеризации для поддержки потоков научных работ в облаках. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 121-136. DOI: 10.15514/ISPRAS-2019-31(2)-9

Data-Oriented scheduling with Dynamic-Clustering fault-tolerant technique for Scientific Workflows in Clouds

Z. Ahmad, ORCID: 0000-0002-4787-1511 <zulfiqarahmad@hu.edu.pk>
A.I. Jehangiri, ORCID: 0000-0001-5920-433X <ali_imran@hu.edu.pk>
M. Iftikhar, ORCID: 0000-0002-7053-2040 <mehreeniftikhar@hu.edu.pk>
A.I. Umer, ORCID: 0000-0002-4148-5062 <arifiqbalumar@yahoo.com>
I. Afzal, ORCID: 0000-0002-3565-1319 <ibrar@hu.edu.pk>
Department of Information Technology, Hazara University, Mansehra, KPK, Pakistan

Abstract. Cloud computing is one of the most prominent parallel and distributed computing paradigm. It is used for providing solution to a huge number of scientific and business applications. Large scale scientific applications which are structured as scientific workflows are evaluated through cloud computing. Scientific workflows are data-intensive applications, as a single scientific workflow may consist of hundred thousands of tasks. Task failures, deadline constraints, budget constraints and improper management of tasks can also instigate inconvenience. Therefore, provision of fault-tolerant techniques with data-oriented scheduling is an important approach for execution of scientific workflows in Cloud computing. Accordingly, we have presented enhanced data-oriented scheduling with Dynamic-clustering fault-tolerant technique (EDS-DC) for execution of scientific workflows in Cloud computing. We have presented data-oriented scheduling as a proposed scheduling technique. We have also equipped EDS-DC with Dynamic-clustering fault-tolerant technique. To know the effectiveness of EDS-DC, we compared its results with three well-known enhanced heuristic scheduling policies referred to as: (a) MCT-DC, (b) Max-min-DC, and (c) Min-min-DC. We considered scientific workflow of CyberShake as a case study, because it contains most of the characteristics of scientific workflows such as integration, disintegration, parallelism, and pipelining. The results show that EDS-DC reduced make-span of 10.9% as compared to MCT-DC, 13.7% as compared to Max-min-DC, and 6.4% as compared to Min-min-DC scheduling policies. Similarly, EDS-DC reduced the cost of 4% as compared to MCT-DC, 5.6% as compared to Max-min-DC, and 1.5% as compared to Min-min-DC scheduling policies. These results in respect of make-span and cost are highly significant for EDS-DC as compared with above referred three scheduling policies. The SLA is not violated for EDS-DC in respect of time and cost constraints, while it is violated number of times for MCT-DC, Max-min-DC, and Min-min-DC scheduling techniques.

Keywords*:* scientific workflows; fault-tolerant; workflows scheduling; cybershake; data-oriented

For citation: Ahmad Z., Jehangiri A.I., Iftikhar M., Umer A.I., Afzal I. Data-Oriented scheduling with Dynamic-Clustering fault-tolerant technique for Scientific Workflows in Clouds. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 121-136 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-9

1. Введение

Облачные вычисления – это универсальная и масштабная парадигма распределенных вычислений. Облачная среда предполагает наличие пула настраиваемых и реконфигурируемых, виртуализированных, абстрагированных и динамически доступных вычислительных услуг и ресурсов [35]. Услуги и ресурсы, предоставляемые облачными вычислениями в подписных средах, формируются в форме: (a) серверов, (b) хранилищ данных, (c) средств обработки и (d) приложений [1]. Кроме того, облачные сервисы и ресурсы обладают высоким уровнем масштабируемости и предоставляются внешним клиентам с архитектурой, включающих три сегментов, а именно: инфраструктура как услуга (Infrastructure as a Service, IaaS), платформа как услуга (Platform as a Service, PaaS) и программное обеспечение как услуга (Software as a Service, SaaS). Многие организации переходят на облачные сервисы для повышения своей эффективности [2] [3] [36] [39].

Упрощенно можно считать, что облачные сервисы и ресурсы ориентированы на подержку деловых и научных приложений. Научные приложения, связанные с объемными вычислениями и хранимыми данными, организуются как потоки научных работ [4]. В потоках научных работ для решения каждой задачи требуется значительный объем

вычислений и памяти, и, таким образом, сбой даже одной задачи наносит значительный ущерб всей системе [5] [38] [42].

Научные приложения, в частности, относятся к областям науки о землетрясениях, астрономии, биологии и гравитационной физики [6]. CyberShake [7] является потоком научных работ в реальном времени, связанным с сейсмологией (наукой о землетрясениях). В потоке научных работ CyberShake сейсмические опасности для конкретного местоположения количественно оцениваются сейсмологом с помощью вероятностного анализа сейсмической опасности (probabilistic seismic hazard analysis, PSHA). В PSHA предусмотрен механизм для оценки вероятности уровней движения грунта при землетрясении в конкретном месте и в течение оговоренного периода времени с применением меры интенсивности (intensity measure, IM) – пиковая скорость или пиковое ускорение движения грунта. Эти вероятностные меры полезны для инженеров-строителей, градостроителей и страховых агентств, поскольку они влияют на эффективность затрат в миллиарды долларов каждый год. CyberShake требует разумного хранения данных и соответствующих вычислительных ресурсов [8]. Облачные вычисления обеспечивают повсеместную доступность и неограниченность ресурсов с приемлемой ценой в среде, в которой ресурсы получаются и освобождаются динамически. Поэтому для поддержки потоков научных работ облачная среда является одной из лучших платформ [9] [10] [11].

Когда поток научных работ, такой как CyberShake, выполняется в реальном времени, требуется решить несколько проблем.

- Предположим, что в потоке научных работ имеются задачи A_1, A_2, A_3,…, A_n, которые выполняются на нескольких уровнях B_1, B_2, B_3,…, B_n на ресурсах C_1, C_2, C_3,…, C_n.
- Несколько задач из A_1, A_2, A_3,…, A_n выполняются в критическом режиме, или на критическом уровне, и их отказ делает выполнение всего потока работ бесполезным; следовательно, требуется отказоустойчивая техника.
- На каждом уровне существует несколько задач, и иногда у них имеются одинаковые требования к услугам и ресурсам, и поэтому для такого выполнения очень полезен отказоустойчивый механизм кластеризации [40].
- Предположим, что для каждой задачи имеется заранее установленное время передачи данных каждому ресурсу. В потоке научных работ есть несколько задач из A_1, A_2, A_3,…, A_n с различными потребностями в ресурсах из C_1, C_2, C_3,…, C_n на нескольких уровнях B_1, B_2, B_3,…, B_n. Таким образом, требуется эффективная политика планирования, ориентированного на данные.

В своей работе мы последовательно исследуем и решаем отмеченные проблемы применительно к выполнения потоков научных работ в облачных средах. Для этого мы усовершенствовали ориентированное на данные планирование потоков научных работ с применением отказоустойчивого метода динамической. В качестве параметров оценки мы рассматривали время, стоимость, сроки, бюджет и нарушение SLA [12]. Работа нацелена на то, чтобы ответить на основной вопрос, который волнует исследователей: насколько будет улучшена производительность, если мы будем совместно использовать ориентированное на данные планирование и отказоустойчивую технику для организации потоков научных работ в облаках?

Основные результаты нашей работы состоят в следующем.

- Мы предложили усовершенствованное ориентированное на данные планирование потоков научных работ в облаках с применением отказоустойчивого метода динамической кластеризации (Enhanced Data-oriented Scheduling with Dynamic-Clustering fault-tolerant technique, EDS-DC) [13].
- Чтобы оценить эффективность EDS-DC, мы сравнили его результаты с результатами трех хорошо известных политик планирования: (a) Minimum-Completion-Time-Dynamic-Clustering (MCT-DC) [16], (b) Maximum-minimum-Dynamic-Clustering (Max-min-DC) [17] и (c) Minimum-minimum-Dynamic-clustering (Min-min-DC) [17].

- Для оценки эффективности EDS-DC, мы провели симуляцию с использованием WorkflowSim [18] и предоставили патч для выполнения этой симуляции.
- В качестве примера мы выполнили поток научных работ реального времени CyberShake [7] с 30, 50, 100 и 1000 задачами. Результаты моделирования показывают, что наш подход превосходит существующий решения.

Оставшаяся часть статьи организована следующим образом: обзор родственных работ представлен в разд. 2. Модель и схема решения описываются в разд. 3, эксперименты и результаты обсуждаются в разд. 4, и, наконец, разд. 5 завершает работу.

2. Родственные работы

Мы подробно изучили родственные работы, касающиеся выполнения потоков научных работ, отказоустойчивых методов и механизмов планирования потоков научных работ. Мы также обнаружили методы отказоустойчивой кластеризации и различные типы политики планирования, ориентированного на данные, применяемые именно в потоках научных работ.

С самого начала было проведено исследование пяти реалистичных потоках научных работ из различных научных приложений [6]. Были изучены структуры, данные и вычислительные требования каждого из этих потоках научных работ. На рис. 1 представлена структура небольшого экземпляра каждого потока научных работ, Рисунок показывает, что основные компоненты потоков работ обладают различными структурными и функциональными свойства: применение конвейера, параллелизм по данным, агрегирование данных, распределение, перераспределение данных и их композиция.

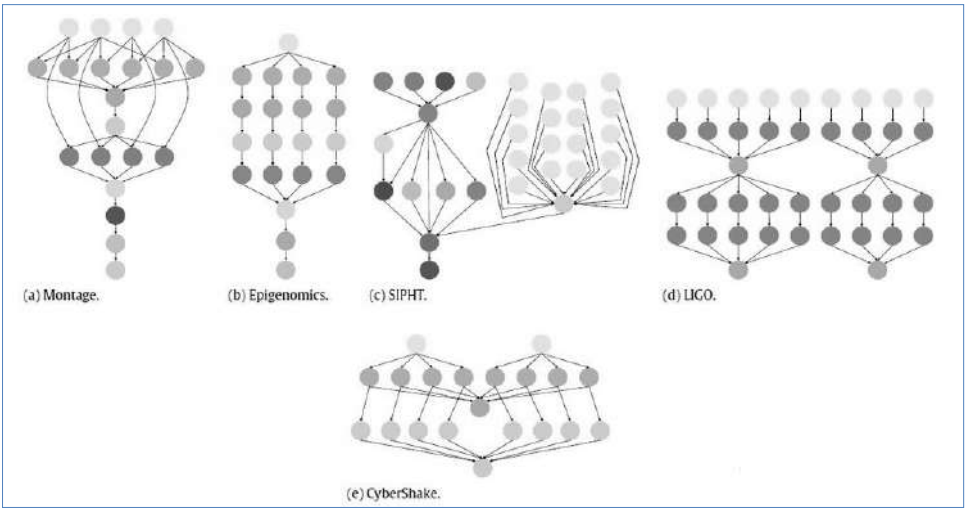


Рис. 1. Общее представление пяти реалистичных потоков научных работ
Fig. 1: An overview of THE five realistic scientific workflows

Большое количество научных приложений, таких как картирование генома, моделирование в физике высоких энергий и моделирование климата [19], являются приложениями, интенсивно использующими данные, и для них требуется планирование с учетом данных [14] [43]. Stork [19] является планировщиком, учитывающим данные, он был специально разработан для учета передачи данных, выделения памяти, удаления данных, освобождения памяти и регистрации метаданных, связанных с традиционными методами планирования. Для учета времени завершения рабочего процесса и использования ресурсов в [20] был предложен метод планирования Adaptive Data Aware Scheduling (ADAS).

Планировщик является основным компонентом, поддерживающим выполнения потоков работ, и его возможностями нельзя пренебрегать на любой стадии выполнения. Поэтому в

[21] был предложен алгоритм планирования для выполнения потока работ под названием «Отказоустойчивое планирование потоков работ с использованием спот-инстансов в облаках» (Fault-Tolerant Workflow Scheduling, FTWS), который является устойчивым к изменениям производительности.

У облачных сред имеются три основные особенности: (а) предоставление ресурсов по требованию, (б) согласованная пропускная способность между сервиса, предоставляемыми облачными поставщиками услуг и (в) модель ценообразования с оплатой по мере использования в различных коммерческих облачных средах [22]. Поэтому с учетом этих особенностей в [9] были предложены два новых алгоритма планирования потоков работ для облаков категории IaaS: IaaS Cloud-Partial Critical Path (IC-PCP) и IaaS Cloud-Partial Critical Path with Deadline Distribution (IC-PCPD2). Эти алгоритмы предназначены для создания расписаний, которые удовлетворяют заданным пользователями срокам, а также сводят к минимуму стоимость выполнения.

Три алгоритма планирования для групп потоков работ были предложены в [23]: Dynamic Provisioning Dynamic Scheduling (DPDS), Workflow Aware DPDS(WA-DPDS) и Static Provisioning Static Scheduling (SPSS). В этих алгоритмах учитываются только ограничения на время выполнения и расходы. Имеется несколько эвристических подходов, таких как (a) Minimum Completion Time (MCT) [24], (b) Maximum-minimum (Max-min) [25] и (c) Minimum-minimum (Min-min) [26], которые также использовались для планирования независимых задачи при выполнении потоков научных работ [16].

Что касается отказоустойчивых методов, эффективным и простым отказоустойчивым методом является повторное выполнение задач [27]: аварийно завершенная задача повторно выполняется либо на тех же ресурсах, либо на других доступных ресурсах [28]. Механизм кластеризации Fault-Tolerant Clustering (FTC) для потоков научных работ был представлен в [15]. В работе описаны три отказоустойчивых метода кластеризации: Dynamic-Clustering (DC), Selective Re-Clustering (SR) и Dynamic Re-Clustering (DR). Эти алгоритмы несовершенны по параметрам стоимости и времени.

The brief comparison of literature review is shown in Table 1.

Краткое сравнение особенностей рассмотренных подходов приведено в таблице 1.

Табл. 1. Сравнение результатов родственных работ
Table 1: Comparison of Related Work

Ссылка	**Политика планирования**	**Механизм отказоустойчивости**	**Управление ресурсами**	**Качество обслуживания (QoS)**	
				Время	**Стоимость**
[29]	Pegasus WMS	✖	✓	✖	✖
[20]	ADAS	✖	✓	✓	✖
[21]	FTWS	Контрольные точки	✓	✖	✓
[15]	✖	FTC	✓	✖	✖
[30]	WSA	✖	✓	✓	✖
[31]	BTC	✖	✓	✓	✖
[9]	IC-PCP & IC-PCPD2	✖	✓	✓	✓
[23]	DPDS, WA-DPDS & SPSS	✖	✓	✓	✓
[27]	✖	Перезапуск задач	✖	✖	✖

Ссылка	**Особенности**	**Ограничения**
[29]	Обеспечивает структуру WMS	Отсутствует механизм QoS
[20]	Улучшает показатель времени завершения потока работ	Отсутствует метод отказоустойчивости
[21]	Используются две ценовые модели: спот-инстансы и инстансы по запросу	Отсутствует метод сокращения времени цикла обработки как показателя QoS
[15]	Обеспечиваются три	Отсутствует планирование с учетом параметров

	метода поддержки отказоустойчивости: DC, SRC & DRC	стоимости и времени
[30]	Используется механизм набора маркеров (token bucket) для сокращения времени выполнения	Отсутствует механизм отказоустойчивости
[31]	Обеспечивается метод балансировки нагрузки	Накладные расходы на анализ показателей и зависимостей
[9]	Задачи планируются с учетом ограничений времени, задаваемых пользователями	Работает только в пределах IaaS
[23]	Обеспечивает ресурсы для групп потоков работ	Пригоден только для групп потоков работ
[27]	Обеспечивает гибридный механизм поддержки отказоустойчивости	Отсутствует метод учета QoS

3. Схема и прототип системы

Мы разработали усовершенствованный планировщик потоков научных работ, ориентированный на данные и использующий отказоустойчивую технику динамической кластеризации [15] (EDS-DC). Планирование в EDS-DC ориентировано на данные [14], но в качестве параметров оценки мы используем (a) время, (b) стоимость, (c) бюджет, (d) крайний срок и (d) нарушение SLA [32].

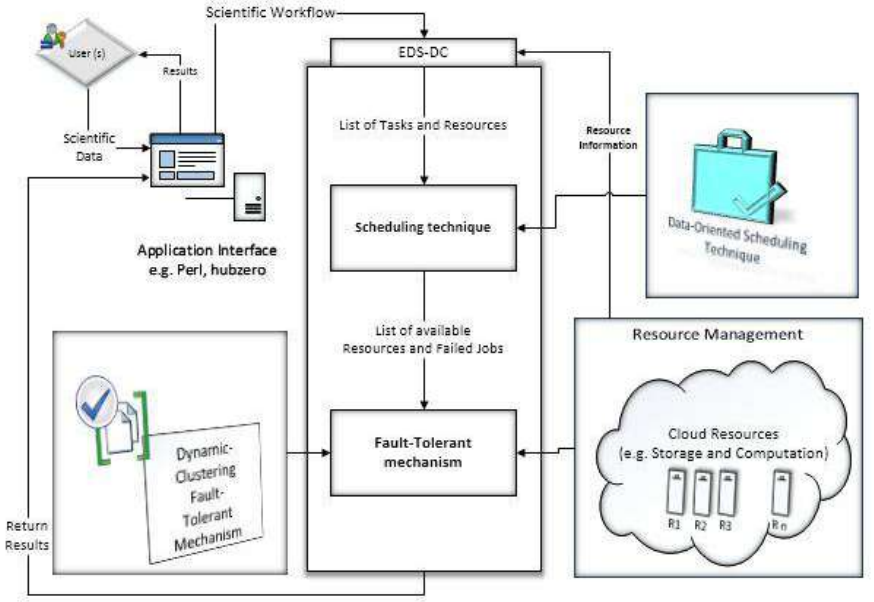


Рис. 2. Архитектура прототипа EDS-DC
Fig 2: An overview of EDS-DC Model

Чтобы оценить эффективность EDS-DC, мы сравнили его результаты с тремя хорошо известными эвристическими политиками планирования: Minimum Completion Time (MCT) [16], Max-min [17] и Min-min [17]. Для оценки эффективности EDS-DC мы провели моделирование с использованием WorkflowSim [18]. В качестве примера мы выполнили поток научных работ реального времени CyberShake [7] с 30, 50, 100 и 1000 задачами. Результаты моделирования показывают, что EDS-DC превосходит существующие решения.

Общая модель показана на рис. 2. Пользователь передает научные данные через интерфейс приложения, например, Perl или hubzero, и модель EDS-DC обрабатывает их с помощью политики планирования, ориентированной на данные, и отказоустойчивой техники динамической кластеризации. Ресурсы и услуги получаются из облачной инфраструктуры в форме IaaS. Наконец, результаты оценки возвращаются пользователю через интерфейс приложения.

3.1 Ориентированное на данные планирование в EDS-DC

Планирование потоков научных работ в EDS-DC ориентировано на данные [14] [34] [41] [44]. В планировании, ориентированном на данные, каждая задача потока научных работ назначается доступному ресурсу, для которого время передачи данных минимально. Алгоритм 1 показывает процедуру планирования, ориентированного на данные, в EDS-DC. Планировщик получает список задач $L(Tn)$, список ресурсов $L(Rn)$ и возвращает отображение списка задач $M(Tn)$ ресурсам $M(Rn)$. Каждая задача отображается на наиболее подходящий доступный ресурс с минимальным временем передачи данных.

```
      Input: L(Tn,Rn) – List of tasks and available resources
      Output: M(Tn,Rn) – Mapped list of tasks to the resources
 1.   procedure Data-Oriented Scheduling (L(Tn,Rn))
 2.      Queue ← Tn
 3.      Ri ← Rn
 4.      M(Tn,Rn) ← 0 ⊳ Mapped list of tasks to resources
                        (initially empty)
 5.      while (Queut is not empty) do
 6.         Ti ← Delete each task from Queue
 7.         for all available resources (Rn) do
 8.             find resource Ri with minimum data transfer time
 9.             for task Ti
10.         end for
11.         M(Tn,Rn) ← M(Tn,Rn) + M(Ti,Ri) ⊳ Mapped and submit to
                                               list
12       end while
13.      return M(Tn,Rn)                  ⊳ The output is M(Tn,Rn)
14.   end procedure
```

Алгоритм 1. Ориентированное на данные планирование в EDS-DC
Algorithm 1. Data-oriented scheduling in EDS-DC

3.2 Отказоустойчивый метод динамической кластеризации в EDS-DC

Алгоритм 2 демонстрирует процедуру Dynamic-Clustering [15] [34] [41] [44], используемую для обеспечения отказоустойчивости. Поскольку в потоках научных работ одна или несколько связанных задач объединяются в одно задание, метод отказоустойчивой динамической кластеризации выбирает задания, которые содержат одну или большее число аварийно завершившихся задач, динамически разбивает их на *k* кластеров задач и повторно выполняет. Входными данными является списки ресурсов $L(Rn)$ и неудачных заданий $L(Fj)$. Алгоритм возвращает список невыполненных заданий $M(Fj)$, сопоставленных требуемым ресурсам $M(Rn)$.

```
      Input: L(Rn,Fi) – List of available resources and failed jobs
      Output: M(Fi,Rn) – Mapped list of failed jobs to resources
 1.   procedure Dynamic-Clustering (L(Rn,Fi))
 2.      Lj ← Fi  ⊳ List of failed jobs
 3.      LR ← Rn  ⊳ List of available resources
 4.      M(Fi,Rn) ← 0 ⊳ Mapped list failed jobs to resources
 5.      Split each job from Lj into k clusters of tasks dynamically
```

```
 6.       for all clusters (k) and available resources (L_R) do
 7.           find resource(s) R_i for cluster ki
 8.           as per data-oriented scheduling algorithm
 9.       end for
10.          M(F_i,R_n) ← M(F_i,R_n) + M(k_i,R_i) ▷ Mapped and submit to
                                                    list
13.      return M(F_i,R_n)                  ▷ The output is M(F_i,R_n)
14.    end procedure
```

Алгоритм 2. Отказоустойчвый метод динамической кластеризации в EDS-DC
Algorithm 2. Dynamic-Clusterind Fault-tolerant technique in EDS-DC

4. Эксперименты, результаты и обсуждение

В этом разделе рассматриваются подготовка имитации, моделирование ресурсов и приложений, а затем приводятся результаты и обсуждение.

4.1 Подготовка имитации

In terms of characteristics of resources and specifications of scientific workflows submitted by the user, the detail description of the simulation environment is given below.

Применительно к характеристикам ресурсов и спецификациям потоков научных работ, предоставленным пользователями ниже приводится подробное описание среды симуляции.

4.1.1 Моделирование ресурсов

Для моделирования использовался WorkflowSim [18] [37], «инструментарий для симуляции потоков научных работ». WorkflowSim – это инструмент симуляции потоков работ, используемый для реализации методов планирования и управления потоками, однако предлагаемая политика планирования и отказоустойчивый механизм в WorkflowSim ранее не были реализованы. Поэтому мы реализовали в WorkflowSim Алгоритм 1 (Политика планирования) и Алгоритм 2 (Механизм отказоустойчивости). Использовались общие ресурсы адресного пространства, а также такие характеристики, как стоимость, период обработки, бюджет и крайний срок выполнения.

Остальные технические характеристики приведены в табл. 2.

Табл. 2. Спецификация русурсов, используемых для симуляции
Table 2: The specification of resources used for simulation

Число VM	**Память**	**BW**	**VM**	**Arch**
100	1 GB	1000	Xen	X86
OS	**Стоимость VM $/час**	**Стоимость памяти $/сек**	**Стоимость хранения данных $/сек**	**Стоимость передачи данных $/сек**
Linux	3.0	0.05	0.1	0.1

4.1.2 Моделирование приложений

При моделировании мы считали, что имитируется один пользователь, который запускает поток научных работ реального потока научных работ рабочего процесса CyberShake является то, что CyberShake обладает большинством характеристик потоков научных работ, таких как интеграция, дезинтеграция, параллелизм и конвейеризация.

4.2 Параметры оценки производительности

Ниже подробно рассматриваются параметры оценки производительности с описанием того, как они рассчитываются в наших сценариях.

4.2.1 Make-span

Make-span – это время, требуемое для завершения выполнения пакета задач. В контексте потоков научных работ это общее время, необходимое для выполнения всего потока научных работ [21]. Оно обозначается как *M.S* и вычисляется по формуле (1).

$$M.S = F.T - S.T \quad (1),$$

где $F.T$ – время окончания потока научных работ, а $S.T$ – время начала потока научных работ.

4.2.2 Крайний срок

Крайний срок – это заранее определенное время окончания выполнения пакета задач. В контексте потоков научных работ заранее задается общее время выполнения всего потока научных работ [17]. Оно обозначается как *D.L* и может быть вычислено по формуле (2).

$$D.L = Comp.T + Comm.Time + Overhead \quad (2)$$

Накладные расходы – это дополнительное время, затрачиваемое на повторное выполнение неудачных заданий/задач.

4.2.3 Стоимость

Стоимость – это бюджет, требуемый для выполнения пакета задач. В контексте потоков научных работ это общий бюджет, необходимый для выполнения всего потока научных работ [21]. Стоимость может быть рассчитан по формуле (3).

$$Cost = Cost\ on\ F.T - Cost\ on\ S.T \quad (3)$$

Кроме того, стоимость выполнение каждой задачи потока научных работ обозначается через $Cost_t$ и может быть вычислена по формуле (4).

$$Cost_t = ProcessingCost + StorageCost + MemoryCost + BandwidthCost \quad (4)$$

4.2.4 Бюджет

Бюджет – это общий объем доступных финансовых ресурсов для выполнения пакета задач [17]. В контексте потоков научных работ это предопределенная стоимость, необходимая для выполнения потоков научных работ целиком. Бюджет может быть рассчитан с помощью формулы (5).

$$Budget = Comp.Cost + Comm.Cost + Overhead \quad (5)$$

Накладные расходы ($Overhead$) – это дополнительные затраты, потребляемые при повторном выполнении неудачных заданий/заданий.

4.2.5 Нарушение SLA

В контексте потоков научных работ нарушением соглашения об уровне обслуживания (SLA Violation) называется ситуация, когда стоимость выполнения потока научных работ превышает размер установленного бюджета или время выполнения выходит за пределы крайнего срока [17]. Формулы (6) и (7) показывают условия, касающиеся нарушения SLA [33].

$$SLAV = SLAV_{I.T} \quad (6)$$

$$SLAV = SLAV_{I.C} \quad (7),$$

где $SLAV$ – это нарушение SLA, $SLAV_{I.T}$ – это нарушение SLA из-за увеличения времени выполнения, а $SLAV_{I.T}$ – увеличение стоимости за пределы доступного бюджета.

4.3 Результаты и обсуждение

Мы определили сценарий для масштабного моделирования своего подхода. Мы рассматриваем одного пользователя, который запускает поток научных работ реального времени CyberShake с 30, 50, 100 и 1000 задачами. В EDS-DC мы использовали отказоустойчивую технику динамической кластеризации вместе с ориентированным на данные планированием. Кроме того, мы выполняли тот же поток научных работ реального времени с применением трех хорошо известных эвристических политик планирования MCT, Max-min и Min-min. Затем мы сравнили результаты EDS-DC с результатами этих политик.

4.3.1 Сценарий симуляции

Цель сценария – оценить EDS-DC и сравнить эффективность нашего подхода с результатами использования MCT, Max-min и Min-min. Параметры оценки: время выполнения, стоимость, крайний срок, бюджет и нарушение SLA. Среднее значение рассчитывается по времени выполнения и стоимости, а затем мы анализируются результаты. Количество пользователей – 1, а время моделирования – 24 часа. Общая спецификация сценария приведена в табл. 3.

Табл. 1. Спецификации сценария 1
Table 3: Scenario 1 specifications

Механизм отказоустойчивости	**Политика планирования**	**Потоки научных работ**
Динамическая кластеризация	EDS-DC	CyberShake-30
		CyberShake-50
		CyberShake-100
		CyberShake-1000
	MCT	CyberShake-30
		CyberShake -50
		CyberShake -100
		CyberShake -1000
	Max-min	CyberShake-30
		CyberShake -50
		CyberShake -100
		CyberShake -1000
	Min-min	CyberShake-30
		CyberShake -50
		CyberShake -100
		CyberShake -1000

Время выполнения: результаты по времени выполнения для EDS-DC по сравнению с MCT, Max-min и Min-min представлены на рисунке. 3. Результаты показывают, что EDS-DC сократил время выполнения на 10,9% как о сравнению с MCT-DC, на 13,7% по сравнению с Max-min-DC и на 6,4% по сравнению с политикой планирования Min-min-DC. Причина в том, что в планировании EDS-DC время выполнения рассматривается как параметр, ориентированный на данные.

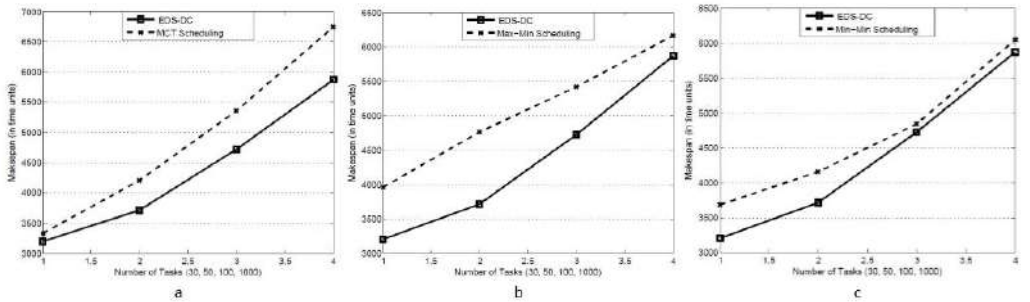


Рис. 3: Сравнение EDS-DC с (a) планированием MCT, (b) планированием Max-Min и (c) планированием Min-Min для CyberShake с использованием метода отказоустойчивости Dynamic-Clustering по времени выполнения

Fig. 3: Comparison of EDS-DC with (a) MCT scheduling, (b) Max-Min scheduling, and (c) Min-Min scheduling for CyberShake in respect of make-span by using Dynamic-Clustering Fault-Tolerant Technique

Стоимость: результаты по стоимости для EDS-DC по сравнению с MCT, Max-min и Min-min планировкой редставлены на рис. 4. Результаты показывает, что EDS-DC позволил снизить стоимость на 4% по сравнению с MCT-DC, на 5,6% по сравнению с Max-min-DC и на 1,5% по сравнению с политикой Min-min-DC. Причина в том, что в планировании EDS-DC мы рассматриваем стоимость как параметр, ориентированный на данные.

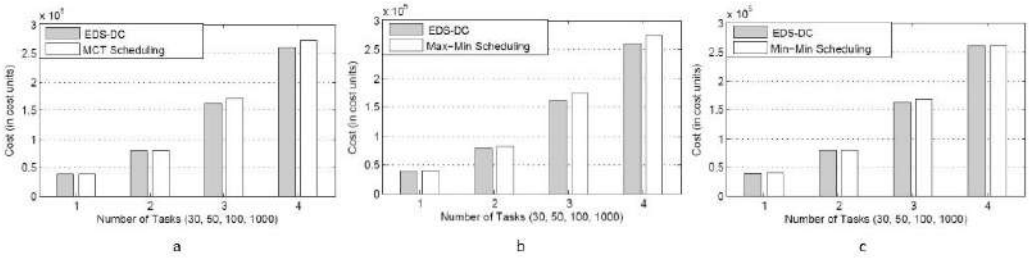


Рис. 4. Сравнение EDS-DC с (a) планированием MCT, (b) планированием Max-Min и (c) планированием Min-Min для CyberShake с использованием метода отказоустойчивости Dynamic-Clustering по стоимости

Fig. 4: Comparison of EDS-DC scheduling with (a) MCT scheduling, (b) Max-Min scheduling, and (c) Min-Min scheduling for CyberShake in respect of cost by using Dynamic-Clustering Fault-Tolerant Technique

Нарушение SLA: результаты в табл. 4 показывают, что при использовании EDS-DC SLA не нарушается ни для временных, ни для стоимостных ограничений для всех четырех потоков работ. При использовании MCT, Max-min и Min-min SLA нарушается четыре, восемь и два раза соответственно. Причина в том, что в планировании EDS-DC мы рассматривали время выполнения, стоимость, бюджет, крайний срок и нарушение SLA как параметры, ориентированные на данные.

