DOI: 10.15514/ISPRAS-2024-36(3)-19

A Method of Protocol-Aware Multi-tone Sweep Jamming

H. Grigoryan, ORCID: 0009-0005-1042-7379 <*heghinegrigoryan2111@gmail.com*>
L. Kirakosyan, ORCID: 0009-0003-3034-0313 <*kirakosyan.lilia@student.rau.am*>
S. Sargsyan, ORCID: 0000-0002-8831-4965 <*sevak.sargsyan@rau.am*>

Russian-Armenian University,
123, Hovsep Emin st., Yerevan, 0051, Armenia.

Abstract. This article extensively reviews radio wave jamming methods, focusing on their application to disrupt drone signals. It explores the evolution of these techniques, from basic noise-based methods to more advanced systems that target specific communication protocols. The article analyzes key jamming types such as barrage, tone, sweep, and protocol-aware jamming for their mechanisms and efficacy. Each type is discussed in terms of its operational principles, benefits, and limitations, offering a comprehensive understanding of the impact these methods have on drone communications. The review also discusses contemporary counter-jamming strategies, such as frequency hopping, which are increasingly being used to enhance the resilience of drone systems against interference. In addition, the article emphasizes the significant role of software-defined radio (SDR) systems in developing and improving effective drone communication jamming solutions. The flexibility of SDR technology allows for the dynamic adaptation of jamming techniques, making it an important area of research. We aim to improve understanding of SDR-based jamming methods and their practical application by combining theoretical studies with hands-on experiments.

Keywords: jamming; frequency hopping spread spectrum; software-defined radio; unmanned aerial vehicle.

For citation: Grigoryan H., Kirakosyan L., Sargsyan S. A Method of Protocol-Aware Multi-tone Sweep Jamming, *Trudy ISP RAN/Proc. ISP RAS*, vol. 36, issue 3, 2024. pp. 273-282. DOI: 10.15514/ISPRAS-2024-36(3)-19.

Acknowledgements. This work was supported by the Science Committee of RA (Research projects № 23AA-1B009).

Метод подавления сигналов с помощью движущихся многотональных помех с учётом протокола

Е. Григорян, ORCID: 0009-0005-1042-7379 <*heghinegrigoryan2111@gmail.com*>
Л. Киракосян, ORCID: 0009-0003-3034-0313 <*kirakosyan.lilia@student.rau.am*>
С. Саргсян, ORCID: 0000-0002-8831-4965 <*sevak.sargsyan@rau.am*>

Российско-Армянский университет,
123, ул. Овсепа Эмина, Ереван, 0051, Армения.

Аннотация. Подробно рассматриваются методы радиопомех, с акцентом на их применение для глушения сигналов беспилотных аппаратов. Рассматривается эволюция этих методов: от простых подходов на основе анализа шумов до более продвинутых систем, нацеленных на определенные протоколы взаимодействия. Анализируются ключевые типы помех, такие как заградительные, тональные, сканирующие и протоколо-ориентированные помехи, с точки зрения их механизмов и эффективности. Каждый тип обсуждается с учетом принципов его работы, преимуществ и ограничений, что позволяет получить всестороннее понимание влияния этих методов на взаимосвязи дронов. Также обсуждаются современные стратегии противодействия помехам, такие как скачкообразная перестройка частоты, которые все чаще используются для повышения устойчивости систем дронов к помехам. Кроме того, в статье подчеркивается значительная роль систем радиосвязи с программируемыми параметрами в разработке и улучшении эффективных решений для подавления связи дронов. Гибкость технологий программируемой радиосвязи позволяет динамически адаптировать методы создания помех, что делает их важной областью исследований. Целью работы является стремление улучшить понимание программных методов подавления помех и их практического применения, сочетая теоретические исследования с практическими экспериментами.

Ключевые слова: Глушение радиосигналов; частотно-скачкообразный расширенный спектр (FHSS); радиосвязь с программируемыми параметрами (SDR); беспилотные летательные аппараты (UAV).

Для цитирования Григорян Е., Киракосян Л., Саргсян С. Метод подавления сигналов с помощью движущихся многотональных помех с учётом протокола. Труды ИСП РАН, том 36, вып. 3, 2024 г., стр. 273–282 (на английском языке). DOI: 10.15514/ISPRAS–2024–36(3)–19.

