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]).

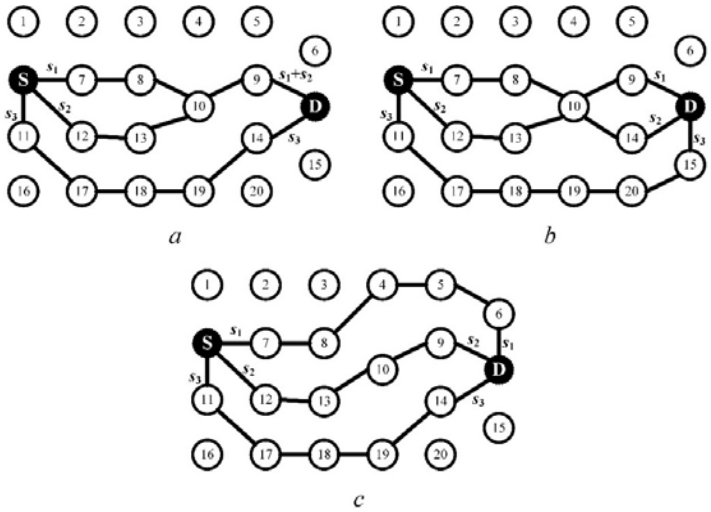

Рис. 1. Различные методы многопутевой маршрутизации: a – общий случай, b – с разделением по маршрутам, c – с разделением по узлам.
Fig. 1. Different types of Multi-Path Routing: a – general case, b – Link-Disjoint, c – Node-Disjoint.

На рис. 1c 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 (ССРС, 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.

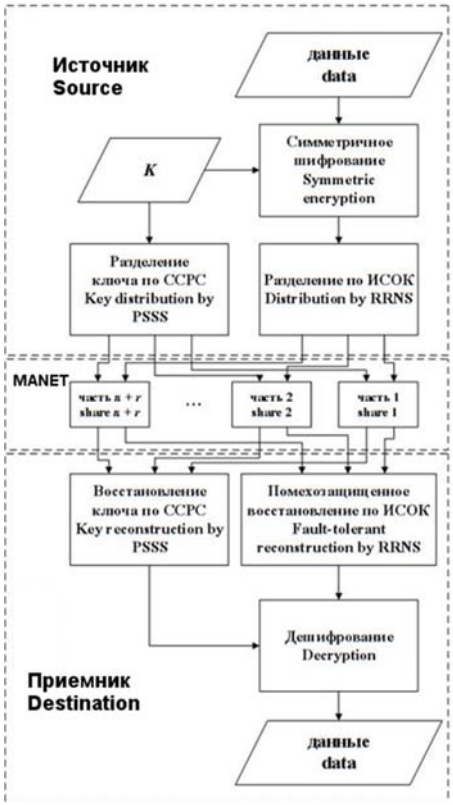

Рис. 2. Обобщенная схема безопасной и надежной передачи данных в MANET на основе вычислительно стойкой схемы разделения секрета
Fig. 2. Generalized scheme of the secure and reliable data transmission over MANET based on computationally secure secret sharing scheme

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).

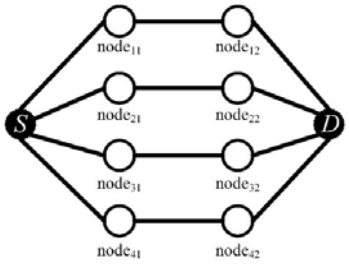

Рис. 3. Пример маршрутизации с 4 маршрутами без пересечения по узлам и 8 промежуточными узлами (по 2 на каждом из маршрутов)
Fig. 3. Routing example for 4 node-disjoint routes and 8 intermediary nodes (2 per each route)

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}
	$P = 0.672352030$		$P = 0.976473630$		$P = 0.9999689481$	

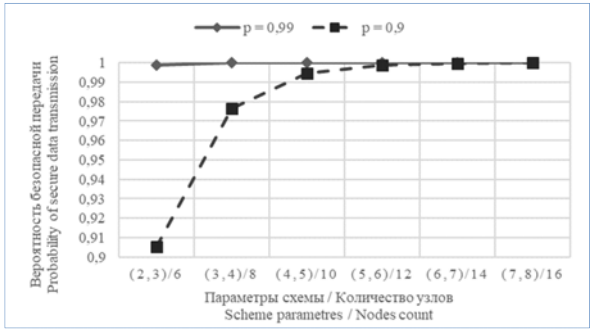

Рис. 4. Вероятность безопасной передачи данных при различном количестве маршрутов и общем количестве узлов
Fig. 4. The probability of secure data transmission with a different number of routes and the total number of nodes

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.