Табл. 4. Крайний срок, бюджет и нарушение SLA
Table 4: Deadline, budget and SLA Violation

Поток научных работ	**Политика планирования**	**Время выполнения (сек)**	**Стоимость (**центы**)**
CyberShake-30	***EDS-DC***	***3197.626***	***38876.576***
	MCT	3335.92	38594.654
	Max-min	3955.87	40389.53
	Min-min	3677.02	40232.162
CyberShake - 50	***EDS-DC***	***3711.602***	***78421.248***
	MCT	4207.002	79516.86

	Max-min	4764.942	81624.304
	Min-min	4152.506	79128.504
CyberShake - 100	***EDS-DC***	***4725.288***	***161065.554***
	MCT	5353.238	170969.164
	Max-min	5413.854	174789.57
	Min-min	4835.968	167245.486
CyberShake - 1000	***EDS-DC***	***5871.774***	***260137.452***
	MCT	6745.066	271745.562
	Max-min	6162.442	273448.45
	Min-min	6041.182	260303.37

Поток научных работ	**Крайний срок (сек)**	**Бюджет (центы)**	**Нарушение SLA**	
			For Time	**For Cost**
CyberShake-30	3600.00	40000.00	***No***	***No***
			No	No
			Yes	Yes
			Yes	Yes
CyberShake - 50	4500.00	80000.00	***No***	***No***
			No	No
			Yes	Yes
			No	No
CyberShake - 100	5000.00	170000.00	***No***	***No***
			Yes	Yes
			Yes	Yes
			No	No
CyberShake - 1000	6500.00	270000.00	***No***	***No***
			Yes	Yes
			No	Yes
			No	No

5. Заключение

Мы представили EDS-DC для планирования потоков научных работ. EDS-DC – это планировщик, ориентированный на данные и использующий отказоустойчивую технику динамической кластеризации. Мы рассмотрели пример потока научных работ реального времени CyberShake с 30, 50, 100 и 1000 задачами. Чтобы узнать эффективность EDS-DC, мы сравнили его результаты с тремя известными политиками планирования MCT-DC, Max-min-DC и политики Min-min-DC. Результаты по времени выполнения для CyberShake (1180 задач) составляют 17506,29, 19641,23, 20297,11 и 18706,68 секунд для EDS-DC, MCT-DC, Max-min-DC и Min-min-DC соответственно. Результаты по стоимости CyberShake (1180 задач) составляют 538500,8, 560826,2, 570251,9 и 546909,5 цента для политик планирования EDS-DC, MCT-DC, Max-min-DC и Min-min-DC соответственно. Изучение результатов моделирования показывает, что EDS-DC уменьшил время выполнениязон на 10,9% по сравнению с MCT-DC, на 13,7% по сравнению с Max-min-DC и на 6,4% по сравнению с политикой планирования Min-min-DC. Аналогично, EDS-DC снизил стоимость на 4% по сравнению с MCT-DC, на 5,6% по сравнению с Max-min-DC и на 1,5% по сравнению с политикой планирования Min-min-DC. SLA не нарушается для EDS-DC по отношению к временных и стоимостных ограничениям, но нарушается несколько раз при использовании MCT-DC, Max-min-DC и Min-min-DC.

В будущих исследованиях мы рассчитываем разработать основанные на QoS энергосберегающие и ориентированные на данные политики отказоустойчивого планирования для потоков научных работ в облачных средах.

Список литературы / References

[1] J. Shi, J. Luo, F. Dong, J. Zhang, and J. Zhang, “Elastic resource provisioning for scientific workflow scheduling in cloud under budget and deadline constraints,” Cluster Comput., vol. 19, no. 1, pp. 167–182, 2016.

[2] D. Sun, G. Chang, C. Miao, and X. Wang, “Analyzing, modeling and evaluating dynamic adaptive fault tolerance strategies in cloud computing environments,” J. Supercomput., vol. 66, no. 1, pp. 193–228, 2013.

[3] D. Lifka, “XSEDE Cloud Survey Report,” no. September, 2013.

[4] X. Li, J. Song, and B. Huang, “A scientific workflow management system architecture and its scheduling based on cloud service platform for manufacturing big data analytics,” Int. J. Adv. Manuf. Technol., pp. 119–131, 2016.

[5] B. P. Abbott et al, “LIGO: the Laser Interferometer Gravitational-Wave Observatory,” Reports Prog. Phys., vol. 72, no. 7, p. 76901, 2009.

[6] S. Bharathi, E. Deelman, G. Mehta, K. Vahi, A. Chervenak, and M. Su, “Characterization of Scientific Workflows,” in The 3rd Workshop on Workflows in Support of Large Scale Science, 2008.

[7] S. Callaghan, P. Maechling, P. Small, K. Milner, G. Juve, T. H. Jordan, E. Deelman, G. Mehta, K. Vahi, D. Gunter, K. Beattie, and C. Brooks, “Metrics for heterogeneous scientific workflows : A case study of an earthquake science application,” 2011.

[8] S. Callaghan, P. Maechling, E. Deelman, K. Vahi, G. Mehta, K. Milner, R. Graves, E. Field, D. Okaya, D. Gunter, and T. Jordan, “Reducing Time-to-Solution Using Distributed High-Throughput Mega-Workflows – Experiences from SCEC CyberShake,” pp. 151–158, 2008.

[9] S. Abrishami, M. Naghibzadeh, and D. H. J. Epema, “Deadline-constrained workflow scheduling algorithms for Infrastructure as a Service Clouds,” Futur. Gener. Comput. Syst., vol. 29, no. 1, pp. 158–169, 2013.

[10] D. Chakraborty, V. V. Mankar, and A. A. Nanavati, “Enabling runtime adaptation of workflows to external events in enterprise environments,” Proc. - 2007 IEEE Int. Conf. Web Serv. ICWS 2007, no. Icws, pp. 1112–1119, 2007.

[11] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, “The cost of doing science on the cloud: The montage example,” 2008 SC - Int. Conf. High Perform. Comput. Networking, Storage Anal. SC 2008, no. November, 2008.

[12] D. Serrano, S. Bouchenak, Y. Kouki, F. A. De Oliveira, T. Ledoux, J. Lejeune, J. Sopena, L. Arantes, and P. Sens, “SLA guarantees for cloud services,” Futur. Gener. Comput. Syst., vol. 54, pp. 233–246, 2016.

[13] J. Choi, T. Adufu, and Y. Kim, “Data-Locality Aware Scientific Workflow Scheduling Methods in HPC Cloud Environments,” Int. J. Parallel Program., vol. 45, no. 5, pp. 1128–1141, 2017.

[14] W. Tang, J. Jenkins, F. Meyer, R. Ross, R. Kettimuthu, L. Winkler, X. Yang, T. Lehman, and N. Desai, “Data-aware resource scheduling for multicloud workflows: A fine-grained simulation approach,” Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 2015–Febru, no. February, pp. 887–892, 2015.

[15] W. Chen and E. Deelman, “Fault tolerant clustering in scientific workflows,” Proc. - 2012 IEEE 8th World Congr. Serv. Serv. 2012, pp. 9–16, 2012.

[16] B. Santhosh, P. K. A, and D. H. Manjaiah, “Comparative Study of Workflow Scheduling Algorithms in Cloud Computing,” pp. 31–37, 2014.

[17] T. Mathew, “Study and Analysis of Various Task Scheduling Algorithms in the Cloud Computing Environment,” Int. Conf. Adv. Comput. Informatics, pp. 658–664, 2014.

[18] W. Chen and E. Deelman, “WorkflowSim: A toolkit for simulating scientific workflows in distributed environments,” 2012 IEEE 8th Int. Conf. E-Science, e-Science 2012, 2012.

[19] T. Kosar and M. Balman, “A new paradigm: Data-aware scheduling in grid computing,” Futur. Gener. Comput. Syst., vol. 25, no. 4, pp. 406–413, 2009.

[20] L. Zeng, B. Veeravalli, and A. Y. Zomaya, “An integrated task computation and data management scheduling strategy for workflow applications in cloud environments,” J. Netw. Comput. Appl., vol. 50, pp. 39–48, 2015.

[21] D. Poola, K. Ramamohanarao, and R. Buyya, “Fault-tolerant workflow scheduling using spot instances on clouds,” Procedia Comput. Sci., vol. 29, pp. 523–533, 2014.

[22] D. Kumar, G. Baranwal, Z. Raza, and D. P. Vidyarthi, “A systematic study of double auction mechanisms in cloud computing,” J. Syst. Softw., vol. 125, pp. 234–255, 2017.

[23] M. Malawski, G. Juve, E. Deelman, and J. Nabrzyski, “Algorithms for cost-and deadline-constrained provisioning for scientific workflow ensembles in IaaS clouds,” Futur. Gener. Comput. Syst., vol. 48, pp. 1–18, 2015.
[24] X. He, X. Sun, and G. Laszewski, “A QoS Guided Scheduling Algorithm for Grid Computing,” Office, vol. 18, no. 4, pp. 1–15, 2002.
[25] A. M. Madureira and A. B. Definitions, “Ordered Minimum Completion Time Heuristic for Unrelated Parallel-Machines Problems.”
[26] R. J. Priyadarsini, “Performance Evaluation of Min-Min and Max-Min Algorithms for Job Scheduling in Federated Cloud,” vol. 99, no. 18, pp. 47–54, 2014.
[27] K. Qureshi, F. G. Khan, P. Manuel, and B. Nazir, “A hybrid fault tolerance technique in grid computing system,” J. Supercomput., vol. 56, no. 1, pp. 106–128, 2011.
[28] A. Bala and I. Chana, “Fault Tolerance- Challenges , Techniques and Implementation in Cloud Computing,” Int. J. Comput. Sci., vol. 9, no. 1, pp. 288–293, 2012.
[29] E. Deelman, K. Vahi, G. Juve, M. Rynge, S. Callaghan, P. J. Maechling, R. Mayani, W. Chen, R. Ferreira Da Silva, M. Livny, and K. Wenger, “Pegasus, a workflow management system for science automation,” Futur. Gener. Comput. Syst., vol. 46, pp. 17–35, 2015.
[30] R. Tolosana-Calasanz, J. Á. Bañares, C. Pham, and O. F. Rana, “Enforcing QoS in scientific workflow systems enacted over Cloud infrastructures,” J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1300–1315, 2012.
[31] W. Chen, R. Ferreira, E. Deelman, and R. Sakellariou, “Balanced Task Clustering in Scientific Workflows,” pp. 1–8.
[32] A. F. Antonescu and T. Braun, “Simulation of SLA-based VM-scaling algorithms for cloud-distributed applications,” Futur. Gener. Comput. Syst., vol. 54, pp. 260–273, 2016.
[33] S. Mustafa, B. Nazir, A. Hayat, A. ur Rehman Khan, and S. A. Madani, “Resource management in cloud computing: Taxonomy, prospects, and challenges,” Comput. Electr. Eng., vol. 47, p. , 2015.
[34] Barladian, B. Kh, et al. "An efficient mulithreading algorithm for the simulation of global illumination." Programming and Computer Software 43.4 (2017): 217-223.
[35] Fursova, N. I., et al. "A lightweight method for virtual machine introspection." Programming and Computer Software 43.5 (2017): 307-313.
[36] Gusev, A. D., Andrey V. Nasonov, and Andrey S. Krylov. "Fast parallel grid warping-based image sharpening method." Programming and Computer Software 43.4 (2017): 230-233.
[37] Kuplyakov, D., Evgeny Shalnov, and Anton Konushin. "Markov chain Monte Carlo based video tracking algorithm." Programming and Computer Software 43.4 (2017): 224-229.
[38] Massobrio, Renzo, et al. "Towards a cloud computing paradigm for big data analysis in smart cities." Programming and Computer Software 44.3 (2018): 181-189.
[39] Muruganantham, R., and P. Ganeshkumar. "Quality of Service Enhancement in Wireless Sensor Network Using Flower Pollination Algorithm." Programming and Computer Software44.6 (2018): 398-406.
[40] Raja, R., and P. Ganeshkumar. "QoSTRP: A Trusted Clustering Based Routing Protocol for Mobile Ad-Hoc Networks." Programming and Computer Software 44.6 (2018): 407-416.
[41] Pashchenko, N. F., K. S. Zipa, and A. V. Ignatenko. "An algorithm for the visualization of stereo images simultaneously captured with different exposures." Programming and Computer Software 43.4 (2017): 250-257.
[42] Varnovskiy, N. P., et al. "Secure cloud computing based on threshold homomorphic encryption." Programming and Computer Software 41.4 (2015): 215-218.
[43] Zelenova, Sophia A., and Sergey V. Zelenov. "Schedulability Analysis for Strictly Periodic Tasks in RTOS." Programming and Computer Software 44.3 (2018): 159-169.
[44] Zipa, Kristina S., and Alexey V. Ignatenko. "Algorithms for the analysis and visualization of high dynamic range images based on human perception." Programming and Computer Software 42.6 (2016): 367-374.

Информация об авторах / Information about authors

Зульфикар АХМАД – преподаватель фпкультета информационных технологий Университета Хазара, Мансехра, Пакистан.

Zulfiqar AHMAD is a lecturer in the Department of Information Technology, Hazara Universtiy, Mansehra, Pakistan.

Али Имран ДЖЕХАНГИРИ – преподаватель факультета информационных технологий Университета Хазара, Мансехра, Пакистан. Он получил степень PhD в 2015 году в Университете им. Георга Августа Геттингена, Германия. Занимается исследовательской деятельностью, связанной с параллельными вычислениями, грид-вычислениями, облачными вычислениями и большими данными.

Ali Imran JEHANGIRI is a lecturer in the Department of Information Technology, Hazara Universtiy, Mansehra, Pakistan. He received Ph.D. degree in Computer Science from the Georg-August-Univesity Goettingen, Germany in 2015. He is involved in research activities dealing with parallel, Grid computing, Cloud computing and Big data.

Мехрин ИФТИХАР, преподаватель факультета информационных технологий, Университет Хазара, Мансехра, Пакистан

Mehreen IFTIKHAR is a lecturer in the Department of Information Technology, Hazara Universtiy, Mansehra, Pakistan.

Ариф Икбал УМАР получил докторскую степень в области компьютерных наук в Университете Бэйхан (БУАА), Пекин, Китай. В настоящее время он работает доцентом (компьютерные науки) на факультете информационных технологий Университета Хазара, Мансехра, Пакистан. Его исследовательские интересы включают интеллектуальный анализ данных, машинное обучение, поиск информации, цифровую обработку изображений, безопасность компьютерных сетей и сенсорных сетей.

Arif Iqbal UMAR obtained his PhD in computer science from BeiHang University (BUAA), Beijing, China. Currently, he is working as an assistant professor (computer science) at the Information Technology Department of Hazara University, Mansehra, Pakistan. His research interests include data mining, machine learning, information retrieval, digital image processing, computer networks security, and sensor networks.

Ибрар АФЗАЛ – преподаватель факультета информационных технологий Университета Хазара, Мансехра, Пакистан.

Mr.Ibrar AFZAL is a lecturer in the Department of Information Technology, Hazara Universtiy, Mansehra, Pakistan.

DOI: 10.15514/ISPRAS-2019-31(2)-10

Internet of Things for evaluating foraging and feeding behavior of cattle on grassland-based farming systems: concepts and review of sensor technologies

[1] *G.R. Garay Alvarez, ORCID: 0000-0002-2216-2436 <godofredo.garay@reduc.edu.cu>*
[2] *J.A. Bertot Valdés, ORCID: 0000-0003-1562-6754 <jose.bertot@reduc.edu.cu>*
[3] *K. Perez-Teruel, ORCID: 0000-0003-2154-3111 < karinaperez@uapa.edu.do >*

[1] *Department of Informatics, University of Camaguey, Camaguey, Cuba.*
[2] *Veterinary Department, University of Camaguey, Camaguey, Cuba.*
[3] *Universidad Abierta para Adultos UAPA, Av. Hispanoaméricana #100, Santiago, República Dominicana.*

Abstract. In this paper, we give an overview of the movement, foraging and feeding ecology as well as sensors technologies that could be embedded into an IoT-based platform for Precision Livestock Farming (PLF). A total of 43 peer-reviewed journal papers indexed by Web of Science were surveyed. Firstly, sensors technologies (e.g., RFID, GPS, or Accelerometer) used by the authors of each paper were identified. Then, papers were classified according to their applicability to ecological studies in the fields of foraging and feeding behavior.

Keywords: Internet of Things; IoT, sensors; precision agriculture; precision livestock farming

For citation: Garay Alvarez G.R., Bertot Valdés J.A., Perez-Teruel K. Internet of Things for evaluating foraging and feeding behavior of cattle on grassland-based farming systems: concepts and review of sensor technologies. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 137-152. DOI: 10.15514/ISPRAS-2019-31(2)-10

Acknowledgments. This work is partially supported by VLIR-UOS, Belgium.

Интернет вещей для оценки поведения крупного рогатого скота при поиске корма и кормлении в пастбищных системах земледелия: концепции и обзор сенсорных технологий

[1] *Г.Р Гарай Альварес, ORCID: 0000-0002-2216-2436 <godofredo.garay@ reduc.edu.cu>*
[2] *Х. Бертот Вальдес, ORCID: 0000-0003-1562-6754 <jose.bertot@reduc.edu.cu>*
[3] *К. Перес-Теруэль, ORCID: 0000-0003-2154-3111 <karinaperez@uapa.edu.do>*

[1] *Факультет информатики, Университет Камагуэй, Куба*
[2] *Факультет ветеринарии, Университет Камагуэй, Куба*
[3] *Открытый университет для взрослых, Сантьяго, Доминиканская Республика*

Аннотация. В этой статье приводится обзор экологических аспектов перемещения, кормодобывания и кормления крупного рогатого скота, а также технологий датчиков, которые могут быть встроены в основанную на Интернете вещей платформу для поддержки точного животноводства. Всего были проанализированы 43 рецензированных журнальных статьи, проиндексированные Web of Science. Во-первых, были идентифицированы сенсорные технологии (например, RFID, GPS или акселерометр), используемые авторами каждой статьи. Затем документы были классифицированы в соответствии с их применимостью к экологическим исследованиям в области кормодобывания и кормления скота.

Ключевые слова: Интернет вещей; датчики; точное земледелие; точное животноводство

Для цитирования: Гарай Альварес Г.Р., Бертот Вальдес Х., Перес-Теруэль К. Интернет вещей для оценки поведения крупного рогатого скота при поиске корма и кормлении в пастбищных системах земледелия: концепции и обзор сенсорных технологий. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 137-152 (на английском языке). DOI: 10.15514/ISPRAS-2019-31(2)-10

Благодарности. Эта работа поддерживается VLIR-UOS, Бельгия.

1. Introduction

The Internet of Things (IoT) is a paradigm where every-day objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective [1].

In Precision Livestock Farming, IoT is extended to farm animals, i.e., real-time monitoring technologies aimed at managing the smallest manageable production unit's temporal variability. This approach is known as 'the per animal' [2].

For ecologists, understanding the reaction of animals to environmental changes is critical. Using networked sensor technology to measure wildlife and environmental parameters can provide accurate, real-time and comprehensive data for monitoring, research, and conservation of wildlife [3], [4].

The scientific motivation of our review is to provide a comprehensive summary of the rapidly developing area of sensors technologies for Precision Livestock Farming (PLF) from an IoT perspective. The survey seeks to encourage computer scientists to conduct transdisciplinary research in the field of veterinary computer sciences/veterinary sciences.

In this paper, we give an overview of the movement, foraging and feeding ecology as well as sensors technologies that could be embedded into an IoT-based platform for Precision Livestock Farming (PLF). A total of 43 peer-reviewed journal papers indexed by Web of Science were surveyed. Firstly, sensors technologies (e.g., RFID, GPS, or Accelerometer) used by the authors of each paper were identified. Then, papers were classified according to their applicability to ecological studies in the fields of foraging and feeding behavior.

The paper is organized as follows. We first motivate the need for an IoT-based collection of movement and behavior data from the perspective of PLF. In addition, background information on ecology is given (Section 2). We then present a level-based approach for conducting the review (Section 3) and a classification of the literature based on such approach (Section 4). Next, we discuss some potential areas of transdisciplinary research (Section 5) and finally provide concluding remarks (Section 6).

2. Background

2.1 IoT-based platform for livestock farming

Detailed observation of the movement and behavior of animals at pasture offers the potential to understand spatial population processes as the ultimate consequence of individual behavior, physiological constraints and fine-scale environmental influences such as heat stress [5], [6], [7], [8].

Fig. 1 illustrates the integrated framework for farm management decision-making considered in this paper. It consists of four main phases: a collection of animal movement data using IoT sensors, transfer of data using communication technologies, analysis & planning conducted by data managers, and, finally, decision-making. Particularly, in this paper, we focus on collecting animal movement and behavior data on grassland-based farms.

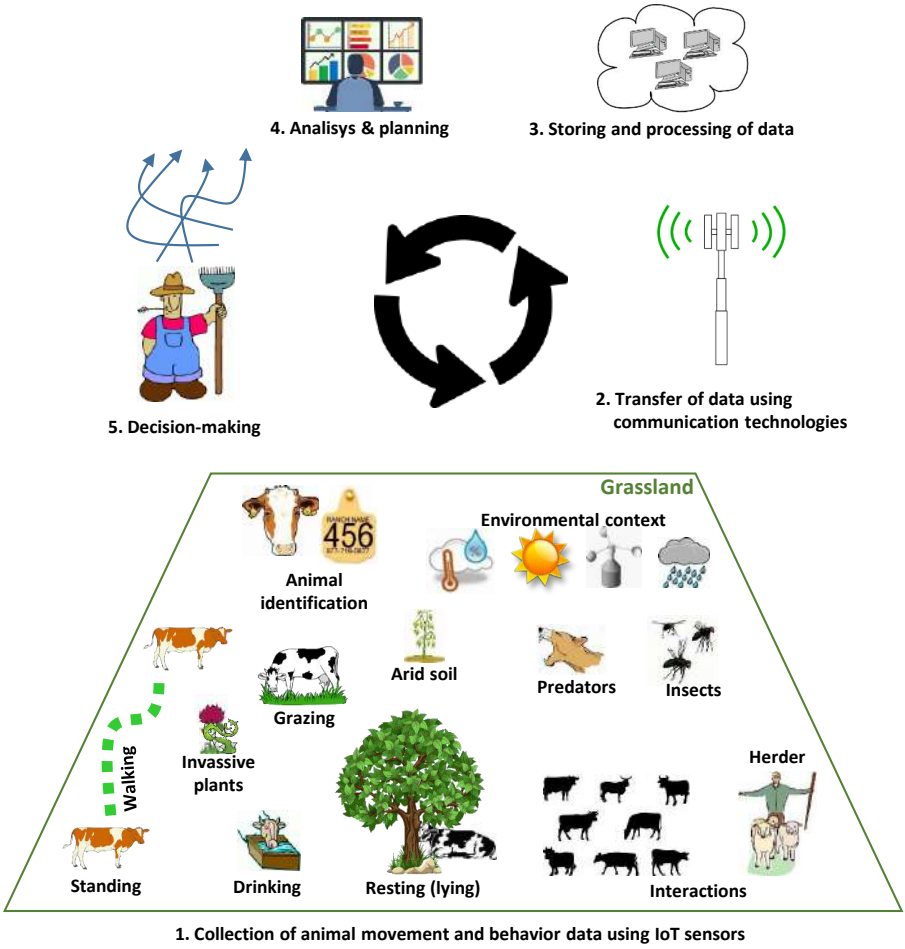


Рис. 1. Иллюстрация IoT-экосистемы для точного животноводства
Fig. 1. Illustration of IoT Ecosystem for Precision Livestock Farming

2.2 Animal ecology

Ecology is the scientific study of the interactions of organisms with the environment that determine their distribution and abundance. The environment of an organism consists of all those factors and phenomena that can influence it, whether those factors be physical and chemical (abiotic) or other organisms (biotic). Biotic means living, and biotic factors are the other, living parts of the ecosystem with which an organism must interact (e.g., predators, invasive plants, etc.). Abiotic means a nonliving condition or thing, as climate or habitat, that influences or affects an ecosystem and the organisms in it, (e.g., arid soils). In animal ecology, every scientific problem resolves itself into a quest for the relationship between two or more variables. The discovery of these inter-relations provides the basis for prediction and control [9].

2.2.1 Movement Ecology

In the context of movement ecology, movement of an organism is defined as a change in the spatial location of the whole individual in time [9]. Animal positions data provide the elemental unit of movement paths and show where individuals interact with the ecosystems around them.

The movement paths of animals over landscapes are represented by sequences of points (xi, yi) occurring at times ti. Modeling animal movement from spatiotemporal data is generally performed using two approaches, i.e., (i) the Lagrangian approach and (ii) the Eulerian approach [10]. The Lagrangian approach is individual-based and entails tracking a specific individual, while the Eulerian approach is place-based and deals with the probability of the presence of an individual or a group in a place and the change of this occurrence over time. Movement metrics are quantities that might be calculated directly from raw, uncorrected and unprocessed movement data. These metrics can be grouped into two large categories: trajectory analysis metrics and space-use analysis metrics [11]. For describing the path, the most basic ones are the step length (the Euclidean distance between consecutive relocations) and turning angle (the angle of one step relative to the step immediately prior), and the distance traveled by animals [12]. Such distance is an important ecological variable that links behavior, energetics, and demography. It is usually measured by summing straight-line distances between intermittently sampled locations along continuous animal movement paths [13].

On the other hand, the space-use analysis is based on spatial data types. These data types define points, lines, areas, and volumes. To measure the spatiotemporal change in a field population of individuals, the population may often be sampled in two-dimensional space on a series of occasions. The spatial pattern of data is usually shown in the form of maps where the two-dimensional coordinates of every individual are recorded. In animal ecology, spatial data are often recorded as counts of the number of individuals occurring in each of several sample units, where the location of each unit is known [14].

In this review, movement ecology metrics are the basis for the rest of the subdisciplines shown below.

2.2.2 Foraging Ecology

How animals search for their food arguably represents one of the most important aspects of foraging ecology. Grazing behavior is an important process directly associated with animal nutrition intake, fitness, and productivity [15], [16]. Ruminants are mammals that have a unique digestive system that allows them to better use energy from fibrous plant material than other herbivores. The ruminant digestive system uniquely qualifies ruminant animals such as cattle to efficiently use high roughage feedstuffs, including forages. Monitoring the specific behaviors of ruminants, particularly grazing and rumination, is important because these behaviors occupy much of the grazing cattle's time-budget [17]. Ruminant activity is an important index reflecting the health of animals with rumens. When cows suffer from the disease, rumination time decreases significantly. The influence of a variety of diseases affects the rumination time uniquely.

In general, animal's states can be classified into sub-classes according to different standards and purposes. Following the classification suggested in [18], the state classes we are using are shown in Fig. 2.

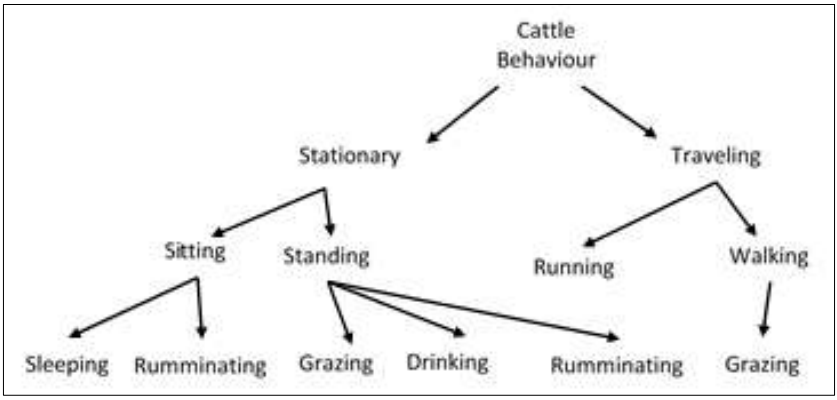


Рис. 2. Классы поведения скота
Fig. 2. Classification of cattle behavior classes

A better understanding of how cattle behave can be obtained with the help of fine spatiotemporal scales. For example, the provision of shade to cows under heat stress conditions is an essential component of heat management animals ruminating [19]

2.2.3 Feeding Ecology

Central to the study of animal ecology is how the environment is used by an animal: specifically, the kinds of foods it consumes and the varieties of habitats it occupies. We define habitats as regions in environmental space that are composed of multiple dimensions, each representing a biotic or abiotic environmental variable; that is, any component or characteristic of the environment related directly (e.g., forage biomass and quality) or indirectly (e.g., elevation) to the use of a location by the animal. Environmental variables can be dynamic or static (e.g., predator density and slope, respectively) and may be positively or negatively associated with use. Habitat use is the proportion of their time that animals spend in a particular habitat [20], [21].

The abundance of a component is the quantity of that component in the environment, as defined independently of the consumer. The availability of that component is its accessibility to the consumer. The usage of a component by the consumer is the quantity of that component utilized by the consumer in a fixed period. The selection of a component is a process in which an animal chooses that component. Usage is said to be selective if components are used disproportionately to their availability. The preference of a consumer for a particular component is a reflection of the likelihood of that component being chosen if offered on an equal basis with others. In theory, components can be ranked from "most preferred" to "least preferred." [21]. That what the animals select to eat given a set of physical constraints can be defined as ‘selection.’ For example, animals offered a sward containing grass and clover in an intimate mixture have to search through the mixture to find their preferred herbage. This requirement to search imposes a constraint on the animal’s ability to eat what it wants, so is an example of selection [22]. Intuitively, animals should distribute themselves according to the quality of habitats. If the selection is consistent with fitness, we should find more animals in better-quality habitats [23].

3. Planning the review

Fig. 3 illustrates the flow of this section. Three levels of information are provided: animal level offers brief information on animals considered in the context of this paper, IoT elements level provides an overview on IoT sensors, and finally, Ecology levels focus on the application of sensor technologies for ecological studies.

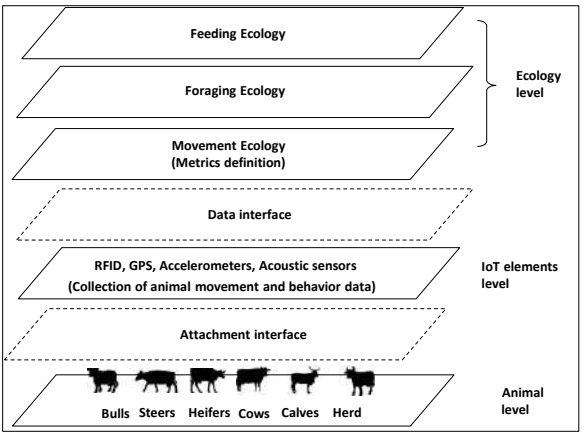


Рис. 3. Концептуальная структура анализа литературы
Fig. 3. The conceptual framework for the literature analysis

3.1 Animal level

Cattle are social animals. They live in large groups, called herds. A herd may consist of just a single or several cattle families. A bull is a mature male animal that is used for breeding. A steer is a castrated male calf raised for beef. A dominant male (bull) guards a group of females (cows) and their young (calves) protectively. A heifer is a female animal that has never had a calf. Once a heifer has a calf, she automatically becomes a cow.

3.2 IoT level

Radio Frequency Identification (RFID). Cattle identification and tracking refer to the process of accurately recognizing individual cattle and their products via a unique identifier or marker. Animal identification plays an influential role in understanding disease trajectory, vaccination and production management, animal traceability, and animal ownership assignment. Classical cattle identification systems can be grouped into three categories: permanent methods (e.g., ear notching, ear tattooing, etc.), temporary methods, and electrical methods [24]. The RFID technology is a breakthrough in the embedded communication paradigm which enables the design of microchips for wireless data communication. They help in the automatic identification of anything they are attached to acting as an electronic barcode. The passive RFID tags are not battery powered. They use the power of the reader's interrogation signal to communicate the ID to the RFID reader. Radio frequency identification (RFID) tags can be activated by a specific radiofrequency to send location information to a receiver. A passive RFID tag does not need any power source because it produces needed energy by an antenna. The reading distances can be a few meters. The tracking system can also work so that the moving objects have RFID tags and when a tag is close enough to a reader, the location is measured. The RFID technology is usually used like this for animal identification. The tracking resolution depends on the number of readers and the reading distance [25].

Accelerometry. Remote sensors, such as accelerometers, can monitor the behavior of animals constantly. These devices are small, relatively low-cost and noninvasive. Accelerometers should not influence the natural behavior patterns of animals in free-living conditions. An accelerometer detects bodily acceleration, which is represented as an analog voltage created by a piezoelectric instrument that is sensitive to compression in a vertical direction. Different types of devices are available and the choice about which to use depends on various factors: cost (especially when large populations are studied), physical characteristics (weight, size, and battery life), performance

(number of axes, possible epochs, system of data transfer, recording duration, function of the epochs, and the memory capacity), and the validity and intra- and inter-instrument reliability [26], [27]. It is worth noting that according to the number of axes, accelerometers can be classified in uniaxial, two-axil or tri-axial devices (a.k.a. unidimensional (1D), two-dimensional (2D) and tri-dimensional (3D), respectively). The tri-axial acceleration data is of specific interest as it provides quantitative data on body posture and motion. The three axes of the accelerometer are aligned to the dorso-ventral axis, the anterior-posterior axis and the lateral axis of the subject animal. These are termed (in biological parlance) heave, surge and sway respectively. These axes are analogous to the Y, Z, and X axes in cartesian coordinates [27] (fig. 4).

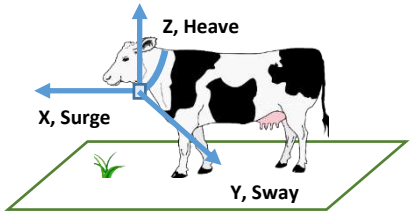


Рис. 4. Схема коровы с нашейным датчиком
Fig. 4. Schematic of cow with a collar

Global Positioning System. Today, the majority of movement ecology research depends upon more advanced satellite technology, referred to broadly as Global Positioning Systems (GPS), to record animal locations at finer spatial and temporal resolutions. Global Positioning System (GPS) units derive positions from internal receivers monitoring signals from an array of 24 earth-orbiting [28]. Radio-collars and other sensors equipped with global positioning systems (GPS) allow providing a continuous record of animal locations (a.k.a relocations) that remains unobtainable using traditional technologies such as very-high-frequency (VHF) devices. The determination of the GPS relocations is based on receiving track and time mark signals from satellites and calculating a receiver location based on distances to satellites.

Acoustic sensors. Eating and ruminating last for a considerable period and account for most of a ruminant's daily activity. The direct and continuous observation of these activities is labor-intensive, time-consuming, and frequently not feasible. These difficulties have promoted the development of automatic recording devices. Regurgitation and rumination produce distinctive sounds that are recorded by a microphone, processed, digitally stored. The method allows accurate counts of ruminant bites, chews, and complex chew-bite events. Acoustic monitoring can be carried out offline (i.e., restricted to desktop computers) or in real-time [29], [30]. Acoustic sensors can be found as independent devices on the market (e.g. [31] or embedded into accelerometer devices.

3.3 Interfaces

Attaching measuring devices to animals is often the only way to acquire vital life-history information on species that do not lend themselves to observation. However, the ethics of acceptable practice for attached devices are poorly defined. Here, we consider the need for further research and attempt to identify a system that allows animal restraint practices and device-induced effects to be quantified and monitored so that ethics committees can have a defined scale on which to base decisions [32].

In general, sensors here reviewed can be attached to different parts of the animal body, e.g., legs, neck, and ears. Miniaturized sensors play a significant role in ecology-related researches. In the seminal paper by (Ungar et al., 2005), cows were fitted with leg-attached GPS collars weighing

about 1.15 kg [33]. Nowadays, GPS collars are commonly used. It should be noted that many sensors are dataloggers; hence, handing animal is needed for retrieving data.

4. Classification of literature

The literature was classified according to its content into the following major categories: Movement Ecology, Foraging Ecology, and Feeding Ecology. Some of these top-level categories were further broken down into sub-categories.

4.1 Movement Ecology

A variety of global positioning system tracking collars for use on cattle has been developed. In general, these collars can be manufactured by companies or custom-built. According to [34], the effect of GPS sample interval and paddock size on estimates of distance traveled by grazing cattle in rangeland is an important issue to consider.

The number of animals required to represent the collective characteristics of a group remains a concern in animal movement monitoring with GPS. Monitoring a subset of animals from a group instead of all animals can reduce costs and labor; however, incomplete data may cause information losses and inaccuracy in subsequent data analyses. In cattle studies, little work has been conducted to determine the number of cattle within a group needed to be instrumented considering subsequent analyses. In [35], a characterization of cattle movement is conducted. Metrics for analyzing herd movements, such as average herd travel speed, daily travel distances, average herd radius, average centroid location deviation, and average herd radius deviation, are considered. In [36], it is evaluated how closely do collared animals cluster in their herd and how well do different logging intervals affect estimations of total distance traveled by collared animals.

4.2 Foraging ecology

Animal behavior such as, walking, foraging, standing, lying, can be derived from high-frequency GPS. This approach allows tracking cows in open and forested habitat [37], [38], [39]. Spatio-temporal patterns of cattle grazing were studied in four annual grassland pastures in North America, differing mainly in tree canopy cover. Cows were equipped with global positioning collars that recorded position, temperature and head movements at 5-min intervals during six days in each of four seasons repeated during two years. The time animals took to traverse areas of varying diameter revealed patches of 6–9-m diameter in the pastures with low, and 18–21-m diameter in the pastures with high tree canopy cover [40]. The authors of [41] analyze a high-frequency movement dataset for a group of grazing cattle and investigate their spatiotemporal patterns using a mobility model. In [42], the spatiotemporal dynamics of cattle behavior and resource selection patterns on East African rangelands. Based on the integration of GPS-tracking and field observations, this study links cattle behavioral types with statistical parameters of movement, analyzes spatiotemporal dynamics of behavior and predicts resource selection patterns.

In livestock farming, the accurate prediction of calving time is a key factor for profitability and animal welfare. Continuous monitoring systems can detect behavioral changes occurring on the actual day of calving, some of them being accentuated in the last few hours before delivery; standing/lying transitions, tail raising, feeding time, and dry matter and water intakes differ between cows with poor health conditions. Use of these behavioral changes has the potential to improve the management of calving [43].

In [44], a behavioral model of the pasture-based dairy cow that requires incoming, transformed GPS data collected from cattle to be partitioned into segments of a fixed length before behavioral classification into grazing, resting or walking. GPS data such as distance traveled (m) and turning angle (degrees) were used by the developed model. In [45], GPS data collected over a 4-yr period

on 52 crossbred young cows grazing a 146-ha pasture were used to determine whether cattle establish patch-scale rotational grazing patterns within pastures.

Distinguishing cattle foraging activities using accelerometry-based activity monitors is widely reported in the literature. For example, grazing behavior [46], lying, standing or walking [47], walking and standing [48], lying time and frequency of lying bouts [49], lying behavior [50], grazing, rest, travel [51]. In [52], an in-depth study of wireless sensor networks applied to the monitoring of animal behavior in the field is described. Herd motion data, such as the pitch angle of the neck and movement velocity, were monitored by a sensor equipped with a 2-axis accelerometer.

In many studies, rumination is assessed by using accelerometers with acoustic sensors included. In [53], accelerometer systems have been validated for detecting rumination time, chewing cycles, and rumination bouts. Accelerometer data on cow activity and rumination have been used for improving prediction of the start of calving in dairy cows [54] as well as monitoring feeding behavior in feedlot cattle [55]. In [56], various supervised machine learning techniques were applied to classify cattle behavior patterns recorded using collar systems with 3-axis accelerometer, fitted to individual dairy cows to infer their physical behaviors. In [57], estimation of grass intake on pasture for dairy cows using tightly and loosely mounted di- and tri-axial accelerometers combined with bite count. In [58], the influence of breed, milk yield, and temperature-humidity index on dairy cow lying time, neck activity, reticulorumen temperature, and rumination behavior is assessed. In [59], cattle adaptation to heat stress is assessed. The movement, ruminating time and weight gain between 2 breeds kept for 80 days at pasture during tropical spring are compared. Animal motility (measured using an accelerometer) and rumination time (minutes/day, using a sound sensitive sensor) were evaluated through a collar-sensor by radio telemetry. Rumen temperature was recorded at 10 min intervals using RFID rumen temperature sensor. A 3-dimensional accelerometer is attached to the RFID ear tag, and an online application provided by the manufacturer records time spent feeding, ruminating, active, and resting per hour and per day. Raw data were transmitted every minute through radio ZigBee-based frequency technology [57].

Other authors have assessed rumination and activity patterns by using accelerometers. For example, rumination, feeding, activity, and animal temperature [54], feeding, ruminating, active, and resting [55], rumination time, chewing cycles, and rumination bouts [53], lying time, neck activity, reticulorumen temperature, and rumination time [58], grazing, searching, ruminating, resting, and scratching [56], level of activity and rumination [60], grazing, ruminating, walking, resting behaviors to develop algorithms for pasture intake by individual grazing cattle [61], rumination and its relationship to feeding and lying behavior in Holstein dairy cows] [62]. In [63], GPS locations were recorded to calculate mean slope, elevation, distance from water, distance traveled per day, and elevation for each cow.

Relationships between ambient conditions, thermal status, and feed intake of cattle during summer heat stress with access to shade. Ear tags, telemetrically connected to a feed monitoring system, provided animal data using RFID technology. Data loggers recorded ambient conditions in the sun and shade, along with black globe temperature [64]. The authors of [40] hypothesize that when forage is of low quality and abundant, animals will fill up faster and tend to travel shorter distances while grazing, thus imposing greater heterogeneity of forage utilization. GPS collars were programmed to record a position every 5 min for each one-week grazing period. Collars recorded longitude, latitude, date, time, elevation, temperature, forward-backward collar movement, left–right collar movement and satellite ephemeris information. Data were downloaded from the collars following each grazing period and differentially corrected by removing the positional error recorded by a stationary ‘base’ unit whose true coordinates were known. Authors conclude that shade distribution can modulate meal start and duration. [65] investigates the direct effects of tightly bunched herding versus loosely bunched herding on foraging behavior, nutrition, and

performance (weight gain) of cattle in semiarid savanna rangeland. To this end, the mean daily distance covered by the herds under study are quantified.

4.3 Feeding ecology

To understand the spatial extent of grazing bouts and to determine the speed at which the animals were moving, the authors of [66] record GPS coordinates at the start and end of each feeding bout to determine the distance covered by the herd. In the conducted experiments, feeding ecology of four livestock species under different management in a semi-arid pastoral system is assessed. In [67], the development of a threshold-based classifier for real-time recognition of cow feeding and standing behavioral activities from accelerometer data is presented. In [68], the use of sensors combining local positioning and acceleration is used to measure feeding behavior differences associated with lameness in dairy cattle. It is worth noting that cattle lameness is one of the most significant welfare and productivity issues in dairy farming. That is why, to asses lameness by visual methods, a 5-point lameness scoring system that assessed gait and back posture has been developed (see [69]). In [57], estimation of grass intake on pasture for dairy cows using tightly and loosely mounted di- and tri-axial accelerometers combined with bite count are carried out. In [70], determination of minimum meal interval and analysis of feeding behavior in shaded and open-lot feedlot heifers as conducted by using RFID technology.

In [71], GPS units are deployed to monitor cattle movements and habitat use and to assess the impact of cattle grazing on vegetation. In [72], GPS data were used to quantify the movement patterns of elephant bulls, buffalo and cattle at multiple scales and according to seasonal changes of surface water availability. In [73], space use and movement trajectory statistics are assessed to We identify site fidelity patterns in animal location data.

Electronic radio-frequency-identification-based systems can be used for measuring: feeding behavior traits in beef cattle [74,75]; factors affecting water intake of growing beef cattle [62]; feeding time and dry matter intake (DMI) by recording each time each cow placed her head into the feed bin, and calculated the total duration of the feeder visit as well as the amount of feed consumed during that visit. In [76], RFID-based system for monitoring individual feeding and drinking behavior and intake in young cattle is validated. In [77], RFID technology is used to record grazing beef cattle water point use.

4.4 Summary

In Table 1, based on the subdisciplines of Ecology shown in Section 2, we summarize the studies published in the literature. We want to note that the scope of some is not limited to a single category. For example, [40] studies aspects of the three subdisciplines here reviewed while [55], [57], [64], [68] address only aspects of foraging and feeding ecology.

Табл, 1. Классификация статей, рассмотренных в подразделах 4.1-4.3.
Table 1. Classification of the reviewed papers in Subsections 4.1-4.3

Major category	GPS	RFID	Accelerometer
Movement Ecology	[40], [63], [34], [35], [36], [44], [65], [66]		
Foraging Ecology	[37], [38], [39], [40], [41],[42], [43], [44], [46], [47], [48], [78], [50], [51], [66], [67], [69]	[64], [68]	[52], [53], [54], [55], [56], [57], [58], [59], [60], [61]

Feeding Ecology	[40], [42], [43], [63], [64], [65], [69], [70]	[61], [64], [68], [71], [72], [73], [74],	[55], [57], , [61]

5. Discussion

Rapid advances in technology are allowing scientists to use data-recording units to acquire huge, quantitative datasets of behavior from animals moving freely in their natural environment. For analyzing animal movement data, a number of R software packages have been developed, e.g., moveHMM [79], ctmm [80], feedr and animalnexus.ca [81], trajr [82].

Data-driven agriculture involves the collection of enormous, dynamic, complex and spatial data which requires storage and processing. Great gains can be made by sharing online and exchanging animal tracking data. Two examples are: (1) Movebank project [83], [84], and (2) OzTrack project, [85]. Cloud-based data storage or farm-based storage can be considered for storing data. The use of cloud IoT platforms allows for big data collected from sensors to be stored in the cloud.

The ultimate goal is to suggest managerial options to the farmer. Specialized grassland management techniques allow farmers to improve the decision-making process by applying sound principles and guidelines for managing cattle grazing in the grazing lands [86]. To this end, behavioral models for a pasture-based dairy cow from GPS data can be developed. These models can use, for example, data mining, machine learning techniques [87], or Markov models [44].

Foraging activities and questions of energy optimization are difficult to quantify in practice, but recent advances in Geographic Information Systems (GIS) and Global Positioning Systems (GPS) have a greatly simplified examination of many spatially related phenomena.

From the hardware viewpoint, custom-built, open-source GPS datalogger based on Arduino for collecting data can be designed and built (see [36]).

6. Conclusions

This paper has reviewed the literature on sensors in livestock farming and provides an overview of existing applications. The review shows that the subject received a lot of attention from the scientific community. The value of technology can be best realized when integrated with agronomic knowledge, using the information gathered in the improvement of decision support systems.

Both computer science scientists and veterinary science scientists can use the information here provided for conducting transdisciplinary researches.

References

[1]. Whitmore, A., Agarwal, A., Xu, L.D. The Internet of Things – A survey of topics and trends. I Information Systems Frontiers, vol. 17, no. 2, 2015, pp. 261–274.

[2]. Halachmi, I., Guarino, M. Editorial: Precision livestock farming: a ‘per animal’ approach using advanced monitoring technologies. Animal, vol. 10, no. 9, 2016, pp. 1482–1483.

[3]. Guo S., Qiang M., Luan X., Xu P., He G., Yin X., Xi L., Jin X, Shao J, Chen X, Fang D., Li B. The application of the Internet of Things to animal ecology. Integrative zoology, vol. 10, no. 6, 2015, pp. 572-578.

[4]. Ingrand S. Opinion paper: ‘monitoring te salutant:’ combining digital sciences and agro-ecology to design multi-performant livestock farming systems. Animal, vol. 12, no. 1, 2018, pp. 2–3.

[5]. Nathan R., Getz W.M., Revilla E., Holyoak M., Kadmon R., Saltz D., Smouse P. E. A movement ecology paradigm for unifying organismal movement research. Proceedings of the National Academy of Sciences, vol. 105, no. 49, 2008, pp. 19052-19059.

[6]. Getz W.M., & Saltz D.A framework for generating and analyzing movement paths on ecological landscapes. Proceedings of the National Academy of Sciences, vol. 105, no. 49, 2008, pp.19066-19071.

[7]. Lallo C. H., Cohen J., Rankine D., Taylor M., Cambell J., & Stephenson T. Characterizing heat stress on livestock using the temperature humidity index (THI) – prospects for a warmer Caribbean. Regional Environmental Change, vol. 18, no. 8, 2018, pp.1-12.

[8]. Polsky L., & von Keyserlingk M.A. Invited review: Effects of heat stress on dairy cattle welfare. Journal of dairy science, vol. 100, no. 11, 2017, pp. 8645-8657.

[9]. Nathan R., Getz W.M., Revilla E., Holyoak M., Kadmon R., Saltz D., & Smouse P.E. A movement ecology paradigm for unifying organismal movement research. Proceedings of the National Academy of Sciences, vol. 105, no. 49, 2008, pp. 19052-19059.

[10]. Smouse P.E., Focardi S., Moorcroft P.R., Kie J.G., Forester J.D., & Morales J.M. Stochastic modelling of animal movement. Philosophical Transactions of the Royal Society B: Biological Sciences, vol. 365, no. 1550, 2010, pp. 2201-2211.

[11]. Seidel D.P., Dougherty E., Carlson C., Getz W.M. Ecological metrics and methods for GPS movement data. International Journal of Geographical Information Science, vol. 32, no. 11, 2018, pp. 2272-2293.

[12]. Dougherty E.R., Seidel D.P., Carlson C. J., Spiegel O., & Getz W.M. Going through the motions: incorporating movement analyses into disease research. Ecology letters, vol. 21, no. 4, 2018, pp. 588-604.

[13]. Marcus Rowcliffe J., Carbone C., Kays R., Kranstauber B., & Jansen P. A. Bias in estimating animal travel distance: the effect of sampling frequency. Methods in Ecology and Evolution, vol. 3, no. 4, 2012, pp. 653-662.

[14]. Perry J.N., Liebhold A.M., Rosenberg M.S., Dungan J., Miriti M., Jakomulska A., & Citron-Pousty S. Illustrations and guidelines for selecting statistical methods for quantifying spatial pattern in ecological data. Ecography, vol. 25, no. 5, 2002, pp. 578-600.

[15]. DelCurto T., Porath M., Parsons C.T., & Morrison J.A. Management strategies for sustainable beef cattle grazing on forested rangelands in the Pacific Northwest. Rangeland Ecology & Management, vol. 58, no. 2, 2005, pp. 119-127.

[16]. Sanon H.O., Kaboré-Zoungrana C., & Ledin I. Behaviour of goats, sheep and cattle and their selection of browse species on natural pasture in a Sahelian area. Small Ruminant Research, vol. 67, no. 1, 2007, pp. 64-74.

[17]. Kilgour R.J. In pursuit of "normal": A review of the behaviour of cattle at pasture. Applied Animal Behaviour Science, vol. 138, no. 1-2, 2012, pp. 1-11.

[18]. Guo Y., Corke P., Poulton G., Wark T., Bishop-Hurley G., & Swain D. Animal behaviour understanding using wireless sensor networks. In Proc. of the 31st IEEE Conference on Local Computer Networks, 2006, pp. 607-614.

[19]. Polsky L., & von Keyserlingk M.A. Invited review: Effects of heat stress on dairy cattle welfare. Journal of dairy science, vol. 100, no. 11, 2017, pp. 8645-8657.

[20]. Beyer H.L., Haydon D.T., Morales J.M., Frair J.L., Hebblewhite M., Mitchell M., & Matthiopoulos J. The interpretation of habitat preference metrics under use–availability designs. Philosophical Transactions of the Royal Society B: Biological Sciences, vol. 365, no. 1550, 2010, pp. 2245-2254.

[21]. Johnson D.H. The comparison of usage and availability measurements for evaluating resource preference. Ecology, vol. 61, no. 1, 1980, pp. 65-71.

[22]. Rutter S.M. Diet preference for grass and legumes in free-ranging domestic sheep and cattle: current theory and future application. Applied Animal Behaviour Science, vol. 97, no. 1, 2006, pp.17-35.

[23]. Johnson C.J., & Seip D.R. Relationship between resource selection, distribution, and abundance: a test with implications to theory and conservation. Population Ecology, vol. 50, no. 2, 2008, pp. 145-157.

[24]. Awad A.I. From classical methods to animal biometrics: A review on cattle identification and tracking. Computers and Electronics in Agriculture, vol. 123, 2016, pp. 423-435.

[25]. Huhtala A., Suhonen K., Mäkelä P., Hakojärvi M., & Ahokas J. Evaluation of instrumentation for cow positioning and tracking indoors. Biosystems Engineering, vol. 96, no. 3, 2007, pp. 399-405.

[26]. Vanhelst J., Béghin L., Duhamel A., Bergman P., Sjöström M., & Gottrand F. Comparison of uniaxial and triaxial accelerometry in the assessment of physical activity among adolescents under free-living conditions: the HELENA study. BMC medical research methodology, vol. 12, no. 1, 2012.

[27]. Grundy E., Jones M.W., Laramee R. S., Wilson R.P., & Shepard E.L. Visualisation of sensor data from animal movement. In Computer Graphics Forum, vol. 28, no. 3, pp. 815-822.

[28]. Frair J.L., Fieberg J., Hebblewhite M., Cagnacci F., DeCesare N.J., & Pedrotti L. Resolving issues of imprecise and habitat-biased locations in ecological analyses using GPS telemetry data. Philosophical Transactions of the Royal Society B: Biological Sciences, vol. 365, no. 1550, 2010, pp. 2187-2200.

[29]. Tani Y., Yokota Y., Yayota M., & Ohtani S. Automatic recognition and classification of cattle chewing activity by an acoustic monitoring method with a single-axis acceleration sensor. Computers and Electronics in Agriculture, vol. 92, 2013, pp. 54-65.
[30]. Deniz N.N., Chelotti J.O., Galli J.R., Planisich A.M., Larripa M.J., Rufiner H.L., & Giovanin L.L. Embedded system for real-time monitoring of foraging behavior of grazing cattle using acoustic signals. Computers and Electronics in Agriculture, vol. 138, 2017, pp. 167-174.
[31]. Schirmann K., von Keyserlingk M.A., Weary D.M., Veira D.M., & Heuwieser W. Validation of a system for monitoring rumination in dairy cows. Journal of Dairy Science, vol. 92, no. 12, 2009, pp. 6052-6055.
[32]. Wilson R.P., & McMahon C.R. Measuring devices on wild animals: what constitutes acceptable practice? Frontiers in Ecology and the Environment, vol. 4, no. 3, 2006, pp. 147-154.
[33]. Ungar E.D., Henkin Z., Gutman M., Dolev A., Genizi A., & Ganskopp D. Inference of animal activity from GPS collar data on free-ranging cattle. Rangeland Ecology & Management, vol. 58, no. 3, 2005, pp. 256-266.
[34]. McGavin S.L., Bishop-Hurley G.J., Charmley E., Greenwood P.L., & Callaghan M.J. Effect of GPS sample interval and paddock size on estimates of distance travelled by grazing cattle in rangeland, The Rangeland Journal, vol. 40, no. 1, 2018, pp. 55-64.
[35]. Liu T., Green A.R., Rodríguez L.F., Ramirez B.C., & Shike D.W. Effects of number of animals monitored on representations of cattle group movement characteristics and spatial occupancy. PloS one, vol. 10, no. 2, 2015.
[36]. McGranahan D.A., Geaumont B., & Spiess, J.W. Assessment of a livestock GPS collar based on an open-source datalogger informs best practices for logging intensity. Ecology and Evolution, vol. 8, no. 11, 2018, pp. 5649-5660.
[37]. de Weerd N., van Langevelde F., van Oeveren H., Nolet B.A., Kölzsch A., Prins H.H., & de Boer W.F. Deriving animal behaviour from high-frequency GPS: tracking cows in open and forested habitat. PloS one, vol. 10, no. 6, 2015.
[38]. Tofastrud M., Hegnes H., Devineau O., & Zimmermann B. Activity patterns of free-ranging beef cattle in Norway. Acta Agriculturae Scandinavica, Section A — Animal Science, vol. 68, issue 1, 2018, pp. 39-47.
[39]. Meunier B., Pradel P., Sloth K.H., Cirié C., Delval E., Mialon M.M., & Veissier I. Image analysis to refine measurements of dairy cow behaviour from a real-time location system. Biosystems Engineering, vol. 173, 2018, pp. 32-44.
[40]. Larson-Praplan S., George M.R., Buckhouse J.C., & Laca E.A. Spatial and temporal domains of scale of grazing cattle. Animal Production Science, vol. 55, no. 3, 2015, pp. 284-297.
[41]. Zhao K., & Jurdak R. Understanding the spatiotemporal pattern of grazing cattle movement. Scientific reports, vol. 6, 2016.
[42]. Liao C., Clark P.E., Shibia M., & DeGloria S.D. Spatiotemporal dynamics of cattle behavior and resource selection patterns on East African rangelands: evidence from GPS-tracking. International Journal of Geographical Information Science, vol. 32, no. 7, 2018, pp. 1523-1540.
[43]. Saint-Dizier M., & Chastant-Maillard S. Methods and on-farm devices to predict calving time in cattle. The Veterinary Journal, vol. 205, no. 3, 2015, pp. 349-356.
[44]. Williams M.L., James W.P., & Rose M.T. Fixed-time data segmentation and behavior classification of pasture-based cattle: Enhancing performance using a hidden Markov model. Computers and Electronics in Agriculture, vol. 142, 2017, pp. 585-596.
[45]. Sawalhah M.N., Cibils A.F., Hu C., Cao H., & Holechek J.L. Animal-driven rotational grazing patterns on seasonally grazed New Mexico rangeland. Rangeland ecology & management, vol. 67, no. 6, 2014, pp. 710-714.
[46]. Yoshitoshi R., Watanabe N., Kawamura K., Sakanoue S., Mizoguchi R., Lee H. J., & Kurokawa Y. Distinguishing cattle foraging activities using an accelerometry-based activity monitor. Rangeland ecology & management, vol. 66, no. 3, 2013, pp. 382-386.
[47]. Thorup V.M., Munksgaard L., Robert P.E., Erhard H.W., Thomsen P.T., & Friggens N.C. Lameness detection via leg-mounted accelerometers on dairy cows on four commercial farms. Animal, vol. 9, no. 10, 2015, pp. 1704-1712.
[48]. Silper B.F., Madureira A.M.L., Kaur M., Burnett T.A., & Cerri R.L.A. Comparison of estrus characteristics in Holstein heifers by 2 activity monitoring systems. Journal of dairy science, vol. 98, no. 5, 2015, pp. 3158-3165.

[49]. Bonk S., Burfeind O., Suthar V.S., & Heuwieser W. Evaluation of data loggers for measuring lying behavior in dairy calves. Journal of Dairy Science, vol. 96, no. 5, 2013, pp. 3265-3271.

[50]. Kienitz M.J., Heins B.J., & Chester-Jones H. Growth, behavior, and economics of group-fed dairy calves fed once or twice daily in an organic production system. Journal of dairy science, vol. 100, no. 4, 2017, pp. 3318-3325.

[51]. Minnaert B., Thoen B., Plets D., Joseph W., & Stevens N. Wireless energy transfer by means of inductive coupling for dairy cow health monitoring. Computers and Electronics in Agriculture, vol. 152, 2018, pp. 101-108.

[52]. Nadimi E.S., Søgaard H.T., & Bak T. ZigBee-based wireless sensor networks for classifying the behaviour of a herd of animals using classification trees. Biosystems engineering, vol. 100, no. 2, 2008, pp. 167-176.

[53]. Reiter S., Sattlecker G., Lidauer L., Kickinger F., Öhlschuster M., Auer W., Schweinzer V., Klein-Jöbstl D., Drillich M., & Iwersen M. Evaluation of an ear-tag-based accelerometer for monitoring rumination in dairy cows. Journal of dairy science, vol. 101, no, 4, 2018, pp. 3398-3411.

[54]. Rutten C.J., Kamphuis C., Hogeveen H., Huijps K., Nielen M., & Steeneveld W. Sensor data on cow activity, rumination, and ear temperature improve prediction of the start of calving in dairy cows. Computers and Electronics in Agriculture, vol. 132, 2017, pp. 108-118.

[55]. Wolfger B., Timsit E., Pajor E. A., Cook N., Barkema H.W., & Orsel K. Accuracy of an ear tag-attached accelerometer to monitor rumination and feeding behavior in feedlot cattle. Journal of animal science, vol. 93, no. 6, 2015, pp. 3164-3168.

[56]. Dutta R., Smith D., Rawnsley R., Bishop-Hurley G., Hills J., Timms G., & Henry D. Dynamic cattle behavioural classification using supervised ensemble classifiers. Computers and Electronics in Agriculture, vol. 111, 2015, pp. 18-28.

[57]. Oudshoorn F.W., Cornou C., Hellwing A.L.F., Hansen H.H., Munksgaard L., Lund P., & Kristensen T. Estimation of grass intake on pasture for dairy cows using tightly and loosely mounted di-and tri-axial accelerometers combined with bite count. Computers and Electronics in Agriculture, vol. 99, 2013, pp. 227-235.

[58]. Stone A.E., Jones B.W., Becker C.A., & Bewley J.M. Influence of breed, milk yield, and temperature-humidity index on dairy cow lying time, neck activity, reticulorumen temperature, and rumination behavior. Journal of dairy science, vol. 100, no. 3) 2017, pp. 2395-2403.

[59]. Nogueira G., Ajmone-Marsan P., Milanesi M., Zavarez L., Aguiar T.S., Sandre D., Maioli M.A., Ferreira G., Bispo G., Stabile S., Caputo R., Toyama C., Garcia J.F., & Caputo, R. 1283 Understanding behavior patterns of cattle adaptation to heat stress. Journal of Animal Science, vol. 94, issue suppl_5, 2016, pp. 619-619.

[60]. Marchesini G., Mottaran D., Contiero B., Schiavon E., Segato S., Garbin E., Tenti S., & Andrighetto I. Use of rumination and activity data as health status and performance indicators in beef cattle during the early fattening period. The Veterinary Journal, vol. 231, 2018, pp. 41-47.

[61]. Greenwood P.L., Paull D.R., McNally J., Kalinowski T., Ebert D., Little B., Smith D.V., Rahman A., Valencia P., Ingham A.B., & Bishop-Hurley G.J. Use of sensor-determined behaviours to develop algorithms for pasture intake by individual grazing cattle. Crop and Pasture Science, vol. 68, no. 12, 2017, pp. 1091-1099.

[62]. Schirmann K., Chapinal N., Weary D.M., Heuwieser W., & Von Keyserlingk M.A. Rumination and its relationship to feeding and lying behavior in Holstein dairy cows. Journal of dairy science, vol. 95, no. 6, 2012, pp. 3212-3217.

[63]. Knight C.W., Bailey D.W., & Faulkner D. Low-Cost Global Positioning System Tracking Collars for Use on Cattle. Rangeland Ecology & Management, vol. 71, no. 4, 2018, pp. 506-508.

[64]. Curtis A.K., Scharf B., Eichen P.A., & Spiers D.E. Relationships between ambient conditions, thermal status, and feed intake of cattle during summer heat stress with access to shade. Journal of thermal biology, vol. 63, 2017, pp. 104-111.

[65]. Odadi W.O., Riginos C., & Rubenstein D.I. Tightly Bunched Herding Improves Cattle Performance in African Savanna Rangeland. Rangeland Ecology & Management, vol. 71, no. 4, 2018, pp. 481-491.

[66]. Samuels I., Cupido C., Swarts M.B., Palmer A.R., & Paulse J.W. Feeding ecology of four livestock species under different management in a semi-arid pastoral system in South Africa. African Journal of Range & Forage Science, vol. 33, no. 1, 2016, pp. 1-9.

[67]. Arcidiacono C., Porto S.M.C., Mancino M., & Cascone G. Development of a threshold-based classifier for real-time recognition of cow feeding and standing behavioural activities from accelerometer data. Computers and electronics in agriculture, vol. 134, 2017, pp. 124-134.
[68]. Barker Z.E., Diosdado J.V., Codling E.A., Bell N.J., Hodges H.R., Croft D.P., & Amory J.R. Use of novel sensors combining local positioning and acceleration to measure feeding behavior differences associated with lameness in dairy cattle. Journal of dairy science, vol. 101, no. 7, 2018, pp. 6310–6321.
[69]. Sprecher D.J., Hostetler D.E., & Kaneene J.B. A lameness scoring system that uses posture and gait to predict dairy cattle reproductive performance. Theriogenology, vol. 47, no. 6, 1997, pp. 1179-1187.
[70]. Brown-Brandl T.M., & Eigenberg R.A. Determination of minimum meal interval and analysis of feeding behavior in shaded and open-lot feedlot heifers. Transactions of the ASABE, vol. 58, no. 6, 2015, pp. 1833-1839.
[71]. Schieltz J.M., Okanga S., Allan B.F., & Rubenstein D.I. GPS tracking cattle as a monitoring tool for conservation and management. African Journal of Range & Forage Science, vol. 34, no. 3, 2017, pp. 173-177.
[72]. Valls-Fox H., Chamaillé-Jammes S., de Garine-Wichatitsky M., Perrotton A., Courbin N., Miguel E., Guerbois C., Caron A., Loveridge A., Stapelkamp B., & Muzamba M. Water and cattle shape habitat selection by wild herbivores at the edge of a protected area. Animal Conservation, vol. 21, no. 5, 2018, pp. 365–375.
[73]. Mahoney P.J., & Young, J.K. Uncovering behavioural states from animal activity and site fidelity patterns. Methods in Ecology and Evolution, vol. 8, no, 2, 2017, pp. 174-183.
[74]. Mendes E.D.M., Carstens G.E., Tedeschi L.O., Pinchak W.E., & Friend T.H. Validation of a system for monitoring feeding behavior in beef cattle. Journal of animal science, vol. 89, no. 9, 2011, pp. 2904-2910.
[75]. Curtis A.K., Scharf B., Eichen, P.A., & Spiers D.E. Relationships between ambient conditions, thermal status, and feed intake of cattle during summer heat stress with access to shade. Journal of thermal biology, vol. 63, 2017, pp. 104-111.
[76]. Oliveira B.R., Ribas M.N., Machado F.S., Lima J. A.M., Cavalcanti L.F.L., Chizzotti M.L., & Coelho S.G. Validation of a system for monitoring individual feeding and drinking behaviour and intake in young cattle. Animal, vol. 12, no. 3, 2018, pp. 634-639.
[77]. Williams L.R., Fox D.R., Bishop-Hurley G.J., & Swain D.L. Use of radio frequency identification (RFID) technology to record grazing beef cattle water point use. Computers and Electronics in Agriculture, vol. 156, 2019, pp. 193-202.
[78]. Bonk S., Burfeind O., Suthar V.S., & Heuwieser W. Evaluation of data loggers for measuring lying behavior in dairy calves. Journal of Dairy Science, vol. 96, no. 5, 2013, pp. 3265-3271.
[79]. Michelot T., Langrock R., & Patterson T.A. moveHMM: An R package for the statistical modelling of animal movement data using hidden Markov models. Methods in Ecology and Evolution, vol. 7, no. 11, 2016, pp. 1308-1315.
[80]. Calabrese J.M., Fleming C.H., & Gurarie E. ctmm: an r package for analyzing animal relocation data as a continuous-time stochastic process. Methods in Ecology and Evolution, vol. 7, no. 9, 2016, pp. 1124-1132.
[81]. LaZerte S E., Reudink M.W., Otter K.A., Kusack J., Bailey J.M., Woolverton A., Paetkau M., de Jong A., & Hill D.J. feedr and animalnexus. ca: A paired R package and user-friendly Web application for transforming and visualizing animal movement data from static stations. Ecology and evolution, vol. 7, no. 19, 2017, pp. 7884-7896.
[82]. McLean D.J., & Skowron Volponi M. A. Trajr: an R package for characterisation of animal trajectories. Ethology, vol. 124, no. 6, 2018, pp. 440-448.
[83]. Kranstauber B., Cameron A., Weinzerl R., Fountain T., Tilak S., Wikelski M., & Kays R. The Movebank data model for animal tracking. Environmental Modelling & Software, vol. 26, no. 6, 2011, pp. 834-835.
[84]. Gurarie E., Andrews R.D., & Laidre K.L. A novel method for identifying behavioural changes in animal movement data. Ecology letters, vol. 12, no. 5, 2009, pp. 395-408.
[85]. Hunter J., Brooking C., Brimblecombe W., Dwyer R.G., Campbell H.A., Watts M.E., & Franklin C.E. OzTrack--E-Infrastructure to Support the Management, Analysis and Sharing of Animal Tracking Data. In Proc. of the IEEE 9th International Conference on eScience, 2013, pp. 140-147.

[86]. Hirakawa T., Yamashita T., Tamaki T., Fujiyoshi H., Umezu Y., Takeuchi I., Matsumoto A., & Yoda K. Can AI predict animal movements? Filling gaps in animal trajectories using inverse reinforcement learning. Ecosphere, vol. 9, no. 10, 2018.

[87]. Williams M.L., Mac Parthaláin N., Brewer P., James W.P. ., & Rose M.T.A novel behavioral model of the pasture-based dairy cow from GPS data using data mining and machine learning techniques. Journal of dairy science, vol. 99, no. 3, 2016, pp. 2063-2075.

Информация об авторах / Information about authors

Годофредо Рамон ГАРАЙ АЛЬВАРЕС получил степень бакалавра в области вычислительной техники в Высшем политехническом институте им. Хосе А. Эчеверрия, Гавана, Куба в 1994 году и степень доктора философии в университете Гранады, Испания в 2012 году. В настоящее время он является доцентом факультета информатики Камагуэйского университета, Куба. Его исследовательские интересы включают изучение проблем производительности в современных компьютерах, а также моделирование и оценку производительности.

Godofredo Ramón GARAY ALVAREZ received the B.E. degree in Computer Engineering from the ISPJAE, Havana, Cuba in 1994 and the Ph.D. degree in 2012, from the University of Granada, Spain. He is currently an Assistant Professor in the University of Camaguey's Faculty of Informatics, Cuba. His research interests include studying performance bottlenecks in current computers, and performance modelling and evaluation.

Хосе Альберто БЕРТОТ ВАЛЬДЕС в настоящее время является профессором кафедры репродукции животных в Университете Камагуэй, Куба. Он получил докторскую степень в области ветеринарии в Университете Камагуэй и Института наук о животных. Исследования Бертота сосредоточены на моделях прогнозов, направленных на улучшение организации и контроля воспроизводства систем молочного скота, а также на изучение влиянии заражения паразитами на производство молока крупного рогатого скота в провинции Камагуэй.

José Alberto BERTOT VALDÉS is currently a professor of of Animal Reproduction at the University of Camaguey, Cuba. Prof. Bertot received his doctoral degree in veterinary sciences from the University of Camagüey and Institute of Animal Science. Bertot´s research focused on models for forecasts to improve the organization and control of the reproduction of dairy cattle systems and the effects of parasite infestation in the milk production of cattle of the province of Camagüey.

Карина ПЕРЕС-ТЕРУЭЛЬ в настоящее время является директором по инновациям в Открытом университете для взрослых, Доминиканская Республика. Она получила степень PhD в Университете компьютерных исследований на Кубе. Научные интересы включают нейрообразование, нечеткие когнитивные карты, программную инженерию, принятие групповых решений.

Karina PÉREZ-TERUEL is currently a Director of Innovation at Open University for Adults, Dominican Republic. She received her PhD at University for Informatics Science, Cuba. Scientific interests include neuroeducation, fuzzy cognitive maps, software engineering, group decision making.

DOI: 10.15514/ISPRAS-2019-31(2)-11

Безопасная и надежная передача данных в MANET на основе принципов вычислительно стойкого разделения секрета

[1] *Н.И. Червяков, ORCID: 0000-0002-4573-2032 <ncherviakov@ncfu.ru>*
[1] *М.А. Дерябин, ORCID: 0000-0002-6761-3667 <maderiabin@ncfu.ru>*
[1] *А.С. Назаров, ORCID: 0000-0002-0109-6097 <kapitoshking@mail.ru>*
[1] *М.Г. Бабенко, ORCID: 0000-0001-7066-0061 <mgbabenko@ncfu.ru>*
[1] *Н.Н. Кучеров, ORCID: 0000-0003-0337-0093 <nkucherov@ncfu.ru>*
[1] *А.В. Гладков, ORCID: 0000-0002-9454-7618 <agladkov@ncfu.ru>*
[2] *Г.И. Радченко, ORCID: 0000-0002-7145-5630 <gleb.radchenko@susu.ru>*

[1] *Северо-Кавказский федеральный университет,*
355009, Россия, г. Ставрополь, ул. Пушкина, д. 1.
[2] *Южно-Уральский государственный университет,*
454080, Россия, Челябинск, ул. Ленина, д. 76.

Аннотация. Мобильные неиерархические сети (MANET) требуют особых подходов к проектированию и выбору алгоритмов передачи данных и обеспечения безопасности. Мобильность узлов и динамическая топология порождают две ключевые проблемы: сложность обеспечения конфиденциальности при передаче данных через сеть и сложность организации надежной передачи данных. В данной работе предлагается новый подход к организации передачи данных в MANET, базирующийся на многопутевой маршрутизации с разделением узлов и кодированием информации в системе остаточных классов. Распределенное кодирование позволяет использовать схемы разделения секрета, с одной стороны, для обеспечения конфиденциальности и с другой – для помехоустойчивого кодирования. В работе предлагается использовать вычислительно стойкую схему разделения секрета на основе системы остаточных классов, которая обеспечивает конфиденциальность данных и надежность их передачи и позволяет сбалансировать нагрузку в сети.

Ключевые слова: мобильные децентрализованные неиерархические сети; MANET; модулярная арифметика; система остаточных классов; схемы разделения секрета; вычислительно стойкое разделение секрета; распределенная передача данных

Для цитирования: Червяков Н.И., Дерябин М.А., Назаров А.С., Бабенко М.Г., Кучеров Н.Н., Гладков А.В., Радченко Г.И. Безопасная и надежная передача данных в MANET на основе принципов вычислительно стойкого разделения секрета. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 153-170. DOI: 10.15514/ISPRAS-2019-31(2)-11

Благодарности. Работа выполнена при поддержке РФФИ, проект № 18-07-00109, при поддержке Гранта Президента Российской Федерации, проект МК-6294.2018.9 и проект СП-1215.2016.

Secure and Reliable Data Transmission Over MANET Based On Principles of Computationally Secure Secret Sharing

[1] *N.I. Chervyakov, ORCID: 0000-0002-4573-2032 <ncherviakov@ncfu.ru>*
[1] *M.A. Deryabin, ORCID: 0000-0002-6761-3667 <maderiabin@ncfu.ru>*
[1] *A.S. Nazarov, ORCID: 0000-0002-0109-6097 <kapitoshking@mail.ru>*
[1] *M.G. Babenko, ORCID: 0000-0001-7066-0061 <mgbabenko@ncfu.ru>*
[1] *N.N. Kucherov, ORCID: 0000-0003-0337-0093 <nkucherov@ncfu.ru>*
[1] *A.V. Gladkov, ORCID: 0000-0002-9454-7618 <agladkov@ncfu.ru>*
[2] *G.I. Radchenko, ORCID: 0000-0002-7145-5630 <gleb.radchenko@susu.ru>*

[1] *North-Caucasus Federal University,*
1, Pushkin Street, Stavropol, 355009, Russia
[2] *South Ural State University,*
76, Lenin Prospekt, Chelyabinsk, 454080, Russia

Abstract. Mobile Ad-Hoc Networks (MANET) require special approaches to the design and selection of data transmission and security algorithms Nodes mobility and dynamic topology give rise to two key problems of MANET – the difficulty of ensuring confidentiality when transmitting data through a network and the complexity of organizing reliable data transfer. This paper proposes a new approach to organizing data transfer through MANET, based on node disjoint multipath routing and modular coding of data. Distributed modular coding allows the use of secret-sharing schemes to ensure confidentiality on the one hand and reliable coding on the other hand. In this paper, a Computationally Secure Secret Sharing Scheme based on the Residue Number System is used, which ensures the confidentiality of data and the reliability of their transmission. Such an approach also allows for balancing the network loading.

Keywords: Mobile Ad-Hoc Networks; MANET; modular arithmetic; Residue Number System; Secret Sharing Schemes; Computationally Secure Secret Sharing; distributed data transmission

For citation: Chervyakov N.I., Deryabin M.A., Nazarov A.S., Babenko M.G., Kucherov N.N., Gladkov A.V., Radchenko G.I. Secure and Reliable Data Transmission Over MANET Based On Principles of Computationally Secure Secret Sharing. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 153-170 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-11

Acknowledgements. The work was supported by the Russian Foundation for Basic Research, project No. 18-07-00109, and Grants of the President of the Russian Federation, project MK-6294.2018.9 and project SP-1215.2016.

1. Введение

Постоянная миниатюризация и увеличение вычислительной мощности мобильных и встраиваемых устройств накладывают все возрастающие требования на мобильные беспроводные сети. В ряде приложений, таких как сети быстрого развертывания, беспроводные сенсорные сети, Интернет вещей требуется специальная архитектура мобильной беспроводной сети, в которой предполагается децентрализация и самоорганизация узлов сети. Сети такого типа называются Mobile Ad-Hoc Networks (MANET) – мобильные децентрализованные неиерархические сети, или мобильные сети по требованию.

Особенность MANET заключается в том, что в таких сетях каждое устройство или узел является максимально самостоятельным и независимым, а связь с другими узлами происходит по требованию с использованием беспроводных коммуникаций. Это приводит к тому, что MANET обладает динамической топологией, то есть мобильные узлы могут перемещаться, исключаться и добавляться. Такие условия усложняют многие процессы, связанные с функционированием сети. К ним относятся маршрутизация, аутентификация, безопасная и надежная передача данных. Отсутствие единого центра в таких сетях возлагает эти задачи на каждый отдельный узел. В отличие от традиционных типов сетей,

основные функции управления в сетях MANET выполняются совместно всеми доступными узлами. Узлы в MANET используют связь через несколько хостов: узлы, которые находятся в пределах диапазона беспроводного соединения друг друга могут напрямую взаимодействовать через беспроводные каналы, тогда как те, которые находятся далеко друг от друга, должны полагаться на промежуточные узлы, которые действуют как маршрутизаторы для ретрансляции сообщений. В связи с этим сети MANET уязвимы к атакам и помехам, что приводит к необходимости разработки специальных методов передачи данных [1].

В этой статье описан новый подход к передаче данных через MANET, обеспечивающий одновременно ее безопасность и надежность. Предлагаемый метод основывается на многопутевой маршрутизации с разделением узлов (Node-Disjoint Multipath Routing [2]), которая позволяет разделить данные между узлами таким образом, чтобы контролировать количество информации, получаемое каждым из них. Он позволяет обеспечивать конфиденциальность передаваемых данных за счет алгоритмов порогового разделения секрета [3].

Основой предлагаемого метода является система остаточных классов (СОК), которая зарекомендовала себя как надежный и эффективный инструмент проектирования схем разделения секрета (СРС), обладающих определенными свойствами. Большинство совершенных схем разделения секрета (ССРС) не пригодны для передачи данных в MANET, так как приводят к их высокой избыточности [4]. В свою очередь, вариант вычислительно стойкой схемы разделения секрета на основе СОК [5] позволяет решить эту проблему. Кроме того, избыточная система остаточных классов обладает корректирующими свойствами [6], которые позволят сохранить целостность информации в случае потери части пакетов. В данной работе описан подход к кодированию и передаче данных через MANET, позволяющий с одной стороны обеспечить конфиденциальность информации, с другой – защитить ее от потери или повреждения в процессе передачи.

2. Методы обеспечения надежной и безопасной передачи данных в MANET

Устройства сети MANET максимально упрощены для минимизации их размера и энергопотребления, что не может не отразиться на применяемых алгоритмах. Например, при использовании симметричного или ассиметричного шифрования в качестве метода обеспечения конфиденциальности может возникнуть сразу ряд проблем, связанных с управлением ключами [1]. Децентрализация и равноправность узлов осложняет обмен ключами между источником и приемником данных – буквально каждый узел посредник, участвующий в процессе обмена, может ему помешать или тем или иным способом получить доступ к ключам. Сложность аутентификации и динамическая топология делает возможной атаку «человек посередине», при которой один из узлов посредников может подменить ключи для получателя и приемника и вторгнуться в процесс обмена данными. С другой стороны, удовлетворение ограничениям на ресурсы может понизить стойкость алгоритмов.

Для обеспечения безопасности в MANET используется множество различных подходов. Связано это с множеством различных угроз, которым подвергнуты сети такого типа. Большинство протоколов и методов нацелены на решение узкой проблемы и способны бороться лишь с угрозами определенного характера. Например, важным направлением исследований является определение вторжений на основе подозрительных действий узлов. Такие методы используют машинное обучение и статистический анализ [7,8]. Они подходят лишь в определенных случаях и не могут служить основой безопасной и надежной передачи данных.

Общей чертой всех алгоритмов является учет специфических особенностей MANET. Не существует единого центра сертификации и аутентификации, в связи с этим необходимы распределенные алгоритмы. Так, алгоритм, предложенный в [9], использует пороговую криптографию и схемы разделения секрета для организации групповой сертификации в целях предотвращения вторжения.

Существуют ситуации, когда необходимо скрыть передаваемую информацию даже от промежуточных узлов сети, прошедших сертификацию. В таком случае необходимо использовать шифрование данных, которое затруднительно для децентрализованных сетей. Остается вероятность подслушивания и мониторинга трафика, так как в реальных условиях ни одному промежуточному узлу нельзя доверять. Например, при использовании сетей быстрого развертывания на основе MANET во время экстремальных ситуаций, каждый узел может потенциально быть захвачен, продолжая при этом проходить проверки безопасности и функционировать в нормальном режиме.

В основе функционирования MANET лежат специальные протоколы маршрутизации, адаптированные к динамической топологии. Все процессы, включая обмен данными, обеспечение надежности и безопасности сети передачи данных, ориентируются на тот или иной протокол маршрутизации. В зависимости от структуры сети, используемых устройств и решаемых сетью задач применяется один из двух типов протоколов маршрутизации – реактивные и проактивные. Реактивные позволяют строить маршруты «на лету», пользуясь для каждого узла лишь информацией о доступных для передачи данных в текущий момент времени соседних узлах. К таким алгоритмам относятся основные алгоритмы MANET, такие как AODV [10] и DSR [11]. В проактивных протоколах данные о структуре сети периодически собираются каждым узлом, на основе чего составляется таблица маршрутизации, позволяющая строить эффективные маршруты и балансировать нагрузку сети. Одним из основных направлений обеспечения надежности и безопасности передачи данных является использование специальных подходов к маршрутизации [12, 13].

Каждый тип протоколов обладает преимуществами и недостатками. Кроме того, существуют специальные атаки на протоколы маршрутизации, способные негативно повлиять на работу сети: изменить маршруты, создать петли при передаче пакетов, перегрузить сеть для снижения ее эффективности, внести ошибки в построение маршрутов передачи данных и т.п.

В связи с этим разрабатываются различные защищенные протоколы маршрутизации [14-16]. К таким протоколам можно отнести протокол ARIADNE, который использует симметричное шифрование для передачи данных и распределение ключей с использованием схем разделения секрета [17]. Проблема защищенной маршрутизации напрямую связана с аутентификацией пользователей, для которой разработаны специальные методы коллективной аутентификации, адаптированные для MANET [18].

Динамический характер узлов сети MANET, возможность перемещения и потери связи с узлом во время передачи данных или на этапе построения маршрута, вносит дополнительные угрозы целостности и доступности передаваемых данных. Любой передаваемый пакет может быть потерян в связи с изменением топологии сети.

Для борьбы с данным явлением и с целью разгрузки сети были предложены многопутевые (Multi-Path) алгоритмы маршрутизации для MANET (Рис. 1а). Подобные методы позволяют строить несколько маршрутов доставки сообщений, что с применением дополнительных алгоритмов избыточного кодирования [19] позволяет снизить вероятность потери данных при передаче и перераспределить нагрузку в сети. Чаще всего используются многопутевые алгоритмы маршрутизации, основанные на реактивных алгоритмах маршрутизации AOMDV [20] и MP-DSR [21]. Сочетание многопутевой маршрутизации с кодами стирания и избыточным кодированием позволяет значительно увеличить вероятность доставки сообщений – основного параметра надежности сети [22-25].

Однако заметим, что в общем случае четких требований к строящимся маршрутам не предъявляется. Так, на рис. 1a показан пример, в котором доставка частей сообщения s_1, s_2 и s_3 из источника S в приемник D происходит по одним из наиболее эффективных маршрутов. Части сообщения s_1 и s_2 объединяются на узле 10 с целью сокращения маршрута и числа промежуточных узлов и далее передаются либо как единое сообщение, либо по очереди. Такой подход может быть использован для повышения скорости передачи данных по сети, однако неблагоприятно сказывается на надежности передачи. Кроме того, ситуация в примере (рис. 1a) осложняет использование схем разделения секрета для обеспечения конфиденциальности или распределения ключей на основе полученных маршрутов, так как узлы, через которые передаются объединенные сообщения $s_1 + s_2$, получают большее количество информации об исходном секрете (в данном примере – узлы 9 и 10), что является нарушением основных требований пороговой криптографии.

Для повышения надежности передачи данных разработаны еще несколько категорий алгоритмов многопутевой маршрутизации. Важное значение имеют алгоритмы с разделением по маршрутам (Link-Disjoint Multi-Path Routing, рис. 1b), в которых узел может входить одновременно в несколько маршрутов с целью повышения производительности сети и надежности передачи данных (в примере на рис. 1b – узел 10), однако требуется, чтобы различные маршруты не содержали общих соединений между узлами (общих ребер). В приведенном примере сообщение s_1 и сообщение s_2 передаются каждое в соответствии с выделенным для него маршрутом (не объединяясь на узле 10). Примерами алгоритмов с разделением по маршрутам являются AOMDV [18], SMR [26], MP-DSR [21]. Такой подход позволяет сократить время реконструкции маршрутов в случае, если один из маршрутов станет недоступен.

Другой тип многопутевых алгоритмов маршрутизации – многопутевая маршрутизация с разделением узлов (Node-Disjoint Multi-Path Routing) [2], в которой каждый из построенных маршрутов не содержит узлов, входящих в любой другой маршрут (AODVM [27], EMPR [28]).

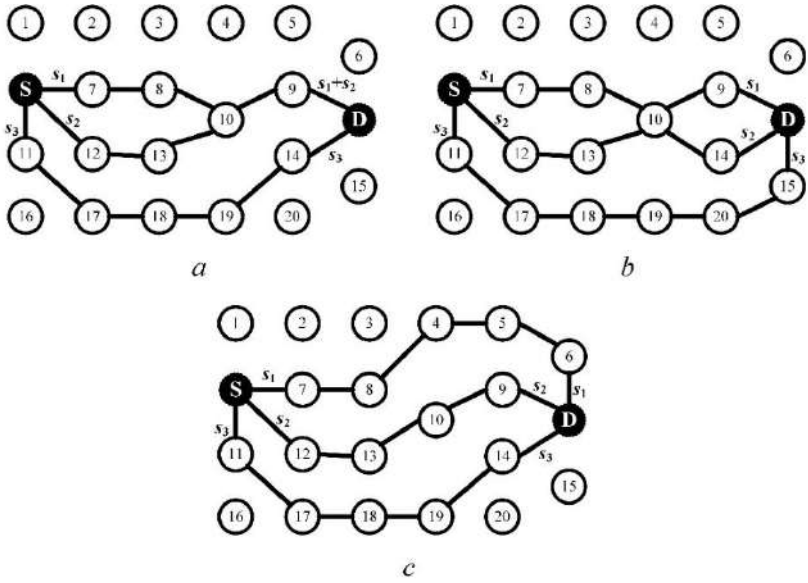


Рис. 1. Различные методы многопутевой маршрутизации: a – общий случай, b – с разделением по маршрутам, c – с разделением по узлам.
Fig. 1. Different types of Multi-Path Routing: a – general case, b – Link-Disjoint, c – Node-Disjoint.

На рис. 1с продемонстрирован пример маршрутов, построенных согласно подобным методам. Отметим, что нет ни одного узла, который получал бы одновременно несколько частей сообщения s_1, s_2 и s_3, кроме приемника D, которому передаваемые данные и пересылаются. Такие протоколы применяются для снижения влияния отдельных узлов на передачу данных, позволяют разгрузить узлы и сеть в целом, снизить общее энергопотребление, однако являются более сложными в реализации и не позволяют строить максимально эффективные сети в плане скорости и надежности передачи данных.

Маршрутизация с разделением узлов является основой для разработки алгоритмов распределенной передачи данных, которые решают одновременно две задачи: обеспечивают надежность передачи данных с одной стороны и конфиденциальность с другой.

В данной работе предлагается использовать вычислительно стойкие схемы разделения секрета и систему остаточных классов (СОК) с целью минимизации вероятности раскрытия или изменения передаваемых данных, перехвата трафика, потери или нарушения целостности данных в процессе передачи.

3. Система остаточных классов и схемы разделения секрета

В качестве основы кодирования информации при передаче через MANET предлагается использовать кодирование в системе остаточных классов (СОК), обладающее целым рядом важных особенностей:

- эффективность кодирования и декодирования, параллелизм кода СОК [29];
- возможность восстановить данные в случае потери некоторых частей за счет избыточного кодирования [30];
- возможность коррекции ошибок, позволяющей отследить изменение данных в результате диверсии или повреждения, за счет избыточного кодирования [6];
- возможность использования СОК в качестве основы для схемы разделения секрета [5].

Система остаточных классов является распространенным инструментом обеспечения конфиденциальности, доступности и целостности данных [31, 32], в частности СОК используется для обеспечения надежности Интернета вещей [33] и безопасного распределения ключей в MANET [34].

Система остаточных классов – это непозиционная система счисления, основанная на непозиционном представлении чисел. СОК определяется набором из n взаимно простых оснований $\{m_1, m_2, \dots, m_n\}$. Позиционное число A из интервала $[0, M)$, где $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$, можно однозначно представить в виде кортежа из n чисел $(a_1, a_2, \dots, a_n)$, где

$$a_i = A \bmod m_i, \qquad i = 1,2, \dots, n$$

Непозиционное представление обеспечивает высокоэффективную параллельную обработку данных, помехоустойчивое кодирование и криптографию, что делает СОК полезной во множестве приложений [29, 35, 36].

Избыточная СОК (ИСОК) определяется на основе исходной СОК с модулями $\{m_1, m_2, \dots, m_n\}$ путем добавления избыточных модулей $m_{n+1}, m_{n+2}, \dots, m_{n+r}$, каждый из которых превышает по величине любой из исходных модулей, и расширения представления числа A на r дополнительных оснований. Новый набор $(a_1, a_2, \dots, a_n, a_{n+1}, \dots, a_{n+r})$ обладает следующими важными свойствами:

- потеря любых r или менее остатков в представлении числа A в СОК не приводит к потере данных, так как A можно восстановить по любым оставшимся n остаткам;
- если любые r остатков были в процессе передачи данных изменены, это может

быть обнаружено с помощью специальных алгоритмов [35];

- если изменены были любые $\lfloor r/2 \rfloor$ или менее остатков, их можно обнаружить и либо декодировать данные, исключив поврежденные остатки, либо исправить эти остатки с применением специальных алгоритмов [6].

Основную сложность при реализации систем, основанных на кодировании в СОК, представляет выбор метода обратного перевода, который может быть основан на различных техниках [37]. При этом существуют методы, объединяющие обнаружение ошибок и декодирование информации из ИСОК.

На основе системы остаточных классов строятся как различные схемы разделения секрета, так и схемы распределения данных. Под пороговой схемой разделения секрета понимается протокол распределения информации (секрета) на части таким образом, чтобы восстановить исходный секрет можно было бы только при объединении подмножества частей, размер которого превышает заранее заданный порог.

Основной атакой на схемы разделение секрета является сговор неразрешенной коалиции с возможность объединить произвольное количество частей. Для такой коалиции, обладающей некоторым количеством частей секрета, должно быть затруднительным восстановить исходный секрет. По степени стойкости к атакам такого рода принято разделять схемы разделения секрета на несколько классов. Среди них можно выделить совершенные схемы разделения секрета на основе СОК (схема Асмута-Блума [38, 39]), которые позволяют максимально обезопасить данные от раскрытия при отсутствии достаточного количества частей. Такие схемы позволяют максимально обезопасить секрет в условиях его распределенного представления, однако приводят к большой избыточности [4].

В противоположность таким схемам, в сетях передачи данных часто используются схемы распределения данных [40], которые позволяют увеличить надежность передачи, не заботясь о конфиденциальности информации. При этом такие схемы минимально избыточны. К данному классу можно отнести «чистый» СОК как метод кодирования данных. Однако такое представление небезопасно, так как, основываясь на остатках, злоумышленник может получить частичный доступ к данным и анализировать содержимое пакета, что нарушает условия конфиденциальности. Тем не менее, определенную надежность подобные схемы обеспечивают.

Компромиссом являются вычислительно стойкие схемы разделения секрета [4], которые обеспечивают достаточную конфиденциальность при сравнительно небольшой избыточности. Примером может быть основанная на СОК AC-RRNS, предложенная в работе [41] как метод кодирования для облачного хранения данных. Другая вычислительно стойкая схема разделения секрета предложена в работе [5] и основывается на симметричном шифровании и распределении данных с помощью СОК. Такая методика обеспечивает минимальную накладную избыточность, обеспечивая высокий уровень конфиденциальности и стойкости.

Преимуществом вычислительно стойких схем разделения секрета на основе СОК является возможность сочетания всех преимуществ СОК как системы представления данных: высокой эффективности кодирования и декодирования, корректирующих свойств для контроля целостности информации и различных вариантов схем разделения секрета для обеспечения конфиденциальности.

4. Принципы безопасной и надежной распределенной передачи данных в MANET

Система остаточных классов позволяет решить целый класс задач и обеспечить одновременно целостность, доступность и конфиденциальность данных. Такие свойства

делают ее эффективным инструментом обеспечения надежности и безопасности при передаче данных в MANET. В данном разделе рассмотрены принципы, лежащие в основе предлагаемого метода передачи данных в неиерархической сети.

В первую очередь отметим, что важную роль играет выбранный протокол маршрутизации. К нему предъявляется два основных требования: данный протокол должен быть многопутевым, и при этом построенные маршруты не должны пересекаться по узлам (рис. 1c). Эти требования принципиально необходимы для того, чтобы обеспечить конфиденциальность передачи информации при использовании схем разделения секрета.

В [5] предложена вычислительно стойкая схема разделения секрета, которая отвечает всем требованиям MANET. Для ее реализации необходимо выбрать надежную симметричную схему шифрования, совершенную схему разделения секрета и систему остаточных классов с компактным набором модулей. Под компактным [42] понимается набор модулей $\{m_1, m_2, \dots, m_n, m_{n+1}, \dots, m_{n+r}\}$, для которого $m_{n+r} < m_1 + \theta m_1$, где $0 < \theta < 1$. Иными словами, для обеспечения необходимого уровня безопасности модули должны быть близки друг к другу по величине.

Сочетание многопутевой маршрутизации, вычислительно стойкого разделения секрета и корректирующих способностей СОК позволяет применить новый подход к передаче данных, обеспечивающий одновременно высокую надежность передачи данных и высокий уровень конфиденциальности.

Основные принципы предлагаемого подхода заключены в следующем:

1) Передаваемое сообщение делится на равные блоки величины M, для обеспечения возможности их представления как чисел в СОК.
2) Информация шифруется с использованием любого надежного алгоритма симметричного шифрования и ключа K, который может быть использован одновременно для нескольких блоков с целью уменьшения избыточности.
3) Зашифрованные данные разделяются с использованием СОК с модулями $\{m_1, m_2, \dots, m_n, m_{n+1}, \dots, m_{n+r}\}$.
4) Ключ K, используемый для шифрования исходных данных, разделяется на основе совершенной схемы Асмута-Блума с целью обеспечения максимальной конфиденциальности ключевой информации.
5) Каждая часть секрета, составленная из части ключа и остатка от зашифрованных данных по одному из модулей, отправляется отдельным ассоциированным с данным модулем маршрутом, полученным согласно алгоритму, поддерживающему многопутевую маршрутизацию с разделением по узлам.
6) Получив все возможные части секрета или часть из них в случае, если некоторые не были доставлены в отведенный период ожидания сообщений, узел-приемник может провести процедуры верификации, основанные на корректирующих способностях системы остаточных классов, для контроля корректности и целостности полученных данных.
7) Удостоверившись в корректности и целостности достаточного количества частей секрета, узел-приемник способен восстановить каждый из зашифрованных блоков данных на основе их кода в СОК.
8) Для восстановления исходных передаваемых данных приемнику необходимо расшифровать полученную информацию, используя восстановленный ключ, разделенный совершенной схемой разделения секрета.
9) На основе служебной информации блоки собираются в исходное сообщение, которое передавал источник.

На рис. 2 представлена обобщенная схема предлагаемого метода передачи данных. В его основе лежит шифрование, кодирование и разделение зашифрованных данных с помощью СОК. Ключ должен быть сгенерирован сразу для нескольких частей секрета, так как его размер так же влияет на избыточность схемы, а вместе с ней и на загруженность сети в целом. Остатки от зашифрованных блоков данных, полученные согласно ИСОК, и части ключа шифрования, полученные при применении совершенной схемы разделения секрета (CCPC, PSSS), образуют части секрета, каждая из которых передается по одному из нескольких заранее построенных маршрутов, не имеющих пересечений по узлам. Приемник, получив все доступные ему части секрета, производит восстановление секрета, выполняя в случае необходимости процедуру помехоустойчивого декодирования. Исходный секрет получается в результате дешифрования декодированных из ИСОК данных с использованием восстановленного ключа шифрования.

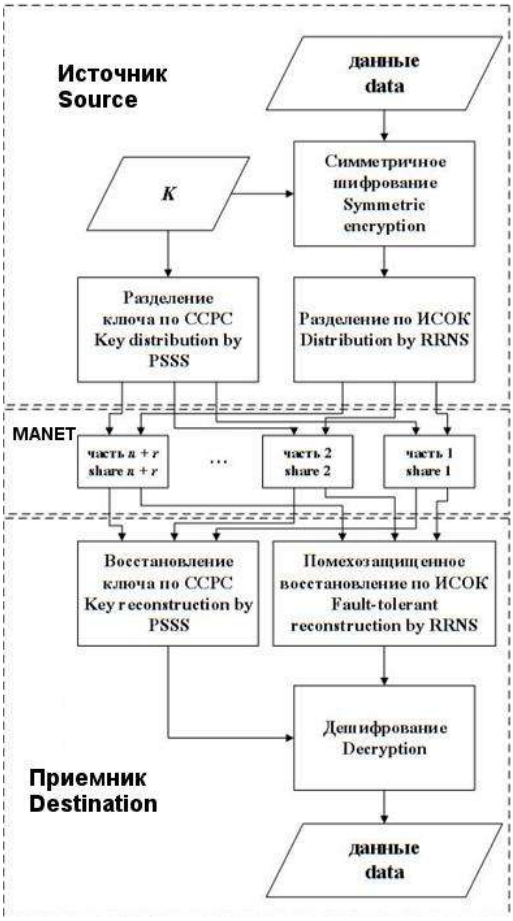


Рис. 2. Обобщенная схема безопасной и надежной передачи данных в MANET на основе вычислительно стойкой схемы разделения секрета
Fig. 2. Generalized scheme of the secure and reliable data transmission over MANET based on computationally secure secret sharing scheme

Кроме того, на основе СОК можно строить взвешенную схему разделения секрета [43]. Используя служебную информацию выбранного алгоритма маршрутизации, такую как вес маршрута, длина маршрута или надежность маршрута (в случае использования безопасного алгоритма маршрутизации), можно использовать особенности СОК для балансирования

нагрузки в сети. Например, с наиболее коротким маршрутом можно ассоциировать наибольший модуль СОК. Удельный вес информации для такого маршрута будет наибольшим, но так как такой маршрут эффективнее остальных, передача по нему будет вестись быстрее. Выбрав эффективную стратегию ассоциирования модулей с маршрутами, можно добиться повышения качества и скорости передачи и общей разгрузки сети передачи данных.

В то же время, часть секрета, представленная по наименьшему модулю, несет меньше информации об исходном секрете, чем информация по большему модулю. Этот факт можно использовать для регулирования потока информации с целью повысить безопасность передачи данных, отправляя по наименее надежному согласно некоторому критерию маршруту части секрета наименьшего размера.

5. Анализ безопасности и надежности

Ключевой особенностью предлагаемого подхода является сочетание высокой надежности и конфиденциальности, обеспечиваемое несколькими факторами. Надежность предлагаемого подхода базируется на надежности многопутевой маршрутизации и надежности кодирования информации в СОК. Согласно [21], надежность конкретного набора маршрутов W зависит от надежности каждого из построенных маршрутов следующим образом:

$$R(t) = 1 - \prod_{\omega \in W} \left(1 - \Pi_{S,D}^{\omega}(t)\right),$$

где $\Pi_{S,D}^{\omega}(t) = \prod_{\{a,b\} \in \omega} A_{a,b}(t)$ – надежность отдельно взятого маршрута $w \in W$, которая является произведением доступностей $A_{a,b}$ каждого из соединений между узлами a и b в определенный момент времени t.

Из формулы следует, что с увеличением количества маршрутов увеличивается надежность передачи данных. При этом использование системы остаточных классов повышает надежность передачи данных за счет избыточного помехоустойчивого кодирования. СОК позволяет контролировать не только ситуацию с потерей доступности отдельного узла или соединения, но и случаи повреждения или намеренной порчи информации.

Теперь рассмотрим безопасность передачи данных через MANET предложенным методом. Как было отмечено ранее, безопасность базируется на стойкости схемы разделения секрета, основанной на СОК. Используемая вычислительно стойкая схема разделения секрета обладает достаточным уровнем безопасности, не приводя при этом к высокой избыточности, в отличие от совершенных схем разделения секрета [5]. За счет свойств СОК данная схема позволяет не только защищенно передавать данные в сетях такого типа, но и балансировать нагрузку, используя распределенную передачу данных, разделенных на относительно небольшие части.

Стойкость конкретной конфигурации сети зависит от устойчивости каждого узла к захвату, топологии сети, количества построенных разделенных по узлам маршрутов, конфигурации схемы разделения секрета и выбора модулей системы остаточных классов. Необходимо учитывать, что условием перехвата данных (и вместе с тем нарушения конфиденциальности) является перехват любого количества узлов на n или более маршрутах. Учитывая, что заранее неизвестно, какие именно узлы будут перехвачены, невозможно выбрать и исключить в протоколе передачи данных скомпрометированный маршрут.

Для расчета вероятности P безопасной передачи данных (то есть вероятности, что передаваемые данные не будут перехвачены в течение времени равного T_0), введем следующие обозначения: p – устойчивость узла к перехвату данных (то есть вероятность

того, что в течение времени равного T_0 данные на узле не будут перехвачены), n – количество рабочих модулей, r – количество избыточных модулей, m_i – модули ИСОК ($i = 1 \ldots n + r$).

Рассмотрим пример расчета вероятности P безопасной передачи данных для случая с одинаковым количеством узлов на каждом из маршрутов. Отметим, что количество узлов на каждом из маршрутов может быть разным, и предложенный подход может быть расширен для случая с произвольным количеством узлов на каждом из маршрутов.

Пусть в результате работы выбранного протокола маршрутизации мы получили четыре возможных маршрута передачи данных, на каждом из которых имеется по два узла, с устойчивостью к перехвату $p = 0.99$. Следует учитывать, что данная величина является предполагаемой для возможности проведения расчетов в данном примере и в реальных условиях будет отличаться. Используем подходящую конфигурацию избыточной СОК, например, (3,4), то есть с тремя рабочими и одним избыточным модулями. Остатки по каждому из модулей будем передавать по разным маршрутам. Каждому узлу присвоим свой номер node_{ij}, где i – номер маршрута, j – порядковый номер узла на этом маршруте (рис. 3).

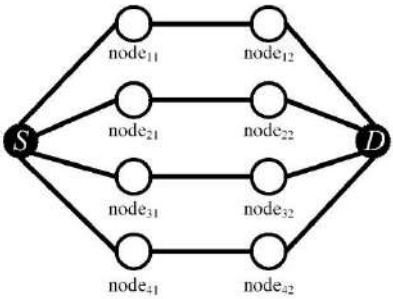


Рис. 3. Пример маршрутизации с 4 маршрутами без пересечения по узлам и 8 промежуточными узлами (по 2 на каждом из маршрутов)

Fig. 3. Routing example for 4 node-disjoint routes and 8 intermediary nodes (2 per each route)

Для расчета вероятности P безопасной передачи данных, вычислим вероятность перехвата $1 - P$. Перехват данных на любом из узлов маршрута будет означать утрату конфиденциальности данных, передаваемых этим маршрутом. В рассматриваемом примере для восстановления передаваемых с помощью избыточной СОК данных необходимо перехватить данные не менее чем на трех различных маршрутах (по числу рабочих модулей n, минимально необходимому для восстановления). Поэтому вероятность перехвата данных при захвате менее чем трех узлов равна нулю и не учитывается.

Если злоумышленником захвачены ровно три узла, то существует два варианта:

- злоумышленник сможет восстановить исходное сообщение, например, если будут захвачены узлы node_{11}, node_{21}, node_{42};
- злоумышленник не сможет восстановить исходное сообщение, например, если будут захвачены узлы node_{11}, node_{12}, node_{22}.

Иными словами, среди всех перестановок из 8 узлов по 3 с повторениями узлов лишь часть приведет к перехвату данных. Количество комбинаций из трех захваченных узлов, приводящих к перехвату (обозначим эту величину через E_3), умноженное на вероятность перехвата ровно трех узлов, даст вероятность перехвата данных при перехвате любых трех узлов:

$$P_3 = Q_3 E_3$$

где $Q_3 = (1-p)^3 p^5$ – вероятность перехвата ровно трех узлов. В общем случае, вероятность перехвата i узлов рассчитывается для рассматриваемого примера по формуле $Q_i = (1-p)^i p^{8-i}$.

Для рассматриваемого примера $E_3 = 32$, тогда

$$P_3 = 32 \cdot (1-0.99)^3 \cdot 0.99^5 = 0.0000304316816$$

Если были перехвачены ровно четыре узла, то также существуют два варианта:

- злоумышленник сможет восстановить исходные данные, например, если будут захвачены узлы node_{11}, node_{12}, node_{21}, node_{42};
- злоумышленник не сможет восстановить исходные данные, например, если будут захвачены узлы node_{11}, node_{12}, node_{21}, node_{22}.

Количество комбинаций E_4 из четырех захваченных узлов, позволяющих восстановить исходные данные, умноженное на вероятность перехвата ровно четырех узлов, даст вероятность перехвата данных при перехвате любых четырех узлов:

$$P_4 = Q_4 E_4$$

Для рассматриваемого примера $E_4 = 64$ и $P_4 = 6.147814464 \cdot 10^{-7}$.

Отдельного внимания заслуживает случай, если перехвачены пять и более узлов. В данной ситуации любая комбинация захваченных узлов даст злоумышленнику возможность восстановить исходные данные. Для таких случаев количество комбинаций захваченных узлов, позволяющих восстановить исходное сообщение, равно общему числу перестановок с повторениями из 8 узлов по 5, 6, 7 и 8 соответственно. Рассчитанные значения: $E_5 = 56$, $E_6 = 28$, $E_7 = 8$, $E_8 = 1$, тогда руководствуясь предложенным ранее подходом получаем, что $P_5 = 5.434 \cdot 10^{-9}$, $P_6 = 2.744 \cdot 10^{-11}$, $P_7 = 7.92 \cdot 10^{-14}$ и $P_8 = 10^{-16}$.

Пользуясь рассчитанными вероятностями для каждого из случаев, мы можем найти общую вероятность перехвата данных:

$$1 - P = \sum_{i=3}^{8} P_i = 0.000031052$$

Таким образом, вероятность P безопасной передачи данных равна $P = 0.999968948$.

В табл. 1 представлен расчет вероятности P безопасной передачи данных в MANET с избыточной СОК (3,4), четырьмя возможными маршрутами передачи данных и двумя узлами на каждом из маршрутов, для различных значений устойчивости одного узла к перехвату p.

Табл. 1. Вероятность P безопасной передачи данных при различной устойчивости одного узла к перехвату
Table 1. Probability P of secure data transmission at different attack resistance of the single node

i	p = 0.7		p = 0.9		p = 0.99	
	P_i	Q_i	P_i	Q_i	P_i	Q_i
0	0	0.057648	0	0.430467	0	0.922
1	0	0.024706	0	0.047829	0	0.00932
2	0	0.010588	0	0.005314	0	0.000094
3	0.145212	0.004537	0.018895	0.000590	0.0000304	$9.509 \cdot 10^{-7}$
4	0.124467	0.001944	0.004199	0.000065	$6.147 \cdot 10^{-7}$	$9.605 \cdot 10^{-9}$
5	0.046675	0.000833	0.000408	0.000007	$5.433 \cdot 10^{-9}$	$9.702 \cdot 10^{-11}$
6	0.010001	0.000357	0.000022	$8.1 \cdot 10^{-7}$	$2.744 \cdot 10^{-11}$	$9.801 \cdot 10^{-13}$
7	0.001224	0.000153	$7.2 \cdot 10^{-7}$	$9 \cdot 10^{-8}$	$7.92 \cdot 10^{-14}$	$9.9 \cdot 10^{-15}$
8	0.0000656	0.000065	10^{-8}	10^{-8}	10^{-16}	10^{-16}
	P = 0.672352030		P = 0.976473630		P = 0.9999689481	

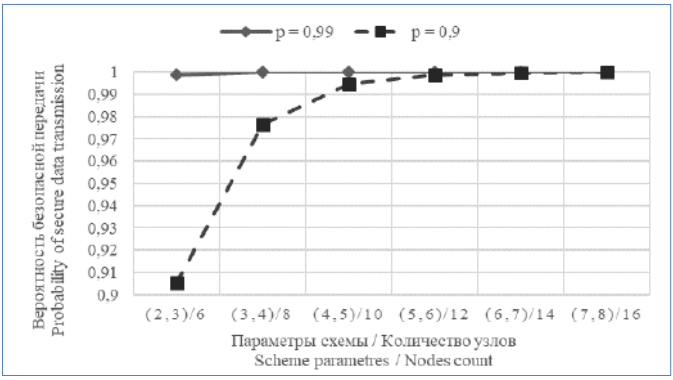


Рис. 4. Вероятность безопасной передачи данных при различном количестве маршрутов и общем количестве узлов
Fig. 4. The probability of secure data transmission with a different number of routes and the total number of nodes

В примере продемонстрирован подход к оценке вероятности безопасной передачи данных в MANET для конкретных параметров сети и избыточной системы остаточных классов. Из табл. 1 видно, что вероятность перехвата i узлов Q_i является наибольшей для $i = 1$ или $i = 2$ узлов, однако в этом случае перехватить данные, передаваемые согласно предлагаемой схеме невозможно.

Вероятность перехвата более чем $i = 2$ узлов быстро уменьшается, что уменьшает общую вероятность перехвата данных P_i при количестве возможных перехваченных узлов i.

Продолжая данный анализ, отметим, что с увеличением количества возможных маршрутов и соответствующими изменениями в параметрах СОК, вероятность безопасной передачи данных возрастает. Этот факт отражен на рис. 4 и в табл. 2. Из графика видно, что чем больше узлов задействовано в построении маршрутов и чем больше маршрутов построено, тем более безопасным является предлагаемый подход. Табл. 2 показывает, что вероятность безопасной передачи растет достаточно быстро и приближается к 1 с увеличением количества маршрутов.

Табл. 2. Вероятность P безопасной передачи данных при различном количестве маршрутов и общем количестве узлов
Table 2. Probability P of secure data transmission at different number of routes and total number of nodes

параметры схемы (n, $n + r$) / количество узлов	Вероятность безопасной передачи данных P	
	при стойкости узла $p = 0.9$	при стойкости узла $p = 0.99$
(2, 3) / 6	0.90541800	0.998827731
(3, 4) / 8	0.97647363	0.999968948
(4, 5) / 10	0.99447439	0.999999228
(5, 6) / 12	0.99874957	0.999999982
(6, 7) / 14	0.99972431	1
(7, 8) / 16	0.99994038	1

Учитывая, что для большинства систем, основанных на MANET и применяющих тот или иной способ коллективной аутентификации, перехват большого количества узлов является маловероятным событием, предлагаемую схему можно использовать в реальных условиях для конфиденциальной передачи данных.

6. Заключение

Безопасность и надежность передачи данных в MANET является актуальной задачей, решение которой позволяет повысить качество сервиса для каждого приложения, использующего в своей основе неиерархические сети. Основное преимущество системы остаточных классов в качестве базы для безопасной и надежной передачи данных заключается в универсальности данного метода представления данных. С одной стороны, СОК является высокоэффективным инструментом для помехоустойчивого кодирования информации, основанного на корректирующих способностях избыточной СОК. С другой, СОК является основой для проектирования схем разделения секрета, в том числе эффективных вычислительно стойких схем. Предложенный подход к передаче данных через MANET, основанный на описанных свойствах СОК, позволяет повысить стойкость сети к атакам различного рода и конфиденциальность передачи, наряду с высокой надежностью за счет использования многопутевой маршрутизации с разделением маршрутов по узлам. Новый подход лишен недостатков, свойственных методам защищенной передачи данных, использующим традиционное шифрование: проблема управления ключами решена за счет использования схем разделения секрета, проблема возможных атак на маршруты решена за счет использования диверсифицированной многопутевой передачи.

Дальнейшая работа заключается в выработке стратегий на случаи изменений маршрутов, которые могут привести к потере свойства разделения по узлам. Кроме того, отдельного исследования требует вопрос выбора модулей СОК и динамической подстройки параметров СОК в условиях меняющейся топологии сети. При этом необходимо учитывать требования к эффективности реализации и криптографической стойкости алгоритмов. Также для максимальной эффективности и надежности передачи данных необходима разработка специализированных протоколов многопутевой маршрутизации, учитывающих взвешенный характер схем разделения секрета на основе СОК.

Список литературы/References

[1] Sen S., Clark J. A., Tapiador J. E. Security threats in mobile ad hoc networks. In Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, CRC Press, 2010, pp. 127-147.

[2] Li X., Cuthbert L. Stable node-disjoint multipath routing with low overhead in mobile ad hoc networks., In Proc. of the IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004. pp. 184-191.

[3] Shamir A. How to share a secret. Communications of the ACM, vol. 22, no. 11, 1979, pp. 612-613.

[4] Krawczyk H. Secret sharing made short. In Proc. of the Annual International Cryptology Conference, 1993. pp. 136-146.

[5] Deryabin M., Chervyakov N., Tchernykh A., Babenko M., Kucherov N., Miranda-López V., Avetisyan A. Secure Verifiable Secret Short Sharing Scheme for Multi-Cloud Storage. In Proc. of the 2018 International Conference on High Performance Computing & Simulation (HPCS), 2018. pp. 700-706.

[6] Goh V.T., Siddiqi M.U. Multiple error detection and correction based on redundant residue number systems. IEEE Transactions on Communications, vol. 56, no 3, 2008, pp. 325-330.

[7] Anantvalee T., Wu J. A survey on intrusion detection in mobile ad hoc networks. In Wireless Network Security. Springer, Boston, MA, 2007, pp. 159-180.

[8] Ahmed T., Rahman R. Survey of anomaly detection algorithms: Towards self-learning networks. In Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, CRC Press, 2010. pp. 65-89.

[9] Zhou L., Haas Z.J. Securing ad hoc networks. IEEE network, vol. 13, №. 6, 1999, pp. 24-30.

[10] Perkins C., Belding-Royer E., Das S. RFC 3561: Ad hoc on-demand distance vector (AODV) routing, 2003. Available at: http://www.ietf.org/rfc/rfc3561.txt, accessed 07.12.2018.

[11] Johnson D.B., Maltz D.A., Broch J. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, vol. 5, 2001, pp. 139-172.

[12] Glass S., Portmann V., Muthukkumarasamy V. Securing Route and Path Integrity In Multihop Wireless Networks. Security of Self-Organizing Networks. MANET, WSN, WMN, VANET, CRC Press, 2010, pp. 25-43.
[13] Yih-Chun H., Perrig A. A survey of secure wireless ad hoc routing. IEEE Security & Privacy, vol. 2. no. 3, 2004, pp. 28-39.
[14] Zapata M.G., Asokan N. Securing ad hoc routing protocols. In Proc. of the 1st ACM workshop on Wireless security, 2002, pp. 1-10.
[15] Hu Y.C., Johnson D. B., Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc networks, vol. 1, no. 1, 2003, pp. 175-192.
[16] Raja R., Ganeshkumar P. QoSTRP: A Trusted Clustering Based Routing Protocol for Mobile Ad-Hoc Networks. Programming and Computer Software, vol. 44, no. 6, 2018, pp. 407–416.
[17] Hu Y. C., Perrig A., Johnson D. B. ARIADNE: A secure on-demand routing protocol for ad hoc networks. Wireless networks, vol. 11, no. 1-2, 2005, pp. 21-38.
[18] Zhu S., Xu S., Setia S., Jajodia S. LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks. In Proc. of the 23rd International Conference on Distributed Computing Systems Workshops, 2003. pp. 749-755.
[19] Liu X., Han J., Ni G., Zhang C., Liu Y. A Multipath Redundant Transmission Algorithm for MANET. In Proc. of the International Conference in Communications, Signal Processing, and Systems, 2017, pp. 518-524.
[20] Yuan Y. H., Chen H. M., Jia M. An optimized ad-hoc on-demand multipath distance vector (AOMDV) routing protocol. In Proc. of the 2005 Asia-Pacific Conference on Communications, 2005. pp. 569-573.
[21] Leung R., Liu J., Poon E., Chan A. L., Li B. MP-DSR: a QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks. In Proc. of the 26th Annual IEEE Conference on Local Computer Networks, 2001. pp. 132-141.
[22] Liang Y., Poor H. V., Ying L. Secrecy throughput of MANETs with malicious nodes. In Proc. of the IEEE International Symposium on Information Theory, 2009. pp. 1189-1193.
[23] Mammeri A., Boukerche A., Fang Z. Video streaming over vehicular ad hoc networks using erasure coding. IEEE Systems Journal, vol. 10, no. 2, 2016, pp. 785-796.
[24] Yang B., Chen Y., Chen G., Jiang X. Throughput Capacity Study for MANETs with Erasure Coding and Packet Replication. IEICE Transactions on Communications, vol. 98, no. 8, 2015, pp. 1537-1552.
[25] Djukic P., Valaee S. Reliable packet transmissions in multipath routed wireless networks. IEEE Transactions on Mobile Computing, vol. 5, no. 5, 2006, pp. 548-559.
[26] Lee S.J., Gerla M. Split multipath routing with maximally disjoint paths in ad hoc networks. In Proc. of the IEEE International Conference on Communications, vol. 1, 2001, pp. 3201-3205.
[27] Ye Z., Krishnamurthy S. V., Tripathi S. K. A framework for reliable routing in mobile ad hoc networks. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, vol. 1, 2003, pp. 270-280.
[28] Mahfoudh S., Minet P. An energy efficient routing based on OLSR in wireless ad hoc and sensor networks. In Proc. of the 22nd International Conference on Advanced Information Networking and Applications-Workshops, 2008. pp. 1253-1259.
[29] Tchernykh A., Babenko M., Miranda-López V., Drozdov A. Y., Avetisyan, A. WA-RRNS: Reliable Data Storage System Based on Multi-cloud. In Proc. of the 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2018. pp. 666-673.
[30] Tchernykh A., Schwiegelsohn U., Talbi E. G., Babenko M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science, 2016. DOI: 10.1016/j.jocs.2016.11.011
[31] Chervyakov N., Babenko M., Tchernykh A., Kucherov N., Miranda-López V., Cortés-Mendoza J. M. AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security. Future Generation Computer Systems, vol. 92, 2019, pp. 1080-1092.
[32] Tormasov A.G., Khasin M.A., Pakhomov Y.I. Ensuring Fault-Tolerance in Distributed Media. Programming and Computer Software, vol. 27, no. 5, 2001, pp. 245–251.
[33] Sarkar S. Kisku B., Misra S., Obaidat M.S. Chinese Remainder Theorem-based RSA-threshold cryptography in MANET using verifiable secret sharing scheme. In Proc. of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2009. pp. 258-262.

[34] Chang C.H., Molahosseini A.S., Zarandi A.A. E., Tay T.F. Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications. IEEE circuits and systems magazine, vol. 15, no. 4, 2015, pp. 26-44.
[35] Ding C., Pei D., Salomaa A. Chinese remainder theorem: applications in computing, coding, cryptography. World Scientific, 1996, 224 p.
[36] Zima E. V., Stewart A.M. Cunningham numbers in modular arithmetic. Programming and Computer Software, vol. 33, no. 2, 2007, pp. 80–86.
[37] Chervyakov N. I., Molahosseini A. S., Lyakhov P. A., Babenko M. G., Deryabin M. A. Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem. International Journal of Computer Mathematics, vol. 94, no. 9, 2017, pp. 1833-1849.
[38] Asmuth C., Bloom J. A modular approach to key safeguarding. IEEE transactions on information theory, vol. 29, no. 2, 1983, pp. 208-210.
[39] Quisquater M., Preneel B., Vandewalle J. On the security of the threshold scheme based on the Chinese remainder theorem. In Proc. of the International Workshop on Public Key Cryptography, 2002. pp. 199-210.
[40] Rabin M. O. Efficient dispersal of information for security, load balancing, and fault tolerance. Journal of the ACM, vol. 36, no. 2, 1989, pp. 335-348.
[41] Tchernykh A., Babenko M., Chervyakov N., Miranda-López V., Kuchukov V., Cortés-Mendoza J. M., Deryabin M., Kucherov N., Radchenko G., Avetisyan A. AC-RRNS: Anti-collusion secured data sharing scheme for cloud storage. International Journal of Approximate Reasoning, vol. 102, 2018, pp. 60-73.
[42] Barzu M., Ţiplea F. L., Drăgan C. C. Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes. Information Sciences, vol. 240, 2013, pp. 161-172.
[43] Morillo P., Padró C., Sáez G., Villar J. L. Weighted threshold secret sharing schemes. Information Processing Letters, vol. 70, no. 5, 1999, pp. 211-216.

Информация об авторах / Information about authors

Николай Иванович ЧЕРВЯКОВ – доктор технических наук, профессор, заведующий кафедрой прикладной математики и информатики Северо-Кавказского федерального университета с 2004 года. Сфера научных интересов: алгебраические структуры в полях Галуа, модулярная арифметика, нейрокомпьютерные технологии, цифровая обработка сигналов, криптографические методы защиты информации.

Nikolay Ivanovitch CHERVYAKOV – Doctor of Technical Sciences, Professor, Head of the Department of Applied Mathematics and Computer Science of the North Caucasus Federal University since 2004. Research interests: algebraic structures in the Galois fields, modular arithmetic, neurocomputer technologies, digital signal processing, cryptographic methods for protecting information.

Максим Анатольевич ДЕРЯБИН является доцентом Северо-Кавказского федерального университета. В 2016 г. защитил кандидатскую диссертацию. В число научных интересов входят модулярная арифметика, система остаточных классов, компьютерная математика, математическое моделирование, теория чисел, разработка системного и прикладного программного обеспечения, проектирование высокоэффективных аппаратных средств, разработка для FPGA.

Maxim Anatolyevitch DERYABIN is an associate professor at the North Caucasus Federal University. In 2016 he defended his PhD thesis. His research interests include modular arithmetic, residual class system, computer mathematics, mathematical modeling, number theory, development of system and application software, design of high-performance hardware, development for FPGA.

Антон Сергеевич НАЗАРОВ получил степень магистра по параллельным технологиям в Северо-Кавказском федеральном университете в 2015 году. Он является аспирантом в Северо-Кавказском федеральном университете с 2015 года и работает инженером-

исследователем. Его исследовательские интересы включают модульную арифметику, системы счисления, FPGA, высокопроизводительные вычисления и отказоустойчивые вычисления.

Anton Sergeevitch NAZAROV received the Master's degree in parallel technologies from North Caucasus Federal University in 2015. He has been a Postgraduate Student at NCFU since 2015. He is working as a Research Engineer at NCFU. His research interests include modular arithmetic, residue number systems, FPGA, high performance computing, and fault-tolerant computing.

Михаил Григорьевич БАБЕНКО окончил Ставропольский государственный университет в 2007 году. Защитил кандидатскую диссертацию в 2011 г. Преподаватель кафедры прикладной математики и математического моделирования Северо-Кавказского федерального университета. Сфера научных интересов: алгебраические структуры в полях Галуа, модулярная арифметика, нейрокомпьютерные технологии, цифровая обработка сигналов, криптографические методы защиты информации.

Mikhail Grigorievitch BABENKO graduated from Stavropol State University in 2007. He defended his thesis in 2011. Currently he is a lecturer of the Department of Applied Mathematics and Mathematical Modeling of the North Caucasus Federal University. Research interests: Algebraic structures in the Galois fields, modular arithmetic, neurocomputer technologies, digital signal processing, cryptographic methods for protecting information.

Николай Николаевич КУЧЕРОВ получил степень доктора философии в Северо-Кавказском федеральном университете в 2018 году. Он также является младшим научным сотрудником в Северо-Кавказском федеральном университете с 2014 года. Сфера его научных интересов: облачные вычисления, модульная арифметика, системы счисления остатков, FPGA, пороговая криптография, высокая производительность вычислений.

Nikolay Nikolaevitch KUCHEROV received a degree of PhD at North Caucasus Federal University in 2018. He is also a junior researcher at North Caucasus Federal University since 2014. His research interests include cloud computing, modular arithmetic, residue number systems, FPGA, threshold cryptography, high performance computing.

Андрей Владимирович ГЛАДКОВ является старшим преподавателем Северо-Кавказского федерального университета. В 2006 окончил физико-математический факультет Ставропольского государственного университета. Научные интересы: нейронные сети; система остаточных классов; криптография; численные методы.

Andrei Vladimirovich GLADKOV is a senior teacher at the North Caucasus Federal University. In 2006 he graduated from the Physics and Mathematics Faculty of Stavropol State University. Research interests: neural networks; residual class system; cryptography; numerical methods.

Глеб Игоревич РАДЧЕНКО – кандидат физико-математических наук, доцент. Он является директором высшей школы электроники и компьютерных наук и заведующим кафедрой «Электронные вычислительные машины» Южно-Уральского государственного университета. Научные интересы: распределенные вычислительные системы, облачные вычисления, научные потоки работ, проблемно-ориентированные вычислительные среды.

Gleb Igorievitch RADCHENKO – Candidate of Physical and Mathematical Sciences, Associate Professor. He is the director of the High School of Electronics and Computer Science and the head of the Electronic Computers Department at South Ural State University. Research interests: distributed computing systems, cloud computing, scientific workflows, problem-oriented computing environments.

DOI: 10.15514/ISPRAS-2019-31(2)-12

Выявление характерных особенностей программ для борьбы с компьютерным пиратством на основе интеллектуального анализа графов

[1] *С. Сарвар, ORCID: 0000-0001-9714-6580 <sohail.sarwar@seecs.edu.pk>*
[1] *З.Уль Кайум, ORCID: 0000-0003-4230-6895 <zia@aiou.edu.pk>*
[2]*М. Сафьян, ORCID: 0000-0003-4501-9699 <msafyan@gcul.edu.pk>*
[3,4]*М. Икбал, ORCID: 0000-0002-8438-6726 <miqbal@lsbu.uk>*
[2]*Я. Махмуд, ORCID: 0000-0002-9676-2100 <yasir@iqra.edu.pk>*
[1] *Университет Гуджарата, Пакистан*
[2] *Правительственный университет колледжа, Лахор, Пакистан*
[3] *Лондонский университет Саут Бэнк, Великобритания*
[4] *Университет Эссекса, Великобритания*

Аннотация. Расширение числа и ассортимента компонентов программного обеспечения в значительной степени подчеркивает необходимость защиты прав интеллектуальной собственности (IPR), затрудняемую компьютерным пиратством, для борьбы с которым требуются эффективные меры. Выявление характерных особенностей программного обеспечения предназначено для противодействия незаконному заимствованию права собственности на программное обеспечение путем установления его происхождения. В этой статье предлагается новый подход к выявлению характерных особенностей программ, основанный на сочетании методов интеллектуального анализа текстов и графов. Элементы кода программы и их связи с другими элементами идентифицируются на основе их особенностей (конструкций кода) и преобразуются в конструкции языка манипулирования графами. Характерные особенности программного обеспечения, выводимые путем исследования теоретических свойств графа (на основе коэффициента кластеризации), используются для установления сходства или различия двух программ. Предложенная методика была оценена по показателям достоверности, устойчивости, заимствования методов, обнаружения модифицированного кода и самокопирования. Результаты подтверждают эффективность предложенного подхода для противодействия незаконному заимствованию права собственности. Сравнительный анализ предложенного подхода с современными решениями показывает лучшие результаты при выявлении свойств и связей узлов программы и при использовании динамических методов анализа графов без дополнительных накладных расходов (таких как увеличение размера программы и затрат на обработку).

Ключевые слова: право интеллектуальной собственности; незаконное использование программного обеспечения; характерные особенности программного обеспечения; интеллектуальный анализ графов; достоверность и устойчивость.

Для цитирования: Сарвар С., Ул Кайум З., Сафьян М., Икбал М. , Махмуд Я. Выявление характерных особенностей программ для борьбы с компьютерным пиратством на основе интеллектуального анализа графов. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 171-186. DOI: 10.15514/ISPRAS-2019-31(2)-12

Graphs Resemblance based Software Birthmarks through Data Mining for Piracy Control

[1] *S. Sarwar, ORCID: 0000-0001-9714-6580 <sohail.sarwar@seecs.edu.pk>*
[1] *Z.Ul Qayyum, ORCID: 0000-0003-4230-6895 <zia@aiou.edu.pk>*
[2]*M. Safyan, ORCID: 0000-0003-4501-9699 <msafyan@gcul.edu.pk>*
[3,4]*M. Iqbal, ORCID: 0000-0002-8438-6726 <miqbal@lsbu.uk>*
[2]*Y. Mahmood, ORCID: 0000-0002-9676-2100 <yasir@iqra.edu.pk>*
[1] *Department of Computer Science, University of Gujrat, Pakistan*
[2] *Department of Computing, GC University Lahore, Pakistan*
[3] *School of Engineering, London South Bank University, England*
[4] *School of Computer Science and Electronic Engineering University of Essex, England*

Abstract. The emergence of software artifacts greatly emphasizes the need for protecting intellectual property rights (IPR) hampered by software piracy requiring effective measures for software piracy control. Software birthmarking targets to counter ownership theft of software by identifying similarity of their origins. A novice birthmarking approach has been proposed in this paper that is based on hybrid of text-mining and graph-mining techniques. The code elements of a program and their relations with other elements have been identified through their properties (i.e code constructs) and transformed into Graph Manipulation Language (GML). The software birthmarks generated by exploiting the graph theoretic properties (through clustering coefficient) are used for the classifications of similarity or dissimilarity of two programs. The proposed technique has been evaluated over metrics of credibility, resilience, method theft, modified code detection and self-copy detection for programs asserting the effectiveness of proposed approach against software ownership theft. The comparative analysis of proposed approach with contemporary ones shows better results for having properties and relations of program nodes and for employing dynamic techniques of graph mining without adding any overhead (such as increased program size and processing cost).

Keywords: Intellectual Property Rights (IPR); Software Ownership Theft; Software Birthmarking; Graph Mining; Credibility and Resilience.

For citation: Sarwar S., Ul Qayyum Z., Safyan M., Iqbal M., Mahmood Y. Graphs Resemblance based Software Birthmarks through Data Mining for Piracy Control. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 171-186 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-12

1. Введение

Достижения программной инженерии изменили ход технического прогресса на основе ряда инновационных идей. Реализация этих идей повлекла за собой смену парадигмы с переходом к мобильным приложениям, интеллектуальным технологиям («умные» дома, офисы, города и т.д.), новым вычислительным парадигмам (грид и облачные вычисления), обучению на основе продвинутых технологий (Technology Enhanced Learning, TeL), Интернет вещей (IoT) и т.д. Эти инновационные разработки программного обеспечения, основанные на новизне идей (то есть на интеллектуальной собственности), сталкиваются с потенциальными угрозами. Эти угрозы правам интеллектуальной собственности (intellectual property right, IPR) включают компьютерное пиратство, незаконное заимствование прав собственности, реверс-инжиниринг, копирование программного обеспечения (или его частей) и т.д.

В одном из опубликованных исследований утверждается, что более 50% потребителей технологий работают с применением пиратского программного обеспечения [1]. Основной причиной этого широко распространенного нарушения законов о пиратстве является присущая программным продуктам природа, позволяющая легко их воспроизводить и распространять, что отличает программные продукты от продуктов других отраслей. Программные продукты приобретаются клиентами с получением прав только на использование только на их использования без права на какие-либо изменение или. Однако

эти этические обязательства нарушаются в результате незаконного распространения программного обеспечения, что влечет огромные убытки для поставщиков.

Поставщики программного обеспечения защищают авторские права на свои продукты, отслеживая передовые подходы [6], которые гарантируют пользователям, имеющим разрешение, полноценное использование программного обеспечения и его настройку при необходимости. Почти все аспекты программного обеспечения скрываются, чтобы предотвратить его несанкционированную продажу. Так что конечной целью продавца продукта программного обеспечения является защита компьютерного пиратства [7].

Для борьбы с компьютерным пиратством разработан ряд методов [2] [3] [4] [5]. Эти методы направлены на противодействие растущему объему пиратского программного обеспечения, реверс-инжинирингу, взлому программного обеспечения и его незаконному использованию. В частности, используются следующие методы.

- Цифровые водяные знаки (Watermarking): используются для подтверждения владения программным обеспечением.
- Проверка подлинности (Tamper-proofing): программа уничтожается при незаконном использовании.
- Обфускация (Obfuscation): скрывает структуру программного обеспечения для противодействия обратной инженерии.
- Шифрование (Encryption): защищает программное обеспечение путем кодирования с использованием открытых или закрытых ключей.
- Выявление характерных особенностей (Birthmarking): незаконное использования программного обеспечения обнаруживается на основе его уникальных свойств.

Все перечисленные методы, кроме последнего, могут добавлять в коде различные операторы принятия решения (decision statement); следовательно, размер кода увеличивается, что влечет за собой снижение производительности и, следовательно, возможности многократного применения. Кроме того, при применении методы выявления характерных особенностей программ идентифицируются уникальные характеристики программы (называемые внутренними свойствами), такие как элементы переменных, циклов, ветвлений, присваиваний и т.д. [8]. Нетривиальной задачей является изменение этих программных конструкций, и еще труднее обосновать эти изменения [7], [9] при выявлении факта незаконного использования программного обеспечения (или прав собственности).

Учитывая вышесказанное, мы предлагаем новый метод выявления характерных особенностей программного обеспечения с использованием интеллектуального анализа графов. Для выявления характерных черт каждого метода и класса используются теория графов [8] и сетевые методы [9]. Предлагаемый метод по своей природе является статическим, основанным на синтаксической структуре программы. Эта структура используется для вычисления значения свойств каждого элемента программы и связей между этими элементами. Впоследствии значения свойств преобразуются в графы. Теоретические свойства этих графов (на основе коэффициента кластеризации) позволяют сравнивать характерные особенности (в виде графов) двух программ. В результате две программы классифицируются как схожие или несхожие (выявляется, была ли скопирована программа, или был заимствован один класс или метод(ы) класса украден).

Кроме того, предлагаемый метод статического определения характерных особенностей программ основе графов может определить, была ли изменена программа. Метод выявляет характерные особенности программного обеспечения на основе связей внутренних *характеристик* каждого метода в программе. Эти *связанные характеристики* играют ключевую роль в выполнении функциональных требований к каждому методу. Все характерные особенности уровня методов классов программ используются для построения характерных особенностей программы. Эти статистические построения обеспечивают меру

сходства или различий между различными программами. Аспекты предлагаемой методики были оценены по показателям достоверности и устойчивости на разных уровнях детализации при отслеживании требуемых накладных расходов.

Оставшаяся часть статьи организована следующим образом. В разд. 2 рассматриваются основные понятия выявления характерных особенностей программ и приводится краткий обзор распространенных методов. В разд. 3 подробно описывается техника определения характерных особенностей программ, представленная в этой работе. В разд. 4 обсуждается оценка предлагаемого подхода. Разд. 5 завершает представленную работу с указанием направлений будущих исследований.

2. Обзор литературы

В этом разделе представлен обзор существующих методов борьбы с компьютерным пиратством в целом; особое внимание уделяется методам выявления характерных особенностей программ.

Пиратство программного обеспечения стало глобальной проблемой, о чем свидетельствует коммерческая оценка в 62,7 млрд. долл. США объема используемого нелицензионного программного обеспечения в 2013 году [1]. Аналогичные исследования указывают на рост пиратства на 42-43% только в 2014 году [2]. Пиратство можно разделить на две основные области: нелегальное распространение программного обеспечения и реверс-инжиниринг. Хотя для минимизации компьютерного пиратства было выполнено множество разработок: обфускация (obfuscation), проверка подлинности (tamper-proofing), цифровые водяных знаки (watermarking), хеширование и контроль потока управления, но их эффективность можно значительно улучшить. Обфускация трансформирует программу, делая ее менее понятной при сохранении семантики [11] [12]. Проверка подлинности [7] основана на расширении кода специальными средствами [13], что чревато дополнительными накладными расходами. Таким образом, эти методы снижают производительность программного обеспечения, требуя специальной среды выполнения, такой как виртуальная Java-машина [14].

Цифровые водяные знаки программного обеспечения – это метод защиты интеллектуальной собственности приложения. Смысл этого метода тот же самый, что и у обычных цифровых водяных знаков, когда в текстовых, графических, аудио- или видеоданных размещается уникальный идентификатор таким образом, что он не может быть обнаружен людьми [19-23].

Некоторые исследователи использовали методы инженерии знаний для классификации плагиата [24]. Внутренний плагиат, внешний плагиат и авторство могут быть обнаружены [25] с помощью интеллектуального анализа текста. В [26] обсуждается практическая и эффективная методика обнаружения пиратского программного обеспечения с использованием метафорического анализа. Для обнаружения незаконного использования программного обеспечения использовались атрибуты минимизации.

В некоторых работах для противодействия компьютерному пиратству предлагалось использовать гибрид методов выявления характерных особенностей и водяных знаков [22] [24] [25], поскольку характерные особенности идентифицирует только внутренние свойства программы. Сочетание обнаружения характерных особенностей и водяных знаков может быть эффективной мерой по борьбе с пиратством без ущерба для производительности программного обеспечения [15].

Помимо обнаружения незаконного использования копий программ, выявление характерных особенностей программного обеспечения использовалось для обнаружения вредоносных программ [27, 28].

В [29] предлагался метод выявления характерных особенностей электронных схем для предсказания возможности их повторного использования.

Вопросы распространенных методов классификации вредоносных программ в приложениях на основе Android обсуждались в [35]. Система FalDroid, основанная на анализе, показала достаточно высокую точность.

В следующих подразделах приводятся классификация методов обнаружения характерных особенностей программного обеспечения и обзор результатов соответствующих исследований.

2.1 Характерные особенности программного обеспечения

Характерными особенностями программного обеспечения называется уникальный набор характеристик компьютерной программы или ее компонента. Каждое характерная особенность программы обладает двумя свойствами: надежностью и устойчивостью к трансформации [7], [15], [16], [9]. Характерные особенности программы могут быть статическими или динамическими.

2.2 Статические характерные особенности

В отношении к понятию статических характерных особенностей программ мы полагаемся на основополагающую работу [8].

Пусть *a* и *b* – это фрагменты кода двух разных программ и *z* – программный компонент, извлекающий уникальный набор особенностей из некоторого метода (методов). У *a* существует набор характерных особенностей *в том и только в том случае, когда*:

1) *z(a)* извлекается из фрагмента *a* (при отсутствии данных о других компонентах программы и
2) если b является копией a, то *z(a)=z(b).*

2.3 Динамические характерные особенности

Другим вариантом являются динамические характерные особенности. Это понятие было введено в фундаментальной работе [15].

Пусть *a* и *b* – это фрагменты кода двух разных программ, вводящие с консоли входные данные *c*. *z* – программный компонент, извлекающий уникальный набор свойств программ *a* и *b*. Тогда можно утверждать, что *z(a,c)* является набором характерных особенностей *a в том и только в том случае, когда*:

1) *z(a,c)* получается из a только после выполнения фрагмента *a* после ввода с консоли данных *c* и
2) если *b* является копией *a*, то *z(a,c)=z(b,c)*.

Некоторые другие вариации характерных особенностей программ можно обнаружить в [8, 9, 15, 16], где для Java-программ устанавливаются четыре значимых типа особенностей:

1) наличие констант в полях классов (CVFV),
2) последовательность вызовов методов (SMC),
3) структура наследования (IS)
4) используемые классы (UC).

Эти характерные особенности не обладают необходимой устойчивостью и тривиальны по своей природе, поэтому легко подвержены трансформации [15]. Подход к выявлению характерных особенностей, основанный на анализе полных путей в программе (whole program path, WPP) и предложенный в [16], может страдать от таких уязвимостей, как преобразования цикла, или атак с подстановкой кода [17].

Другой динамический подход к выявлению характерных особенностей, более устойчивый, чем WPP, основан на последовательности вызовов интерфейса прикладного

программирования (API) [9]. Однако окно коротких вызовов методов может справиться только с ограниченным набором вызовов API.

Методы динамического выявления характерных особенностей для многопоточных приложений с использованием системных вызовов, связанных с потоками, были предложены в [17] [18]. Выявление характерных особенностей для обнаружения плагиата в многопоточных программах является сложной задачей. В [36] был предложен методик динамического выявления характерных особенностей TOB-PD, который демонстрирует надежную работу.

Принимая во внимание недостатки существующих работ и исследований, была мы предлагаем новый и эффективный метод выявления характерных особенностей программного обеспечения. Предлагаемый подход, описываемый в разд. 3, представляет собой гибрид методов анализа текста и графов. Методы интеллектуального анализа графов, такие как кластеризация и поиск клик [30, 31], используются еще и для идентификации модифицированного кода. Применение графов [32], позволяет учитывать связи между элементами метода, а также классов программ (или программ) для определения происхождения соответствующих компонентов.

3. Предлагаемый метод

Предлагаемый метод работает с внутренними особенностями программного кода, идентифицируя элементы в методе(ах), свойства элементов и их связи с другими элементами в других программах. Элементы программы (внутри класса или метода) представляют свойства и связи между элементами. Этими элементами являются переменные методов, повторяемость/циклы, присваивания и операторы принятия решений. Связь элементов с их свойствами трансформируется в граф. Узлы в графе представляют элементы метода, а ребра представляют – связи между элементами (как показано на рис. 4 и 5). Это подразумевает, что в фрагментах кода элементы метода всех должны иметь как минимум одно соединение (или связь) с другими элементами [8]. Другими словами, для графа *G*, с узлами *N* и ребрами *E* должно выполняться следующее условие.

$\boldsymbol{G = \{N, E\}, N = \{n_1, n_2, \dots, n_k\}, E = \{e_1, e_2, \dots, e_m\}}$

Для каждой пары узлов $\boldsymbol{n_i}$ и $\boldsymbol{n_j}$ $(\boldsymbol{i \neq j})$ существует ребро $\boldsymbol{e_l}$. соединяющее $\boldsymbol{n_i}$ и $\boldsymbol{n_j}$.

Чтобы сделать набор характерных особенностей более надежным, мы выбираем фрагмент кода (или метода) включающий многочисленные элементы и свойства (вместо взаимно-однозначного отображения между узлами и ребрами). Это приводит к сложному преобразованию внутренних характеристик методов, называемых характерными особенностями программ. Такие характеристики (или характерные особенности) позволяют установить, является ли фрагмент кода копией или оригиналом.

Примеры связей между элементами показаны в табл. 1.

Табл. 1. Внутренние характеристики: свойства и связи 1.
Table 1. Intrinsic Characteristics: Properties and Relations in Elements

Название элемента	Свойства				
	Глобальная переменная	Локальная переменная	Цикл	Условие	Данные
Глобальная переменная		присваивание	использование	использование	присваивание
Локальная переменная	присваивание	присваивание	использование	использование	присваивание
Цикл	использование	использование	одинаковые уровни	использование	использование
Условие	выход	использование	использование	одинаковые уровни	использование
Данные	присваивание	присваивание	использование	использование	присваивание

Имеются разные типы связей (включение или обобщение) между циклами и связи по одноуровневости (sibling relation) с другими циклами. Подобные типы связей могут наблюдаться между глобальными и локальными переменными. Эти комбинации связей и свойств элементов методов важны для классификации характерных особенностей.

Процесс сборки и формирования набора характерных особенностей проиллюстрирован на рис. 1. Первым этапом является *очистка и маркировка* кода. Программный код сканируется и очищается от примесей, таких как неиспользуемые экземпляры или комментарии. Затем выявляются свойства методов программы, элементы методов и связи. Эти элементы и их свойства собираются для получения графового представления характерных особенностей уровня методов. Извлеченный набор характерных особенностей помогает различить две программы (реализованные в изолированных средах) на основе свойств и элементов методов.

Как правило, характерные особенности программ используются для обнаружения исходного кода, когда у двух программ имеется одинаковое происхождение. Однако на основе использования графовых связей можно обнаружить и то, какая программа из сравниваемых программ является исходной: ее граф содержит более строгие и реалистичные связи.

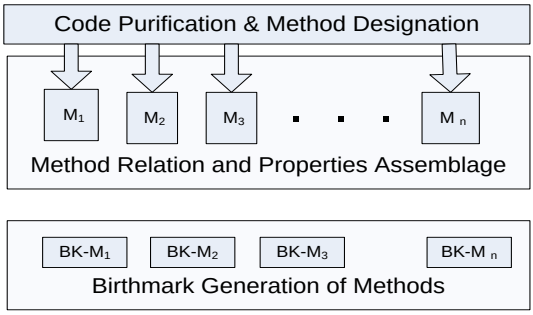


Рис. 1. Процесс формирования набора характерных особенностей
Fig 1. Process for Birthmark Generation

Характерные черты двух программ считаются схожими, если их свойства и связи совпадают при соблюдения условий достоверности. Условие достоверности гласит, что все коды, разработанные в изолированных средах, не должны иметь сходства. Кроме того, если содержание копируемой программы изменяется, такое преобразование также должно раскрываться по набору характерных особенностей (это называется устойчивостью набора характерных особенностей) [7, 8, 9, 10, 11]. Предлагаемый метод обеспечивает обе требуемые черты характерных особенностей, которые обсуждались в подразделе 2.1.

```
Int a;
for(int i=0;i<5; i++)
{
   if(i<3)
        a=1;
   else
        a=3;
}
```

```
char b;
for(int i=0;i<10; i++)
{
   if(i='Z')
        b='A';
   else
        b='Z';
}
```

Рис. 2. Характерные особенности двух разных программ
Fig 2. Code Sample with Birthmark Comparison of two Different Programs

Как показано в [7-9], при традиционном построении наборов характерных особенностей приведенные фрагменты программ будут неразличимы. Следовательно, традиционные

методы устойчивость не обеспечивают. Логика этих двух примеров программ различна, и правильный метод построении наборов характерных особенностей может это распознать. Предлагаемый нами метод способен правильно идентифицировать эти программы как отличающиеся одна от другой. Эта обеспечивается за счет выявления отдельных элементов и их свойств, как показано в табл. 1.

3.1 Извлечение набора характерных особенностей

Процесс извлечения характерных особенностей из кода метода состоит с следующем.

- Читается код метода(ов) и определяются элементы в методе(ах).
- Определяются свойства в элементах метода(ов).
- Определяются связи элементов и вычисляются веса ребер.
- На основе весов ребер связи преобразуются в графы.
- На основе связей и свойств формируется набор характерных особенностей.

Генерируемый набор характерных особенностей состоит из различных программных конструкций: элементов метода, свойств элементов и связей между идентифицированными элементами. Сгенерированный набор характерных особенностей используется для выявления степени сходства или несходства рассматриваемых методов.

```
void PrintStack () {
        int i;
        if (count == -1) return;
        else
        {
                for (i=0 i<count; i++)
                {
                        Print (Stack[i]);
                }
        }
}
```

Рис. 3. Фрагмент кода гипотетической программы
Fig 3. Code Sample from Hypothetical Software Program

Поясним суть предлагаемого метода на примере фрагмента кода гипотетической программы *A*, приведенного на рис. 3. Метод *PrintStack ()* в этом фрагменте выводит содержимое стека на консоль (если стек не пуст). В этом фрагменте кода используются две глобальные переменные (*count* и *stack*), локальная переменная метода (*i*), два оператора принятия решения (*if*/*else*) и один цикл. В этом фрагменте элементы кода *i*, *if* и *else* имеют связи по одноуровневости. В то же время между элементом *else* и элементом *for* имеется связь по подчиненности (*parent-child*). Графовое представление элементов и связей показано на рис. 4.

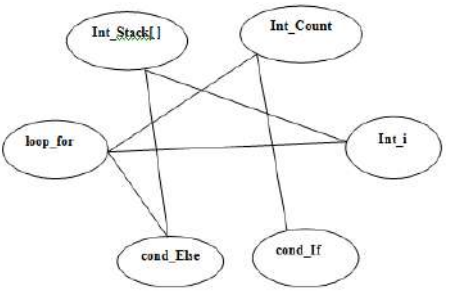


Рис. 4. Граф элементов и связей для фрагмента с рис. 3
Fig 4. Sample pre-birthmark computation graph

После того как для обеих программ (исходной программы и предполагаемой копии) сформированы наборы характерных особенностей (в форме графов), должна быть рассчитана степень сходства этих наборов характерных особенностей (каждый из которых представляет соответствующую программу).

3.2 Выявление сходства

Процесс выявления сходства наборов характерных особенностей (графов) двух программ состоит в следующем.

- Одна из программ полагается оригинальной, а другая – предполагаемой копией.
- В обоих графах выявляются *схожие* элементы.
- Сравниваются коэффициенты кластеризации и значения свойства схожих элементов.
- Вычисляется степень сходства между элементами фрагментов кода.

Процесс выявления сходства может привести к одному из следующих четырех результатов.

a. *Полное сходство*: когда все элементы сформированных характерных черт метода(ов) схожи по свойствам и связям; это означает, что рассматриваемые методы в коде являются «полными копиями» исходных методов, как показано на рис. 4.
b. *Модифицированное сходство*: если копируются все свойства исходной программы, получается модифицированная копия. Методы дублируются для незаконной настройки и маскировки программы.
c. *Предполагаемое сходство*: если некоторые связи и свойства оказываются схожими, копия считается измененной. Этот случай сложно обнаружить, так как можно, а можно и не доказать, что вторая программа является копией.
d. *Отсутствие сходства*: если нет сходства в свойствах и связях наборов характерных свойств, можно утверждать, что программы имеют различное происхождение.

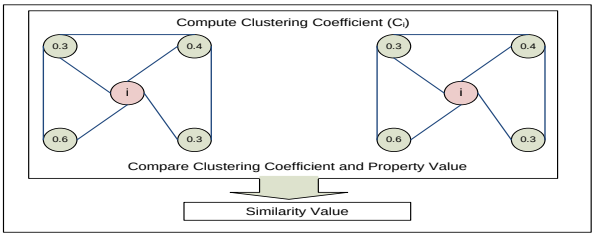


Рис. 5. Полное сходство двух графов
Fig 5. Similarity Comparison of two graph nodes

Первый и последний случаи довольно просты и могут быть достаточно легко проверены, в отличие от второго и третьего случаев, когда имеются частичная модификация или трансформация. С учетом этих сценариев определяются четыре уровня сходства элементов. Уровень 0 подразумевает отсутствие сходства между элементами, уровень 1 представляет предполагаемое сходство, уровень 2 означает, что, возможно, код был модифицирован, а уровень 3 означает полное сходство.

Предполагаемое сходство и сходство с модификацией выявляются с использованием установленного порога. Если ε представляет собой заданный порог, то степень сходства может быть рассчитана по формуле *eq(i).*

$$P(p_i) \,||\, P(q_i) \; > \varepsilon > P(q_i) \;||\, P(p_i) \qquad eq(i)$$

Уровни сходства 2 и 3 можно различить, измеряя расстояние между свойствами элемента. Расстояние между свойствами элементов *pi* и элементов *qi* вычисляется по формуле *eq(ii).*

$$\sum_{j=1}^{m} P(p_i) \,||P(q_i) \qquad eq(ii)$$

Если между расстоянием между элементами $(p_i,\ q_i)$ и $(q_i,\ p_i)$ появляется определенный порог, то устанавливается сходство на уровне 2, то есть с сходство с модификацией. Когда для обеих программ вычисляется сходство для каждого элемента всего метода, вычисляется расстояние между свойствами p и q. Рассчитанное расстояние для всех элементов метода позволяет установить сходство на уровне 3, то есть предполагаемое сходство.

4. Анализ и перспективы

Степень сходства различных программ вычислялась на основе взвешенного коэффициента кластеризации разных узлов графа характерных особенностей. Предложенный метод выявления происхождения программ на основе графов оценивается по показателям достоверности, устойчивости, обнаружения измененного кода и самокопирования с целью оценки общей эффективности. Кроме того, был проведен сравнительный анализ с применением нескольких атак, при этом основное внимание уделялось атакам с целью преобразования и модификации кода. Результаты атак трансформации и модификации оценивались с помощью матрицы несоответствий для методов объектов. Каждый из аспектов оценки обсуждается в следующих подразделах.

4.1 Достоверность и устойчивость

Свойство достоверности набора характерных свойств не позволяет идентифицировать сходство независимых программ. Свойство устойчивости позволяет идентифицировать сходство измененных и преобразованных программ. Свойство устойчивости важно, когда программы модифицируются путем атаки на связи, существующие в наборе характерных особенностей. Например, про два независимо разработанных фрагмента кода можно утверждать, что они несходные с нулевым процентом сходства; с другой стороны, фрагменты кода, имеющие 100% сходства, по-видимому являются идеальными копиями. Процент сходства был разделен на 10 равных уровней, уровень 1 показывает сходство от 0% до 10%, уровень 2 – 11-20%, и т.д.; уровень 10 демонстрирует сходство от 90% до 100%.

В табл. 2 приведены результаты выявления сходства выбранных программ с упором на достоверность и устойчивость. Степени сходства рассчитывались для пар независимо разработанных программ и между одной программой и ее полной копией. Результаты показывают, при сравнении программы с ней же самой выявляется наличие совершенной копии, тогда как в других случаях устанавливается полное отсутствие сходства.

Табл. 2. Достоверность и устойчивость при выявлении сходства
Table 2. Similarity Classification for Credibility and Reliability

Пакет Java-программ	Банкомат	Библиотечная система	Торговая точка	Больничная система	Метод k-средних
Банкомат	100	0	0	0	0
Библиотечная система	0	100	0	0	0
Торговая точка	0	0	100	0	0
Больничная система	0	0	0	100	0
Метод k-средних	0	0	0	0	100

Результаты, представленные в табл. 3, в графической форме показаны на рис. 6. На горизонтальной оси показаны программные пакеты банкомата, торговой точки, библиотечной системы и больничной системы. Степень сходства банкоматов с банкоматами

составляет 100%, а банкоматов с остальными программами – 0%. Каждая программа разрабатывалась независимо; поэтому между ними не было обнаружено сходство.

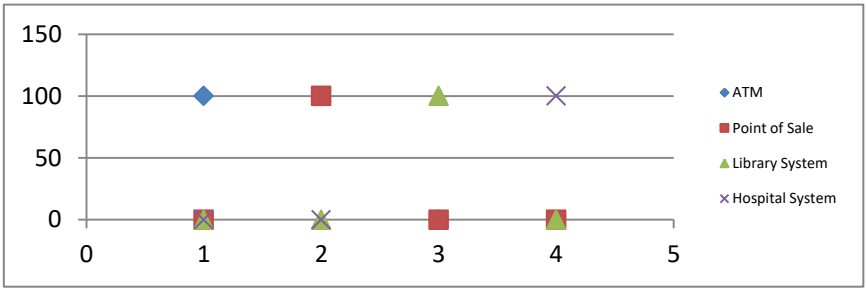


Рис. 6. Результаты достоверности и устойчивости для выбранных систем
Fig 6. Credibility and Reliability results for selected systems.

4.2 Выявление модификаций и трансформаций

Программы модифицируются и трансформируются для того, чтобы скрыть существующие наборы характерных особенностей. Предложенный метод выявляет сходство как преобразованных, так и измененных программы на основе прогнозного анализа. У каждого элемента в наборе характерных особенностей имеется значение свойства, основанное на связях между элементами (узлами), и эти значения используются для выявления сходства в модифицированных и преобразованных кодах. В табл. 3 показана матрица несоответствий для похожих и непохожих объектов. Точность, рассчитанная для похожих и непохожих объектов, составляет 0,90. Коды методов объектов класса были изменены, но не преобразованы.

Табл. 3. Вычисление степени сходства для измененных программ на основе матрицы несоответствия
Table 3. Confusion Matrix Similarity Calculation for Modified Programs

Классыs	**Похожие объекты**	**Непохожие объекты**	**Всего**
Похожие объекты	974	36	1010
Непохожие объекты	164	826	990
Всего	1138	862	2000

4.2 Анализ атак

Характерные особенности извлекаются из методов как связи между элементами программы вместе со свойствами элемента. Чтобы предложенный метод обнаружения заимствований не сработал, код (то есть методы) нужно полностью переписать. В результате время, требуемое для модификации кода, может превысить время, необходимое для разработки новой программы. Преобразование небольших программ кажется тривиальным, но преобразовывать крупные программы затруднительно. Кроме того, изменение одного или нескольких методов может оказаться бесполезным для злоумышленника, поскольку у каждого из этих методов имеются зависимости.

В другом сценарии успешной атаки на предложенный метод код можно изменить, добавив в программу дополнительные блоки (внешние циклы, внешние условия) или преобразовав цикл *for* в цикл *while* и т.д. Такие изменения кода правильно обнаруживаются, но устанавливается предполагаемое, а не полное копирование.

Другим известным недостатком предлагаемого метода является невозможность обнаружения преобразования одной переменной в две переменные. Например, переменную a можно заменить на две новые переменные b и c для сохранения значения переменных и дальнейшей обработки (рис. 7). Такие преобразования трудно идентифицировать. Однако

такие преобразования увеличивают размер кода и, следовательно, время обработки. Кроме того, такие преобразования отнимают много времени, утомительны, и время, требуемое для модификации или преобразования, может превышать фактическое время разработки.

Поскольку предлагаемый подход извлекает характерные особенности уровня метода, можно определить сходство методов даже при очень низкой степени сходства программ целиком. Поэтому поддержка набора характерных особенностей на уровне методов позволяет противодействовать копированию методов и, следовательно, пиратству в более широком спектре.

Пример	**Преобразование**

`int a;`
`a = 10;`
	`int a = 10;`
	`int b = a*a;`
	`int c = b/a;`

Рис. 7. Пример преобразования кода
Fig 7. Example of Code Transformation

4.4 Сравнение с распространенными подходами

Ниже представлены результаты сравнения предложенного подхода с тремя распространенными методами: набор характерных особенностей по полным путям программы (Whole Program Path, WPP) [15], метод на основе K-грамм [16] и динамические наборы характерных особенностей [9]. Для сравнения были выбраны четыре разные и независимые программы из sorceforge.net [34]. Каждая программа сравнивалась сама с собой и с другими тремя программами. Сравнение подходов проиллюстрировано на рис. 8. Как видно из результатов, предложенный метод на основе графа работает лучше, чем другие методы, когда программный код сравнивается с самим собой. Причиной лучшей эффективности нашего подхода является учет связей и свойств каждого узла в графе (наборе характерных особенностей).

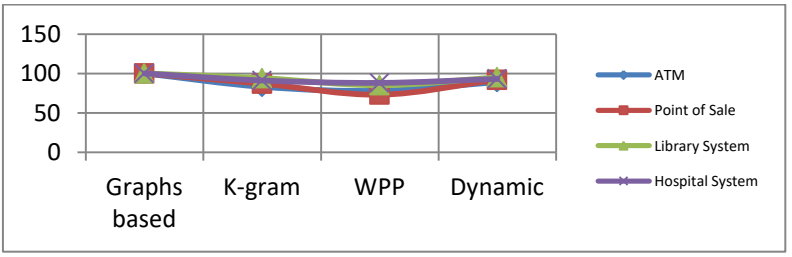


Рис. 8. Сравнение с распространенными методами
Fig 8. Comparison with Prevalent Techniques

Далее в коде программы были скопированы различные методы для проверки возможности выявления сходства методов в рассматриваемой программе. Экспериментальные результаты показаны в табл, 4. При использовании других методов статического формирования наборов характерных особенностей классификация методов была невозможна.

Табл. 4. Обнаружение копирования методов
Table 4. Method Copy Detection Comparison

Пакеты программ	**Метод на основе графов**	**K-граммы**	**WPP**	**Динамический метод**
Банкомат	30	0	0	0
Торговая точка	20	0	0	0

Библиотечная система	10	0	0	0
Больничная система	10	0	0	0

Например, в программном пакете банкомата 30% методов были классифицированы как «скопированные». Другие методы копирование вообще не определяют. Таким образом, можно утверждать, что предложенный метод является эффективной мерой против компьютерного пиратства для обнаружения копирования методов и программ целиком.

Как отмечалось в разд. 3, в методе, основанном на графах, используется структура метода с существующими связями между элементами программы. Сравнительно просто можно выполнить преобразование специального вида, скрывающее копирование кода. Поэтому предлагаемый метод может быть неэффективной мерой защиты от копирования для программ, в которых содержатся методы небольшого размера. При наличии крупных методов специальное преобразование кода является громоздким, и время, необходимое для преобразования каждого элемента метода, может превышать время разработки нового метода.

5. Заключение и направления будущих исследований

Для обнаружения незаконного использования прав собственности на программное обеспечение был предложен новый подход к формированию наборов характерных особенностей программ, основанный на графах. Уникальные характеристики кода (элементов методов) с соответствующими связями преобразуются в графы для выявления сходства или различия программ. Характерные особенности уровня методов дополняют другие методы выявления сходства. Сравниваются два набора характерных особенностей, и элементу набора характерных особенностей присваивается показатель сходства с учетом его глубины. На основе таких вычисления выявляется один из четырех уровней сходства двух программ. Предложенный метод соответствует принципам надежности и устойчивости наборов характерных особенностей программ. С помощью предложенного подхода в коде также могут быть обнаружены измененные элементы. Предложенный подход сравнивался с распространенными методиками; сравнение показывает, что предложенный метод классификации превосходит другие методы, даже если потоки исполнения программы не меняются, но логика кода является преобразованной.

В будущем мы планируем выполнить эксперименты с динамическим решением для обнаружения незаконного использования программного обеспечения с использованием гибридных наборов характерных особенностей программ и водяных знаков.

Список литературы / References

[1]. Ninth Annual BSA Global Software 2013 Piracy Study, Business Software Alliance (BSA), 2013.
[2]. Anckaert B., De Sutter, D. Chanet, and Bosschere K. Steganography for executables and code Transformation Signatures. Lecture Notes in Computer Science, volume 3506, 2005, pp. 425–439.
[3]. Fu B., Richard G., and Chen Y. Some New Approaches for Preventing Software Tampering. In Proc. of the 44th Annual Southeast regional conference, pp. 655–660, 2006.
[4]. Collberg S., Thomborson C. Watermarking, tamper-proofing, and obfuscation-tools for software protection. IEEE Transactions on Software Engineering, vol. 28, issue 8, 2002, pp. 735–746.
[5]. Udupa S. K., Debray K., and Madou M. Deobfuscation: Reverse engineering obfuscated code. In Proc. of the 12th Conference on Reverse Engineering, 2009, pp. 10–19.
[6]. Palsberg J., Krishnaswamy S., Kwon M. Experience with software watermarking. In Proc. of the 16th Computer Security Applications Conference, 2003, pp. 308–316.
[7]. Bai Y., Sun X., Sun G., Deng X., and Zhou X. Dynamic k-gram based software birthmark. In Proc. of the 19th Australian Conference on Software Engineering, 2008, pp. 644–649.

[8]. Mahmood Y., Pervez Z., Sarwar S., and Ahmed H. F. Similarity Level Method Based Static Software Birthmarks. In Proc. of the International Symposium on High Capacity Optical Networks and Enabling Technologies, 2008, pp. 205–210.
[9]. Schuler D., Dallmeier V., Lindig C. A dynamic birthmark for java. In Proc. of the 22nd IEEE/ACM International conference on Automated software engineering, 2007, pp. 274–283.
[10]. Nazir S., Shahzad S., Binti N., Alias, and Anwar S. A Novel Rules Based Approach for Estimating Software Birthmark. The Scientific World Journal, 2015.
[11]. Jorge E. N., Pirmez L., Costa O., Boccardo R., Bento M. Tiny Watermark: a code obfuscation-based software watermarking framework for wireless sensor networks. In Proc. of the ICWN'14-The 2014 International Conference on Wireless Networks, 2014.
[12]. Nayakoji N., Sonavane S. JavaScript Theft Detection using Birthmark and Subgraph Isomorphism. Journal of Engineering Computers & Applied Sciences, vol. 3, no. 8, 2014, pp. 1–5.
[13]. Che S. and Wang Y. A Software Watermarking Based on PE File with Tamper-proof Function. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 12, no. 2, 2014, pp. 1012–1021.
[14]. Zhu F. Concepts and techniques in software watermarking and obfuscation. PhD Thesis, The University of Auckland, New Zealand, 2007, 160 p.
[15]. Myles G., and Collberg C. Detecting software theft via whole program path birthmarks. Lecture Notes in Computer Science, vol. 3225, 2004, pp. 404–415.
[16]. Myles G. and Collberg C. K-gram based software birthmarks. In Proc. of the 2005 ACM symposium on Applied computing, 2005, pp. 314–318.
[17]. Tian Z., Liu T., Zheng Q. A new thread-aware birthmark for plagiarism detection of multithreaded programs. In Proc. of the 38th International Conference on Software Engineering Companion, 2016, pp. 734–736.
[18]. Tian Z., Liu T., Zheng Q. Exploiting Thread-Related System Calls for Plagiarism Detection of Multithreaded Programs. Journal of Systems and Software, vol. 119, 2016, pp. 136-148.
[19]. Bhattacharya S. Survey on Digital Watermarking–A Digital Forensics & Security Application. International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, issue 11, 2014.
[20]. Khan A., Siddiqa A., Munib S. A recent survey of reversible watermarking techniques. Information Sciences, vol. 279, 2014, pp. 251–272.
[21]. Zhou W., Zhang X., and Jiang X. AppInk: watermarking android apps for repackaging deterrence. In Proc. of the 8th ACM SIGSAC symposium on Information, computer and communications security, 2013, pp. 1–12.
[22]. Ren C., Chen K., and Liu P. Droidmarking: resilient software watermarking for impeding android application repackaging. In Proc. of the 29th ACM/IEEE international conference on Automated software engineering, 2014, pp. 635–646.
[23]. Guang S., Xiaoping F., Sha F., Yingjie S. Software Watermarking in the Cloud: Analysis and Rigorous Theoretic Treatment. Journal of Software Engineering, vol. 9, issue 2, 2015, pp. 410–418.
[24]. Rubini P., Leela S. A Survey On Plagiarism Detection In Text Mining. International Journal of Research in Computer Applications and Robotics, vol. 1, issue 9, 2013, pp. 117-119.
[25]. Oberreuter G., and Velásquez J. D. Text mining applied to plagiarism detection: The use of words for detecting deviations in the writing style. Expert Systems with Applications, vol. 40, issue 9, 2013, pp. 3756–3763.
[26]. Rana H., Stamp M. Hunting for Pirated Software Using Metamorphic Analysis. Information Security Journal: A Global Perspective, vol. 23, issue 3, 2014, pp. 68–85.
[27]. Costa M., Gong Z. Web structure mining: an introduction. In Proc. of the 2005 IEEE International Conference on Information Acquisition, 2005, pp. 590-595.
[28]. Vemparala S., Di Troia F., Corrado V., Austin H., and Stamo M. Malware Detection Using Dynamic Birthmarks. In Proc. of the 2016 ACM- International Workshop on Security And Privacy Analytics, 2016, pp. 41–46.
[29]. Zeng K., and Athanas P. A q-gram birthmarking approach to predicting reusable hardware. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016, pp. 1112–1115.
[30]. Bogdanov P., Baumer B., Basu P. As Strong as the Weakest Link: Mining Diverse Cliques in Weighted Graphs. Lecture Notes in Computer Science, vol. 8188, 2013, pp. 525–540.
[31]. Getoor L., Diehl P. Link mining: a survey. ACM SIGKDD Explorations Newsletter, vol. 7, issue 2, 2005, pp. 3–12.

[32]. Kavitha D., Rao M., Babu K. A Survey on Assorted Approaches to Graph Data Mining, International Journal of Computer Applications, vol. 14, no. 1, 2011, pp. 43–46.
[33]. Tamada H., Nakamura M., Monden A. Java Birthmarks–Detecting the Software Theft. IEICE transactions on information and systems, Vol. E88-D, issue 9, 2005, pp. 2148–2158.
[34]. Sorceforge.net, accessed on Nov 2, 2017.
[35]. Fan M., Liu J., Luo X. et al. Android Malware Familial Classification and Representative Sample Selection via Frequent Sub-graph Analysis, IEEE Transactions on Information Forensics and Security, vol. 13, issue 8, 2018, pp. 1890-1905.
[36]. Tian Z., T. Liu, Zheng Q. et al. Reviving Sequential Program Birthmarking for Multithreaded Software Plagiarism Detection. IEEE Transactions on Software Engineering, vol. 44, issue 5, 2018, pp. 491-511.

Информация об авторах / Information about authors

Сохаил САРВАР получил степень магистра в области информационных технологий в Национальном университете науки и технологии, Исламабад, Пакистан. Получил степень PhD на компьютерном факультете университета Гуджарата, Пакистан. Исследовательские интересы включают электронное обучение, семантические технологии и методы инженерии знаний.

Sohail SARWAR received the M.S. degree in information technology from National University of Science and Technology, Islamabad, Pakistan, and the Ph.D. degree in the Department of Computing, University of Gujrat, Pakistan. His research interests include e-learning, semantic technologies and knowledge engineering techniques.

Зия УЛЬ КАЙУМ в настоящее время является профессором в университете Гуджарата в Пакистане. Он получил степень PhD в области компьютерных наук в Университете Лидса, Великобритания, в 2005 году. В число научных интересов входят искусственный интеллект, инженерия знаний, интеллектуальный анализ знаний, семантический Web и электронное обучение.

Zia UL QAYYUM is currently a professor at University of Gujrat, Pakistan. He received his Ph.D. degree in computer science from Leeds University UK in 2005. His research interests include artificial intelligence, knowledge engineering, data mining, semantic web and e-learning.

Мухаммад САФЬЯН работает в Правительственном университете колледжа, Лахор, Пакистан. Он получил степень магистра в 2009 г. Национальном университете науки и технологии. Область его научных интересов включает отображение онтологий, электронное обучение, семантическое распознавание активностей.

Muhammad SAFYAN is in Government College University (GCU), Lahore. He received his MS degree from National University of Sciences and Technology in 2009. His area of interest is ontology alignment, e-learning and semantic activity recognition.

Муддессар ИКБАЛ работает старшим преподавателем в Лондонском университете Саут Бэнк и в университете Эссекса, Великобритания. Он получил степень PhD в Кингстонском университете, Лондон, Великобритания. Его научные интересы включают сетевые технологии 5G, мультимедийные облачные вычисления, мобильные граничные вычисления, туманные вычисления, интернет вещей, программно-конфигурируемые сети, виртуализацию сетевых функций, качество восприятия, облачные инфраструктуры и службы.

Muddessar IQBAL is working as senior lecturer in London South Bank University and University of Essex, England. Dr. Iqbal completed his PhD from Kingston University in 2010. His research interests include 5G networking technologies, multimedia cloud computing, mobile edge computing, fog computing, Internet of Things, software-defined networking, network function virtualisation, quality of experience, and cloud infrastructures and services.

Ясир МАХМУД работает преподавателем в Правительственном университете колледжа, Лахор, Пакистан. Он получил степень магистра в Национальном университете науки и

технологии. Область его научных интересов включает отображение онтологий, электронное обучение, защиту программного обеспечения.

Yasir MAHMOOD is a lecturer in Government College University (GCU), Lahore. He received his MS degree from National University of Sciences and Technology. His area of interest is ontology alignment, e-learning and software protection.

DOI: 10.15514/ISPRAS-2019-31(2)-13

Эффективное сравнение чисел в системе остаточных классов на основе позиционной характеристики

[1] *М.Г. Бабенко, ORCID: 0000-0001-7066-0061 <mgbabenko@ncfu.ru>*
[2,3,5] *А.Н. Черных, ORCID: 0000-0001-5029-5212 <chernykh@cicese.mx>*
[1] *Н.И. Червяков, ORCID: 0000-0002-4573-2032 <ncherviakov@ncfu.ru>*
[1] *В.А. Кучуков, ORCID: 0000-0002-1839-2765 <viktor-kuchukov@yandex.ru>*
[2] *В. Миранда-Лопес, ORCID: 0000-0002-1128-6660 <vmiranda@cicese.edu.mx>*
[2] *Р. Ривера-Родригес, ORCID: 0000-0002-1968-8525 <rrivera@cicese.mx>*
[4] *Чж. Ду, ORCID: 0000-0002-8435-1611 <duzh@tsinghua.edu.cn>*

[1] *Северо-Кавказский федеральный университет,*
355009, Россия, г. Ставрополь, ул. Пушкина, 1.
[2] *Центр научных исследований и высшего образования Энсенада,*
В.С. 22860, Мексика.
[3] *Институт системного программирования РАН им. В.П. Иванникова,*
109004, Россия, г. Москва, ул. А. Солженицына, д. 25.
[4] *Университет Цинхуа,*
Район Хайдянь, Пекин, 100084, КНР.
[5] *Южно-Уральский государственный университет,*
454080, Россия, г. Челябинск, ул. Ленина, 76.

Аннотация. Операция сравнения чисел широко используется при реализации большинства современных алгоритмов. Реализация алгоритма сравнения чисел в системе остаточных классов (СОК) состоит из двух этапов. Первый этап – вычисление позиционной характеристики модулярного числа. Второй этап – сравнение позиционных характеристик модулярных чисел в позиционной системе счисления. В статье предлагается новый эффективный алгоритм вычисления позиционной характеристики числа в СОК, основанный на использовании приближенного метода. Использование этого метода не требует дорогостоящих модульных операций, которые заменяются быстрыми битовыми операциями сдвиг вправо и взятия младших бит. Доказано, что в случае, когда динамический диапазон СОК является нечетным числом, размер операндов уменьшается на размер модуля. Если одно из оснований СОК является степенью двойки, то размер операндов меньше динамического диапазона.

Ключевые слова: система остаточных классов; немодульные операции; сравнение чисел; приближенный метод

Для цитирования: Бабенко М.Г., Черных А.Н., Червяков Н.И., Кучуков В.А., Миранда-Лопес В., Ривера-Родригес Р., Ду Чж. Эффективное сравнение чисел в системе остаточных классов на основе позиционной характеристики. Труды ИСП РАН, том 31, вып. 2, 2019 г., стр. 187-202. DOI: 10.15514/ISPRAS-2019-31(2)-13

Благодарности. Работа выполнена при поддержке стипендии Президента РФ молодым ученым и аспирантам, МК-341.2019.9, СП-2236.2018.5, а также грантов РФФИ 18-07-01224, 18-07-00109.

Efficient Number Comparison in the Residue Number System based on Positional Characteristics

[1] *M.G. Babenko, ORCID: 0000-0001-7066-0061 <mgbabenko@ncfu.ru>*
[2,3,5] *A.N. Tchernykh, ORCID: 0000-0001-5029-5212 <chernykh@cicese.mx>*
[1] *N.I, Chervyakov, ORCID: 0000-0002-4573-2032 <ncherviakov@ncfu.ru>*
[1] *V.A. Kuchukov, ORCID: 0000-0002-1839- <vkuchukov@ncfu.ru>*
[2] *V. Miranda-López, ORCID: 0000-0002-1128-6660 <vmiranda@cicese.edu.mx>*
[2] *R. Rivera-Rodriguez, ORCID: 0000-0002-1968-8525 <rrivera@cicese.mx>*
[4] *Z. Du, ORCID: 0000-0002-8435-1611 <duzh@tsinghua.edu.cn>*

[1] *North-Caucasus Federal University,*
1, Pushkin st., Stavropol, 355009, Russia.
[2] *CICESE Research Center,*
Ensenada, Baja California, 22860, Mexico.
[3] *Ivannikov Institute for System Programming of the Russian Academy of Sciences,*
25, Alexander Solzhenitsyn st., Moscow, 109004, Russia.
[4] *Tsinghua University,*
Haidian District, Beijing, 100084, P. R. China
[5] *South Ural State University,*
Chelyabinsk, 76 Lenina St., Chelyabinsk, 454080, Russia.

Abstract. An important operation for data processing is a number comparison. In Residue Number System (RNS), it consists of two steps: the computation of the positional characteristic of the number in RNS representation and comparison of its positional characteristics in the positional number system. In this paper, we propose a new efficient method to compute the positional characteristic based on the approximate method. The approximate method as a tool to compare numbers does not require resource-consuming non-modular operations that are replaced by fast bit right shift operations and taking the least significant bits. We prove that in case when the dynamic range of RNS is an odd number, the size of the operands is reduced by the size of the module. If one of the RNS moduli is a power of two, then the size of the operands is less than the dynamic range. It makes our method efficient for hardware implementation of cryptographic primitives and digital signal processing.

Keywords: residue number system, non-modular operation, number comparison, approximate method

For citation: Babenko M., Tchernykh A., Chervyakov N., Kuchukov V., Miranda-López V., Rivera-Rodriguez R., Du Z. Efficient Number Comparison in the Residue Number System based on Positional Characteristics. Trudy ISP RAN/Proc. ISP RAS, vol. 31, issue 2, 2019. pp. 187-202 (in Russian). DOI: 10.15514/ISPRAS-2019-31(2)-13

Acknowledgements. This work was partly supported by the scholarship of the President of the Russian Federation to young scientists and graduate students МК-341.2019.9, СП-2236.2018.5, and also grants of RFBR 18-07-01224, 18-07-00109

1. Введение

При использовании непозиционных систем счисления, таких как система остаточных классов (СОК), выполнение высокопроизводительных вычислений возможно за счет отсутствия переносов между разрядами. Однако во многих прикладных задачах возникает необходимость сравнения чисел. Данная операция является базовой при реализации большого числа алгоритмов защиты информации (Chang et al., 2015 [1], Chervyakov et al., 2017 [2], Sousa et al., 2016 [3]), цифровой обработки сигналов (Chervyakov et al., 2014) [4], систем беспроводной связи (Ye et al., 2018) [5], облачных вычислений (Tchernykh et al., 2016 [6], Miranda-López et al., 2017 [7], Tchernykh et al., 2017 [8], Babenko et al., 2017 [9]) и т.д.

Из-за непозиционной природы СОК немодульные операции, такие как сравнение чисел, определение знака числа и определение переполнения динамического диапазона, относятся к вычислительно сложным операциям.

В позиционной системе счисления существуют простые алгоритмы сравнения чисел, которые сводятся к их поразрядному сравнению. В СОК простых алгоритмов сравнения чисел нет (Szabo & Tanaka, 1969) [10]. Реализация алгоритма сравнения чисел в СОК состоит из двух этапов. Первый этап – вычисление позиционной характеристики (ПХ) модулярных чисел $X = (x_1, x_2, \dots, x_n)$ и $Y = (y_1, y_2, \dots, y_n)$. Второй этап – сравнение позиционных характеристик ПХ(X) и ПХ(Y) модулярных чисел в позиционной системе счисления (ПСС).

В качестве ПХ модулярного числа может выступать его представление в ПСС. Для перевода числа из СОК в ПСС можно использовать один из алгоритмов: Китайскую теорему об остатках (КТО), обобщенную позиционную систему счисления (Bi & Gross, 2008) [11], рекурсивный алгоритм сдваивания чисел (nCRT) (Wang, 2000) [12] и их модификации.

Большая вычислительная сложность алгоритмов вычисления искомого числа в двоичной системе счисления сподвигла исследователей на поиск его аппроксимации. С целью уменьшения вычислительной сложности операции сравнения чисел в СОК исследователи предложили в качестве ПХ модулярного числа использовать следующие функции: диагональная функция (Dimauro et al., 1993) [13], функция ядра (Burgess, 2003) [14], фактор-функция (Dimauro et al., 2003) [15], монотонная функция Pirlo (Pirlo and Impedovo, 2013) [16] и др. Предлагаемые алгоритмы вычисления ПХ позволяют уменьшить вычислительную сложность за счет уменьшения размерности операндов при выполнении операции деления с остатком.

Самым эффективным является подход, основанный на приближенном методе (Chervyakov et al., 2017) [17], так как он позволяет заменить операцию деления с остатком на операцию взятия старших бит числа. В статье мы предлагаем оптимизировать приближенный метод для вычисления операции сравнения чисел за счет уменьшения количества операций деления с остатком и улучшенной точности вычисления для корректной работы алгоритма.

Далее статья организована следующим образом. В разд. 2 нами рассмотрены основные положения СОК и ее свойства. В разд. 3 рассмотрены методы сравнения чисел, основанные на переводе чисел из СОК в ПСС. В разд. 4 проведен обзор методов сравнения на основе вычисления позиционных характеристик. В разд. 5 исследуется вопрос сравнения чисел в СОК с использованием методов определения знака числа. Разд. 6 посвящен модификации метода сравнения чисел и исследованию его свойств. В заключении представлены сравнение предложенного метода с существующими и основные выводы.

2. Система остаточных классов и ее свойства

Под остатком числа X по модулю p_i понимается число x_i, удовлетворяющее выражению $X = x_i + b \cdot p_i$ для некоторого числа b и $0 \leq x_i < p_i$. Остаток от деления можно записать в терминах теории сравнений $x_i \equiv X \bmod p_i$, или для краткости $|X|_{p_i}$.

СОК определяется набором взаимно простых чисел p_i, называемых модулями, т.е. $\{p_1, p_2, \dots, p_n\}$, где НОД$(p_i, p_j) = 1$ для $i \neq j$, n – количество модулей. Любое число $X \in [0, P-1]$ может быть представлено в СОК единственным образом как $X = (x_1, x_2, \dots, x_n)$, где $x_i \equiv X \bmod p_i$, а $P = \prod_{i=1}^{n} p_i$ – динамический диапазон.

Особенностью СОК является возможность выполнения операций сложения, вычитания и умножения параллельно и независимо по каждому из модулей. Пусть даны два числа $X = (x_1, x_2, \dots, x_n)$ и $Y = (y_1, y_2, \dots, y_n)$, тогда, как показано в (Акушский & Юдицкий, 1968) [20], выполняется

$$C = X * Y = \left(|x_1 * y_1|_{p_1}, \dots, |x_n * y_n|_{p_n}\right),$$

где $*= \{+, -, \times\}$.

Однако, при выполнении арифметических операций возможна ситуация, когда результат выходит за диапазон $C \notin [0, P-1]$, т.е. происходит переполнение, и результат будет отличен от ожидаемого на размер диапазона. Для проверки корректности результата в статье (Chervyakov et al., 2017) [2] разработана схема, основанная на использовании свойств ранга числа. Преимущество предложенного подхода заключается в том, что он позволяет проверить корректность результата, не восстанавливая само число.

Использование метода приближенного вычисления ранга числа позволяет уменьшить вычислительную сложность алгоритмов перевода чисел из СОК в позиционную систему счисления.

3. Методы сравнения чисел, основанные на переводе чисел из СОК в ПСС

В большинстве методов задача сравнения чисел решается через перевод числа из СОК в ПСС и их сравнение.

3.1 Китайская теорема об остатках

Согласно (Omondi & Premkumar, 2007) [21], для перевода числа из СОК в ПСС используется стандартное восстановление с помощью КТО, которую можно записать формулой:

$$X = \left| \sum_{i=1}^{n} P_i \cdot x_i \cdot |P_i^{-1}|_{p_i} \right|_P, \quad (1)$$

где $P_i = \frac{P}{p_i}$, а $|P_i^{-1}|_{p_i}$ – мультипликативная инверсия P_i по модулю p_i. Рассмотрим примеры восстановления числа по формуле (1) и сравнения чисел.

Пусть дана СОК {3,5,7} и числа $X = (2, 2, 3)$, $Y = (1, 3, 4)$. Динамический диапазон данной системы остаточных классов равен $P = 3 \cdot 5 \cdot 7 = 105$.

Вычислим P_i:

$$P_1 = \frac{P}{p_1} = \frac{105}{3} = 35, \qquad P_2 = \frac{P}{p_2} = \frac{105}{5} = 21, \qquad P_3 = \frac{P}{p_3} = \frac{105}{7} = 15.$$

Чтобы вычислить мультипликативную инверсию P_i, нужно найти такое x, которое удовлетворяет сравнению $x \cdot P_i \equiv 1 \bmod p_i$. Таким образом, $|P_1^{-1}|_3 = 2$, $|P_2^{-1}|_5 = 1$, $|P_3^{-1}|_7 = 1$. Таким образом, все необходимые для вычисления (1) данные получены. Найдем значение первого числа:

$$X = |35 \cdot 2 \cdot 2 + 21 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 1|_{105} = |227|_{105} = 17.$$

Найдем значение второго числа:

$$Y = |35 \cdot 1 \cdot 2 + 21 \cdot 3 \cdot 1 + 15 \cdot 4 \cdot 1|_{105} = |193|_{105} = 88.$$

Так как $17 < 88$, значит $X < Y$.

Учитывая вычислительную сложность вычисления остатка от деления на большое число P, исследователи предложили альтернативный подход, основанный на обобщенной позиционной системе счисления.

3.2 Обобщенная позиционная система счисления (ОПСС)

ОПСС за счет своих свойств позволяет сравнивать два числа без прямого востановления самого сисла. Число в ОПСС задается кортежем $[a_1, a_2, \dots, a_n]$, а основаниями системы

являются p_1, p_1p_2, $p_1p_2p_3$, …, $p_1, p_2, \dots, p_{n-1}$, где $p_1, p_2, \dots, p_n$ – модули СОК. Связь между двоичной системой счисления и ОПСС определяется по следующей формуле:

$$X = a_1 + a_2p_1 + a_3p_1p_2 + \cdots + a_np_1p_2 \dots p_{n-1},$$

Так как ОПСС является позиционной системой счисления, то сравнение чисел равносильно сравнению двух кортежей $[a_1, a_2, \dots, a_n]$ и $[b_1, b_2, \dots, b_n]$.

Для перевода числа $X = (x_1, x_2, \dots, x_n)$ из СОК в $[a_1, a_2, \dots, a_n]$ ОПСС используется следующий подход:

$a_1 = x_1$,

$a_2 = |(x_2 - a_1) \cdot p_1^{-1}|_{p_2}$,

$a_3 = |(x_3 - a_1 - a_2p_1) \cdot p_1^{-1} \cdot p_2^{-1}|_{p_3}$,

……

$a_n = |(x_n - a_1 - a_2p_1 - \cdots - a_{n-1}p_1p_2 \dots p_{n-2}) \cdot p_1^{-1} \cdot \dots \cdot p_{n-1}^{-1}|_{p_n}$.

Эффективная реализация алгоритма сравнения чисел с использованием ОПСС представлена в работе (Isupov, 2016) [22].

Использование ОПСС позволяет уйти от вычисления остатка от деления на большое число P, но приводит к использованию большего количества модульных операций по модулям СОК.

3.3 Приближенный метод

Для исключения операции деления с остатком на большое простое число в статье (Van, 1985) [23] предложен приближенный метод, основанный на отображении, переводящем $[0, P)$ в $[0, 2)$. Для этого перепишем (1) в виде

$$X = \sum_{i=1}^{n} P_i \cdot x_i \cdot |P_i^{-1}|_{p_i} - P \cdot r_x, \tag{2}$$

для некоторого неотрицательного целого числа r_x - ранга числа. Разделив (2) на $\frac{P}{2}$, получим

$$X_s = \left(\frac{2}{P}\right) \cdot X = \sum_{i=1}^{n} \frac{2}{p_i} \cdot x_i \cdot |P_i^{-1}|_{p_i} - 2r_x. \tag{3}$$

Таким образом, из (3), X_s может быть вычислен как сумма дробных чисел с отбрасыванием кратной двум целой части результата. Это может быть получено довольно тривиально, поскольку вычисления выполняются в двоичном виде. Проиллюстрируем это на примере. Пусть дано число $(2, 2, 3)$, тогда по формуле (3) получим

$$X_s = \left|\frac{2}{3} \cdot 2 \cdot 2 + \frac{2}{5} \cdot 2 \cdot 1 + \frac{2}{7} \cdot 3 \cdot 1\right|_2 = \left|2\frac{34}{105}\right|_2 = \frac{34}{105}.$$

Заметим, что в данном методе слагаемые редко могут быть представлены в виде конечной дроби. Для представления в виде десятичной (двоичной) дроби каждое слагаемое должно быть определенным образом округлено.

Если на каждое слагаемое суммы в формуле (3) выделить $N + 1$ бит, 1 – на целую часть и N – на дробную, и усекать оставшиеся биты, то ошибка в каждом слагаемом будет удовлетворять неравенству $0 \leq e_i < 2^{-N}$. И поскольку таких слагаемых n, то максимальная ошибка при усечении (3) будет $e = n2^{-t}$.

Поскольку числа X_s распределены равномерно на интервале $[0, P)$, то расстояние между двумя соседними числами равно $\frac{2}{P}$.

Кроме того, интервал между наибольшим положительным числом и 1 равен $\frac{2}{P}$ для четного P и $\frac{1}{P}$ для нечетного P.

Таким образом, для того, чтобы усеченное значение X_s соотносилось с точным значением X_s, ошибка должна удовлетворять следующим соотношениям:

$$n \cdot 2^{-N} \leq \frac{2}{P}, \text{для четного } P \tag{4}$$

$$n \cdot 2^{-N} \leq \frac{1}{P}, \text{для нечетного } P, \tag{5}$$

или

$$N \geq \lceil \log_2 P \cdot n \rceil - 1 \text{ для четного } P,$$
$$N \geq \lceil \log_2 P \cdot n \rceil \text{ для нечетного } P.$$

Хотя дробное представление и требует примерно на $\lceil \log_2 n \rceil$ бит больше, но простота и скорость выполнения операций компенсируют эту избыточность. Данный способ вычисления X_s может быть относительно просто вычислен с использованием памяти, хранящей предвычисленные значения, , на вход которой подается остаток $|X|_{p_i}$, а на выход поступает усеченное значение, а далее усеченные значения складываются по модулю 2, что легко реализуется аппаратно.

Рассмотрим численный пример. Пусть в СОК $\{3, 5, 7\}$ заданы два числа $1 = (1, 1, 1)$ и $104 = (2, 4, 6)$. Для данной системы $N \geq \lceil \log_2(105 \cdot 3) \rceil = 9$. Рассмотрим первое число по слагаемым:

$$\left|\frac{2}{3} \cdot 1 \cdot 2\right|_2 = \frac{4}{3} = 1.010101010101011 \ldots \approx 1.010101011,$$
$$\left|\frac{2}{5} \cdot 1 \cdot 1\right|_2 = \frac{2}{5} = 0.011001100110011 \ldots \approx 0.011001101,$$
$$\left|\frac{2}{7} \cdot 1 \cdot 1\right|_2 = \frac{2}{7} = 0.010010010010010 \ldots \approx 0.010010010.$$

Просуммируем по модулю 2 полученные слагаемые и получим 0.000001010.

Рассмотрим второе число:

$$\left|\frac{2}{3} \cdot 2 \cdot 2\right|_2 = \left|\frac{8}{3}\right|_2 = \frac{2}{3} = 0.101010101010101 \ldots \approx 0.101010101,$$
$$\left|\frac{2}{5} \cdot 1 \cdot 4\right|_2 = \frac{8}{5} = 1.100110011001101 \ldots \approx 1.100110011,$$
$$\left|\frac{2}{7} \cdot 1 \cdot 6\right|_2 = \frac{12}{7} = 1.101101101101110 \ldots \approx 1.101101110.$$

Просуммируем по модулю 2 полученные слагаемые и получим 1.111110110.

Сравнивая полученные значения, увидим что $(1, 1, 1) < (2, 4, 6)$.

Данный метод эффективнее, чем восстановление числа с помощью классической Китайской теоремы об остатках, однако возникает вопрос о достаточности или избыточности точности согласно формулам (4)-(5).

Стоит заметить, что использование данного подхода позволяет вычислять позиционную характеристику с применением следующей формулы:

$$V(X) = \left| \sum_{i=1}^{n} \left\lceil \frac{2}{p_i} \left| |P_i^{-1}|_{p_i} \cdot x_i \right|_{p_i} \right\rceil_{2^{-N}} \right|_2, \tag{6}$$

где $\lceil x \rceil_{2^{-N}} = \lceil 2^N x \rceil / 2^N$.

С целью уменьшения количества операций в приближенном методе в (Chervyakov et al., 2017) [17] предложено использовать следующую формулу:

$$C(X) = \left| \sum_{i=1}^{n} W_i x_i \right|_1, \tag{7}$$

где $W_i = \left\lfloor \frac{2^N |p_i^{-1}|_{p_i}}{p_i} \right\rfloor / 2^N$, $|x|_1$-дробная часть числа x, $N = \lceil \log_2(P\rho) \rceil$ и $\rho = -n + \sum_{i=1}^{n} p_i$.

Преимущество данного метода состоит в том, что он не требует дополнительных операции округления вверх, однако при этом увеличились размеры операндов.

4. Методы сравнения чисел в СОК с использованием позиционных характеристик

С целью уменьшения вычислительной сложности алгоритма сравнения чисел исследователи (Dimauro et al., 1993) [13] предложили использовать монотонную диагональную функцию.

4.1 Диагональная функция

Отличным от вышеизложенных методов сравнения чисел является метод на основе специальной диагональной функции, которая определяется как сумма соответствующих коэффициентов P_i и называется методом суммы коэффициентов (Sum of Quotients Technique, SQT), описание которой можно найти, например, в (Dimauro et al., 1993) [13]. Диагональная функция представляет собой монотонно возрастающую функцию, на основе которой возможно сравнение чисел.

Диагональная функция имеет вид:

$$D(X) = \left\lfloor \frac{X}{p_1} \right\rfloor + \left\lfloor \frac{X}{p_2} \right\rfloor + \cdots + \left\lfloor \frac{X}{p_n} \right\rfloor. \tag{8}$$

Однако формула (8) является мало пригодной на практике. В связи с этим (Dimauro et al., 1993) [13] была предложена аналитическая функция для вычисления диагональной функции:

$$D(X) = \left| \sum_{i=1}^{n} k_i^* \cdot x_i \right|_{SQ} \tag{9}$$

где $k_i^* = |-p_i^{-1}|_{SQ}$, где $i = 1, \dots, n$, $SQ = P_1 + P_2 + \cdots + P_n$.

Так как диагональная функция (9) является монотонно возрастающей, то она может быть использована для сравнения чисел, т.е. если $D(X) < D(Y)$, то $X < Y$. Однако, возможны случаи, когда $D(X) = D(Y)$, и тогда $X < Y$, когда $x_i < y_i$, $i = 1, \dots, n$.

Рассмотрим пример сравнения чисел. Возьмем ранее использованные числа $X = (2, 2, 3)$ и $Y = (1, 3, 4)$. Для начала вычислим значения

$SQ = 35 + 21 + 15 = 71,$
$k_1^* = |-p_1^{-1}|_{71} = |-3^{-1}|_{71} = 47,$
$k_2^* = |-p_2^{-1}|_{71} = |-5^{-1}|_{71} = 14,$
$k_3^* = |-p_3^{-1}|_{71} = |-7^{-1}|_{71} = 10.$

Найдем значение диагональной функции:

$D(X) = |2 \cdot 47 + 2 \cdot 14 + 3 \cdot 10|_{71} = 10,$
$D(Y) = |1 \cdot 47 + 2 \cdot 14 + 3 \cdot 10|_{71} = 34.$

Т.к. $D(X) < D(Y)$, то $X < Y$.

4.2 Функция ядра Акушского

Обобщив результат, полученный (Dimauro et al., 1993) [13], исследовательская группа (Pirlo & Impedovo, 2013) [16] предложила использовать минимальную функцию ядра Акушского без критических ядер. Данный подход является аналогичным методу диагональной функции. Функция Pirlo имеет следующий вид:

$$Pi(X) = \left\lfloor \frac{X}{p_n} \right\rfloor \tag{10}$$

Однако формула (10) является мало пригодной на практике, в связи с этим была предложена аналитическая функция для вычисления Pirlo функции:

$$Pi(X) = \left| \sum_{i=1}^{n} k_i^{**} \cdot x_i \right|_{P_n} \tag{11}$$

где $k_i^{**} = \left\lfloor \frac{|P_i^{-1}|_{p_i} P_i}{p_n} \right\rfloor$.

Так как функция Pirlo (11) является монотонно возрастающей, то она может быть использована для сравнения чисел, т.е. если $Pi(X) < Pi(Y)$, то $X < Y$. Однако возможны случаи, когда $Pi(X) = Pi(Y)$, и в этом случае $X < Y$, когда $x_n < y_n$.

Рассмотрим пример сравнения чисел. Возьмем ранее использовавшиеся числа $X = (2, 2, 3)$ и $Y = (1, 3, 4)$. Для начала вычислим значения:

$$P_3 = 15,$$
$$k_1^{**} = \left\lfloor \frac{|P_1^{-1}|_{p_1} P_1}{p_3} \right\rfloor = \left\lfloor \frac{2 \cdot 35}{7} \right\rfloor = 10,$$
$$k_2^{**} = \left\lfloor \frac{|P_2^{-1}|_{p_2} P_2}{p_3} \right\rfloor = \left\lfloor \frac{1 \cdot 21}{7} \right\rfloor = 3,$$
$$k_3^{*} = \left\lfloor \frac{|P_3^{-1}|_{p_3} P_3}{p_3} \right\rfloor = \left\lfloor \frac{1 \cdot 15}{7} \right\rfloor = 2.$$

Найдем значение функции Pirlo:

$$\mathrm{Pi(X)} = |2 \cdot 10 + 2 \cdot 3 + 3 \cdot 2|_{15} = 2,$$
$$\mathrm{Pi(Y)} = |1 \cdot 10 + 3 \cdot 3 + 4 \cdot 2|_{15} = 12$$

и поскольку $Pi(X) < Pi(Y)$, то $X < Y$.

Как показано в работе (Mohan, 2016) [24], функция Pirlo проигрывает Китайской теореме об остатках, так как требует дополнительных сравнений чисел.

5. Сравнение чисел на основе алгоритма определения знака числа

С целью оптимизации алгоритма сравнения чисел иногда целесообразно использовать на втором этапе вместо алгоритма сравнения алгоритм определения знака числа.

Некоторые приложения в СОК требуют использования отрицательных чисел. Для определения знака числа в СОК с отрицательными числами необходимо сравнить это число с серединой диапазона. Следует также обратить внимание, что в данном случае отрицательные числа идут за положительными, и для сравнения чисел сначала нужно определить их знак.

В СОК с модулями $\{p_1, p_2, \dots, p_n\}$ и динамическим диапазоном $P = \prod_{i=1}^{n} p_i$ может быть представлено число X, удовлетворяющее следующим соотношениям:

$$-\frac{P-1}{2} \leq X \leq \frac{P-1}{2}, \text{если } P \text{ нечетное},$$
$$-\frac{P}{2} \leq X \leq \frac{P}{2}-1, \text{если } P \text{ четное}.$$

Тогда, согласно (Omondi & Premkumar, 2007) [21], если $X=(x_1,x_2,\dots,x_n)$, то отрицательным будет число $-X=(\overline{x_1},\overline{x_2},\dots,\overline{x_n})$, где $\overline{x_i}$ является дополнением x_i до модуля m_i. Например, для СОК {3,5,7} и числа $X=17=(2,2,3)$ получим $-X=(3-2,5-2,7-3)=(1,3,4)$. Очевидно, что для перехода от восстановленного числа к отрицательной форме необходимо отнять значение динамического диапазона, т.е. $(1,3,4)=88=88-105=-17$. Если рассматривать весь динамический диапазон, то числа распределяются следующим образом: $\underline{0,1,\dots,52,}$ $\overline{-52,-51,\dots,-1}$.

Теперь, когда заданы отрицательные числа, возникает необходимость определения знака числа. Существует ряд подходов к определению знака чисел в СОК: восстановление числа с помощью Китайской теоремы об остатках (КТО), использование обобщенной позиционной системы счисления (ОПСС) и другие.

Проблемой КТО является необходимость нахождения остатка по большому модулю P, что является довольно трудоемкой задачей, и последующего сравнения с константой.

Введем функцию знака $S(X)$ для системы с нечетным динамическим диапазоном P (в случае четного диапазона границей служит $\frac{P}{2}$):

$$S(X)=\begin{cases}0, \text{если } 0 \leq X < \dfrac{P-1}{2},\\ 1, \text{если } \dfrac{P-1}{2} \leq X < P.\end{cases} \quad (12)$$

Рассмотрим на примере сравнение чисел с использованием отрицательных чисел. Пусть необходимо сравнить числа $X=17=(2,2,3)$ и $Y=-8=(1,2,6)$ в СОК {3,5,7}. Если $X>Y$, то $(X-Y)>0$. Найдем разность

$$X-Y=(2-1,2-2,3-6)=(1,0,4).$$

Применим приближенную формулу на основе КТО и будем сравнивать результат с серединой диапазона, т.е. с $\frac{1}{2}$. Все константы предварительно вычислены в предыдущих примерах.

$$\frac{X}{P}=\left|\sum_{i=1}^{3}\frac{x_i\cdot|P_i^{-1}|_{p_i}}{p_i}\right|_1=\left|\frac{2}{3}+\frac{4}{7}\right|_1=\frac{5}{21}<\frac{1}{2}.$$

Очевидно, что поскольку полученное значение меньше середины диапазона, то оно положительное, и значит $X>Y$.

Стоит отметить, что для корректной работы алгоритма сравнения чисел на основе алгоритма определения знака числа требуется удвоение диапазонов СОК, что ведет к дополнительным вычислительным нагрузкам при обработке данных, однако в данном случае необходимо нахождение лишь одной позиционной характеристики числа

6. *Модификация алгоритма сравнения чисел в СОК*

В качестве позиционной характеристики рассмотрим следующую функцию:

$$f(X)=\left|\sum_{i=1}^{n}\overline{k_i}\ x_i\right|_{2^N},$$

где $\overline{k_i}=\left\lfloor\frac{2^N|P^{-1}|_{p_i}}{p_i}\right\rfloor$.

6.1 Сравнение числа в СОК с нечетным диапазоном

Лемма 1. Если $N = \lceil \log_2(n \cdot P - n) \rceil$, то справедливо следующее равенство:

$$\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}\, x_i}{2^N} \right\rfloor = \left\lfloor \frac{\sum_{i=1}^{n} k_i x_i}{P} \right\rfloor, \qquad (14)$$

где $\overline{k_i} = \left\lfloor \frac{2^N |P^{-1}|_{p_i}}{p_i} \right\rfloor$ и $k_i = |P^{-1}|_{p_i} P_i$.

Доказательство.

Так как k_i и $\overline{k_i}$ связаны равенством $\overline{k_i} = \frac{2^N k_i}{P} - \frac{|2^N k_i|_P}{P}$, то выражение $\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}\, x_i}{2^N} \right\rfloor$ примет вид:

$$\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}\, x_i}{2^N} \right\rfloor = \left\lfloor \frac{1}{P} \sum_{i=1}^{n} k_i\, x_i - \frac{1}{P \cdot 2^N} \sum_{i-1}^{n} |2^N k_i|_P \cdot x_i \right\rfloor \qquad (15)$$

Подставим $\frac{1}{P} \sum_{i=1}^{n} k_i\, x_i = \left\lfloor \frac{1}{P} \sum_{i=1}^{n} k_i\, x_i \right\rfloor + \frac{X}{P}$ в (15), получим:

$$\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}\, x_i}{2^N} \right\rfloor = \left\lfloor \frac{\sum_{i=1}^{n} k_i x_i}{P} \right\rfloor + \left\lfloor \frac{X}{P} - \frac{1}{P \cdot 2^N} \cdot \sum_{i=1}^{n} |2^N k_i|_P\, x_i \right\rfloor \qquad (16)$$

Из (16) следует, что условие леммы 1 эквивалентно следующему неравенству:

$$0 \le \frac{X}{P} - \frac{1}{P \cdot 2^N} \cdot \sum_{i=1}^{n} |2^N k_i|_P\, x_i < 1 \qquad (17)$$

Согласно Китайской теореме об остатках, X удовлетворяет условию $0 \le X < P$, следовательно, $0 \le \frac{X}{P} < 1$. Принимая во внимание, что $\frac{1}{P \cdot 2^N} \cdot \sum_{i=1}^{n} |2^N k_i|_P\, x_i \ge 0$, мы получаем, что правая часть двойного неравенства (17) верна для всех N.

Рассмотрим левую часть двойного неравенства (17). При $X = 0$ она выполняется для любого N. Пусть X удовлетворяет неравенству $1 \le X < P$, тогда левую часть неравенства (17) можно представить в следующем виде:

$$2^N \ge \frac{1}{X} \sum_{i=1}^{n} |2^N k_i|_P\, x_i \qquad (18)$$

Так как $|2^N k_i|_P \le P - 1$, то $\sum_{i=1}^{n} |2^N k_i|_P\, x_i \le (P-1) \sum_{i=1}^{n} x_i$, следовательно, для всех $1 \le X < P$ справедливо следующее неравенство:

$$\frac{1}{X} \sum_{i=1}^{n} |2^N k_i|_P\, x_i \le n \cdot (P-1) \qquad (19)$$

Из (18) и (19) следует, что если $N = \lceil \log_2(-n + n \cdot P) \rceil$, то левая часть неравенства (17) выполняется, следовательно, равенство (14) выполняется. Лемма доказана.

Теорема 1. Если $N = \lceil \log_2(-n + n \cdot P) \rceil$, то функция $f(X)$ – строго возрастающая.

Доказательство.

Для того чтобы $f(X)$ являлась строго возрастающей функцией, необходимо и достаточно, чтобы для всех целых чисел $1 \le X \le P - 1$ выполнялось следующее условие:

$$f(X) - f(X-1) > 0 \qquad (20)$$

Так как $|X|_{2^N} = X - \left\lfloor \frac{X}{2^N} \right\rfloor \cdot 2^N$, то функцию $f(X)$ можно представить в следующем виде:

$$f(X) = \sum_{i=1}^{n} \overline{k_i}\, x_i - \left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}\, x_i}{2^N} \right\rfloor \cdot 2^N \qquad (21)$$

Принимая во внимание, что $\sum_{i=1}^{n} \overline{k_i}\, \left(x_i - |x_i - 1|_{p_i}\right) = \sum_{i=1}^{n} \overline{k_i} - \sum_{x_i=0} \overline{k_\iota}\, p_i$, то получим, что

$$f(X) - f(X-1) = \\ = \sum_{i=1}^{n} \overline{k_i} - \sum_{x_i=0} \overline{k_i} p_i - \left(\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i} x_i}{2^N} \right\rfloor - \left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i} |x_i - 1|_{p_i}}{2^N} \right\rfloor \right) \cdot 2^N \quad (22)$$

Так как условие леммы 1 выполнено, то

$$\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i} x_i}{2^N} \right\rfloor - \left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i} |x_i - 1|_{p_i}}{2^N} \right\rfloor = \left\lfloor \frac{\sum_{i=1}^{n} k_i x_i}{P} \right\rfloor - \left\lfloor \frac{\sum_{i=1}^{n} k_i |x_i - 1|_{p_i}}{P} \right\rfloor \quad (23)$$

Используя теорему из работы (Chervyakov, et. al., 2017) [2] и лемму 1, формула (23) примет вид:

$$\left\lfloor \frac{\sum_{i=1}^{n} k_i x_i}{P} \right\rfloor - \left\lfloor \frac{\sum_{i=1}^{n} k_i |x_i - 1|_{p_i}}{P} \right\rfloor = \left\lfloor \frac{\sum_{i=1}^{n} k_i}{P} \right\rfloor - \sum_{x_i=0} |P_i^{-1}|_{p_i} = \\ = \left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}}{2^N} \right\rfloor - \sum_{x_i=0} |P_i^{-1}|_{p_i} \quad (24)$$

Подставив (24) в (22), получим:

$$f(X) - f(X-1) = \\ = \sum_{i=1}^{n} \overline{k_i} - \sum_{x_i=0} \overline{k_i} p_i - \left(\left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}}{2^N} \right\rfloor - \sum_{x_i=0} |P_i^{-1}|_{p_i} \right) \cdot 2^N \quad (25)$$

Так как $\sum_{i=1}^{n} \overline{k_i} - \left\lfloor \frac{\sum_{i=1}^{n} \overline{k_i}}{2^N} \right\rfloor \cdot 2^N = \left| \sum_{i=1}^{n} \overline{k_i} \right|_{2^N}$ и $|P_i^{-1}|_{p_i} \cdot 2^N - \overline{k_i} p_i = \frac{|2^N k_i|_P}{P_i}$ то для всех $i = \overline{1,n}$ формула (25) примет вид:

$$f(X) - f(X-1) = \left| \sum_{i=1}^{n} \overline{k_i} \right|_{2^N} + \sum_{x_i=0} \frac{|2^N k_i|_P}{P_i} \quad (26)$$

Так как $\left| \sum_{i=1}^{n} \overline{k_i} \right|_{2^N} > 0$, то из (26) следует, что $f(X) - f(X-1) > 0$, и, следовательно, функция $f(X)$ строго возрастает. Теорема доказана.

Из теоремы 1 следует, что введенная функция является строго монотонной, следовательно, ее можно использовать в качестве позиционной характеристики для сравнения чисел в СОК.

Предложенный подход позволяет уменьшить вычислительную сложность алгоритма сравнения чисел в СОК. Эффективная аппаратная реализация операции $|x \cdot y|_{2^N}$ позволяет уменьшить логическую схему при аппаратной реализации по сравнению с классическим умножением двух чисел $x \cdot y$.

6.2 Сравнение чисел в СОК, если один из модулей равен степени двойки

Так как модули СОК являются взаимно простыми числами, следовательно, четный модуль только один. Значит, без потери общности будем считать, что n-ый модуль имеет вид $p_n = 2^t$. Так как $p_n = 2^t$, то используя свойство СОК, числа X, Y могут быть представлены в следующем виде:

$$X = A \cdot 2^t + x_n, Y = B \cdot 2^t + y_n. \quad (27)$$

Для сравнения чисел сравним A и B. Если A$< B$, то $X < Y$. В случае, когда $A = B$, $X < Y$ при условии, что $x_n < y_n$.

Так как n-ый модуль СОК четный, следовательно, модули $p_1, p_2, \dots, p_{n-1}$ являются нечетными числами, тогда P_n - нечетное число. Коэффициенты A и B удовлетворяют

неравествам: $0 \le A < P_n$ и $0 \le B < P_n$. Вычислив значения A и B в СОК по модулям $p_1, p_2, \dots, p_{n-1}$, мы можем сравнить их, используя введеную функцию $f(X)$.

Таким образом, алгоритм сравнение чисел X и Y будет иметь вид:

Алгоритм. Алгоритм сравнения чисел X и Y.

Input: $X \xrightarrow{RNS} (x_1, x_2, \dots, x_n)$,
$Y \xrightarrow{RNS} (y_1, y_2, \dots, y_n)$,
$p_1, p_2, \dots, p_{n-1}, p_n$,
$I_i = \left|\frac{1}{p_n}\right|_{p_i}$ для всех $i = \overline{1, n-1}$,
$\overline{k_\iota} = \left\lfloor 2^N \cdot |1/P_i^*|_{p_i}/p_i \right\rfloor$ для всех $i = \overline{1, n-1}$, где $N = \lceil \log_2(-n + nP_n) \rceil$ и $P_i^* = P_n/p_i$ для всех $i = \overline{1, n-1}$.

Output: $X > Y$-'10', $X < Y$-'01', $X = Y$ - '00'.

1. **For** $i \coloneqq 1$ **to** $n-1$ **do:**
1.1. $a_i \coloneqq |x_i - x_n|_{p_i}$; \\Parallel processing
1.2. $b_i \coloneqq |y_i - y_n|_{p_i}$; \\Parallel processing
2. **For** $i \coloneqq 1$ **to** $n-1$ **do:**
2.1. $a_i \coloneqq |a_i \cdot I_i|_{p_i}$; \\ Parallel processing
2.2. $b_i \coloneqq |b_i \cdot I_i|_{p_i}$; \\Parallel processing
3. $S_A = 0$; $S_B = 0$;
4. **For** $i \coloneqq 1$ **to** $n-1$ **do:**
4.1. $S_A = \left|S_A + \overline{k_\iota} \cdot a_i\right|_{2^N}$;
4.2. $S_B = \left|S_B + \overline{k_\iota} \cdot b_i\right|_{2^N}$;
5. IF $S_A > S_B$ **then return** '10'
6. **IF** $S_A < S_B$ **then return** '01'
7. **IF** $a_n > b_n$ **then return** '10'
8. **IF** $a_n < b_n$ **then return** '01'
9. **return** '01'

End.

Количество операций, необходимых для получения результата у данного алгоритма равно: умножений –$4n$, вычитаний – $2n$, сложений – n.

В таблице 1 представлены свойства методов вычисления позиционной характеристики. Предложенный метод позволяет уменьшить размер операндов по сравнению с алгоритмами из работ (Chervyakov et al., 2017[17], Van, 1985 [23]).

Табл. 1. Свойства алгоритмов сравнения чисел
Table 1. Properties of number comparison methods

Метод		$\lceil\cdot\rceil$	Количество операций '×'	Размер модуля	Вид модуля
КТО (Omondi, 2007)			$4n$	$\lfloor n \cdot \log_2 p_n \rfloor$	P
Диагональная функция (Pirlo, 1993)			$2n$	$\lfloor (n-1) \cdot \log_2 p_n + \log_2 n \rfloor$	SQ
ОПСС (Isupov, 2016)			$n \cdot \frac{n-1}{2}$	$\lceil \log_2 p_n \rceil$	p_i
Приближенный метод, (Van, 1985)	$\lvert P\rvert_2 = 1$	n	$2n$	$\lceil \log_2(Pn) \rceil$	2^N
Приближенный метод, (Chervyakov, 2017)			$2n$	$\lceil \log_2(P\rho) \rceil$	2^N
Наш метод			$2n$	$\lceil \log_2(-n + n \cdot P) \rceil$	2^N
Приближенный метод, (Van, 1985)	$\lvert P\rvert_2$	n	$2n$	$\lceil \log_2(Pn) \rceil - 1$	2^N

Приближенный метод, (Chervyakov, 2017)	$= 0$		$2n$	$\lceil \log_2(P\rho) \rceil - 1$	2^N
Наш метод			$4n$	$\lceil \log_2(-n + n \cdot P_n) \rceil$	2^N

8. Заключение

В статье рассмотрены методы сравнения чисел, представленных в СОК, что особенно важно в задачах цифровой обработки сигналов.

Из табл. 1 видно, что самым быстрым является предложенный модифицированный приближенный метод. Худший результат показал алгоритм, основанный на ОПСС.

Оставшиеся методы показали схожие результаты и их применение зависит непосредственно от решаемой задачи. Диагональная функция требует нахождения остатка по меньшему модулю, однако в случае равенства значений диагональных функций требуется дополнительное уточнение, что занимает дополнительное время.

Список литературы/References

[1]. Chang C.H., Molahosseini A.S., Zarandi A.A.E., Tay T.F. Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications. IEEE circuits and systems magazine, vol. 15? № 4, 2015, pp. 26-44.

[2]. Chervyakov N., Babenko M., Tchernykh A., Kucherov N., Miranda-López V., Cortés-Mendoza J. M. AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security. Future Generation Computer Systems, vol. 92, 2019, pp. 1080-1092.

[3]. Sousa L., Antao S., Martins P. Combining residue arithmetic to design efficient cryptographic circuits and systems. IEEE Circuits and Systems Magazine, vol. 16, № 4, 2016, pp. 6-32.

[4]. Chervyakov N.I., Lyakhov P.A., Babenko M. Digital filtering of images in a residue number system using finite-field wavelets. Automatic Control and Computer Sciences, vol. 48, № 3, 2014, pp. 180-189.

[5]. Ye R., Boukerche A., Wang H., Zhou X., Yan B. RESIDENT: a reliable residue number system-based data transmission mechanism for wireless sensor networks. Wireless Networks, vol. 24, № 2, 2018, pp. 597-610.

[6]. Tchernykh A., Schwiegelsohn U., Talbi E. G., Babenko M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science, 2016 (in Press), DOI: 10.1016/j.jocs.2016.11.011.

[7]. Miranda-López V., Tchernykh A., Cortés-Mendoza J.M., Babenko M., Radchenko G., Nesmachnow S., Du Z. Experimental Analysis of Secret Sharing Schemes for Cloud Storage Based on RNS. In Proc. of the Latin American High Performance Computing Conference, 2017, pp. 370-383.

[8]. Tchernykh A., Babenko M., Chervyakov N., Cortés-Mendoza J. M., Kucherov N., Miranda-López V., Deryabin M., Dvoryaninova I., Radchenko G. Towards mitigating uncertainty of data security breaches and collusion in cloud computing. In Proc. of the 28th International Workshop on Database and Expert Systems Applications (DEXA), 2017, pp. 137-141.

[9]. Babenko M., Chervyakov N., Tchernykh A., Kucherov N., Shabalina M., Vashchenko I., Radchenko G., & Murga D. Unfairness correction in P2P grids based on residue number system of a special form. In Proc. of the 28th International Workshop on Database and Expert Systems Applications (DEXA), 2017, pp. 147-151.

[10]. Szabo N.S., Tanaka R.I. Residue arithmetic and its applications to computer technology. N.Y., McGraw-Hill, 1967, 236 p.

[11]. Bi S., Gross W.J. The mixed-radix Chinese remainder theorem and its applications to residue comparison. IEEE Transactions on Computers, vol. 57. № 12, 2008, pp. 1624-1632.

[12]. Wang Y. Residue-to-binary converters based on new Chinese remainder theorems. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, vol. 47, № 3, 2000, pp. 197-205.

[13]. Dimauro G., Impedovo S., Pirlo G. A new technique for fast number comparison in the residue number system. IEEE transactions on computers, vol. 42, № 5, 1993, pp. 608-612.

[14]. Burgess N. Scaling an RNS number using the core function. In Proc. of the 16th IEEE Symposium on Computer Arithmetic, 2003. pp. 262-269.

[15]. Dimauro G., Impedovo S., Modugno R., Pirlo G., Stefanelli R. Residue-to-binary conversion by the" quotient function". IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing. vol. 50. № 8, 2003, pp. 488-493.
[16]. Pirlo G., Impedovo D. A new class of monotone functions of the residue number system. International Journal of Mathematical Models and Methods in Applied Sciences, vol. 7. № 9, 2013, pp. 803-809.
[17]. Chervyakov N.I., Molahosseini A.S., Lyakhov P.A., Babenko M.G., Deryabin M.A. Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem. International Journal of Computer Mathematics, vol. 94. № 9, 2017, pp.1833-1849.
[18]. Patronik P., Piestrak S.J. Design of Reverse Converters for General RNS Moduli Sets $\{2^k, 2^n-1, 2^n+1, 2^{n+1}-1\}$ and $\{2^k, 2^n-1, 2^n+1, 2^{n-1}-1\}$ (n even). IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 61, № 6, 2014, pp.1687-1700.
[19]. Phatak D.S., Houston S.D. New distributed algorithms for fast sign detection in residue number systems (RNS). Journal of Parallel and Distributed Computing, vol. 97, issue C, 2016, pp. 78-95.
[20]. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М., Советское радио, 1968, 440 с. / Akushsky I. Ya., Yuditsky D. I. Computer arithmetic in residual classes. Moscow, Soviet Radio, 1968, 440 p. (in Russian).
[21]. Omondi A.R., Premkumar B. Residue number systems: theory and implementation. L., Imperial College Press, 2007, 296 p.
[22]. Isupov K. An Algorithm for Magnitude Comparison in RNS based on Mixed-Radix Conversion II. International Journal of Computer Applications, vol. 141, № 5, 2016.
[23]. Van Vu T. Efficient implementations of the Chinese remainder theorem for sign detection and residue decoding. IEEE Transactions on Computers, vol. 100, № 7, 1985, pp. 646-651.
[24]. Mohan P.A. RNS to binary conversion using diagonal function and Pirlo and Impedovo monotonic function. Circuits, Systems, and Signal Processing, vol. 35, № 3, 2016, pp. 1063-1076.

Информация об авторах / Information about authors

Михаил Григорьевич БАБЕНКО окончил Ставропольский государственный университет в 2007 году. Защитил кандидатскую диссертацию в 2011 г. Преподаватель кафедры прикладной математики и математического моделирования Северо-Кавказского федерального университета. Сфера научных интересов: алгебраические структуры в полях Галуа, модулярная арифметика, нейрокомпьютерные технологии, цифровая обработка сигналов, криптографические методы защиты информации.

Mikhail Grigorievitch BABENKO graduated from Stavropol State University in 2007. He defended his thesis in 2011. Currently he is a lecturer of the Department of Applied Mathematics and Mathematical Modeling of the North Caucasus Federal University. Research interests: Algebraic structures in the Galois fields, modular arithmetic, neurocomputer technologies, digital signal processing, cryptographic methods for protecting information.

Андрей Николаевич ЧЕРНЫХ получил степень кандидата наук в Институте точной механики и вычислительной техники РАН. В настоящее время он является профессором Центра научных исследований и высшего образования в Энсенаде, Нижняя Калифорния, Мексика. В научном плане его интересуют многоцелевая оптимизация распределения ресурсов в облачной среде, проблемы безопасности, планирования, эвристики и метаэвристики, энергосберегающие алгоритмы, интернет вещей и т.д.

Andrei TCHERNYKH received his PhD degree at the Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences. Now he is holding a full professor position in computer science at CICESE Research Center, Ensenada, Baja California, Mexico. He is interesting in grid and cloud research addressing multi-objective resource optimization, both, theoretical and experimental, security, uncertainty, scheduling, heuristics and meta-heuristics, adaptive resource allocation, energy-aware algorithms and Internet of Things.

Николай Иванович ЧЕРВЯКОВ – доктор технических наук, профессор, заведующий кафедрой прикладной математики и информатики Северо-Кавказского федерального

университета с 2004 года. Сфера научных интересов: алгебраические структуры в полях Галуа, модулярная арифметика, нейрокомпьютерные технологии, цифровая обработка сигналов, криптографические методы защиты информации.

Nikolay Ivanovitch CHERVYAKOV – Doctor of Technical Sciences, Professor, Head of the Department of Applied Mathematics and Computer Science of the North Caucasus Federal University since 2004. Research interests: algebraic structures in the Galois fields, modular arithmetic, neurocomputer technologies, digital signal processing, cryptographic methods for protecting information.

Виктор Андреевич КУЧУКОВ является специалистом отдела научно-технической информации, наукометрии и экспортного контроля Управления науки и технологий Северо-Кавказского федерального университета. Его научные интересы включают распознавание образов, системы остаточных классов.

Viktor Andreevich KUCHUKOV is a specialist of the department of scientific and technical information, scientometrics and export control of the Department of Science and Technology of the North Caucasus Federal University. His research interests include pattern recognition, residual class systems.

Ванесса МИРАНДА-ЛОПЕС получила степень бакалавра в области электроники в Технологическом институте Соноры, Мексика в 2006 году и степень магистра в области компьютерных наук в исследовательском центре CICESE в 2010 году. Ее интересы включают облачные вычисления, сетевое планирование, большие данные, безопасность и электронный дизайн.

Vanessa MIRANDA-LÓPEZ received a Bachelor degree in electronics engineering from Technological Institute of Sonora, Mexico in 2006, and Master degree in computer sciences from CICESE Research Center in 2010. Her interests include cloud computing, grid scheduling, big data, security and electronic design.

Рауль РИВЕРА РОДРИГЕС получил степень доктора философии в Автономном университете Нижней Калифорнии, Британская Колумбия, Мексика. В настоящее время он является директором отделения телематики в исследовательском центре CICESE, B.C., Мексика. Научные интересы включают сети связи для HPC и BigData.

Raúl RIVERA RODRÍGUEZ obtained a PhD degree from Autonomous University of Baja California, B.C., Mexico. Currently he is a Director of the Telematics Division at CICESE Research Center, B.C., Mexico. Research interests include communications networks for HPC and BigData.

Чжихуэй ДУ получил степень PhD в области компьютерных наук и технологий в Пекинском университете, КНР в 1998 г. В настоящее время он работает доцентом на факультете Компьютерных наук и технологий университета Цинхуа, КНР. В число научных интересов входят параллельное программирование, высокопроизводительные / облачные / энергосберегающие вычисления и анализ больших данных.

Zhihui DU received the degree of PhD in Computer Science & Technology from Peking University, China in 1998. Currently he is the associate professor at the Department of Computer Science and Technology of Tsinghua University, China. His research interests include parallel computing, high performance/cloud/energy efficient computing, and Big Data analysis.