Благодарности: Работа поддержана Комитетом по науке Республики Армения (Исследовательские проекты № 23AA-1B009).

1. Introduction

In today's world, drones have become very common and affordable. They are used in many areas, such as entertainment, photography, delivery services, and military operations. However, as the number of drones increases, so does the potential for their misuse. People can use drones to break laws, invade private property, or even conduct harmful activities.

One significant countermeasure against such misuse is the deployment of radio wave jammers, which intentionally transmit interference to disrupt communications between drones and their controllers. This technique, rooted in electronic warfare, has undergone substantial advancements. Jamming initially relied on simple methods to disrupt communication channels. However, modern methods have evolved to more sophisticated approaches, targeting specific frequencies and utilizing advanced signal processing algorithms to improve efficiency and effectiveness.

Alongside the development of jamming techniques, there are anti-jamming systems like Frequency Hopping Spread Spectrum (FHSS) [1]. FHSS is a spread spectrum technique where the carrier frequency shifts randomly over time within a specified bandwidth. The modulation frequency varies in a pseudorandom pattern based on a pseudo-noise (PN) sequence while maintaining a central frequency within a fixed bandwidth. Many common drones use FHSS to ensure they stay connected.

In this article, we describe the types of jamming that can effectively disrupt the communication of commercially available, off-the-shelf drones and controllers, such as those widely sold. Many of these drones and their controllers use Orthogonal Frequency Division Multiplexing (OFDM) modulation [2]. OFDM is a digital modulation technique that divides a signal into multiple closely spaced subcarriers, each carrying a separate data stream. This approach enables efficient use of available bandwidth and minimizes interference between subcarriers due to their orthogonality.

We used the HackRF One Software Defined Radio (SDR) [3] system for testing jamming methods [4]. The HackRF One is a versatile SDR platform that can transmit and receive radio signals from 1 MHz to 6 GHz, making it ideal for testing and developing wireless communication systems.

2. Jamming Techniques

Jamming in wireless communications means disrupting wireless signals by increasing the noise level at the receiver's end. Unlike regular network interference, which happens accidentally, jamming involves intentionally using wireless signals to interrupt communications.

Several jamming strategies can be used against specific targets, each with advantages and disadvantages. This paper will review the most common and fundamental methods and methods derived from these fundamental strategies [5]. Each type of jamming strategy may be optimal for specific target scenarios.

2.1 Barrage Jamming

The first method is a barrage, which disrupts wireless communications by sending jamming signals across a wide range of frequencies simultaneously [6]. This approach aims to simultaneously interfere with multiple communication channels by flooding the target frequencies with noise. As a result, it becomes challenging for users to communicate, as the jamming masks their signals. By covering a large frequency spectrum, barrage jamming increases the chances of interrupting different types of wireless communications within the affected area, significantly impacting their effectiveness.The barrage jamming method generates Gaussian noise as interference that spreads across the radio frequency spectrum.

This concept of noise affecting channel capacity, particularly under Gaussian noise conditions, was first examined by Shannon in 1948 [7]. Shannon's theory outlines the maximum data rate that a channel can sustain while maintaining a low error rate. If a digital signal is transmitted through a channel at a bit rate higher than the channel's capacity, it will inevitably result in errors in the received signal. The maximum capacity of a channel, when subjected to such noise, is defined by

$$C = W_{ss} log_2 \left(1 + \frac{R}{P_T}\right)$$

The variable W_{ss} represents the bandwidth of the signal, R denotes the average power of the signal, and P_T stands for the total average noise present. When Gaussian noise is added to the channel, the noise level increases, which reduces the Signal-to-Noise Ratio (SNR), lowering the channel capacity. The SNR is a measure used to quantify the level of a desired signal relative to the level of background noise [8]. It is typically calculated using the formula:

$$SNR\ (dB) = 10\ log_{10} \left(\frac{P_{Signal}}{P_{Noise}}\right)$$

Barrage interference increases the noise level in the receiver and directly affects the channel capacity of the communication system. The spectrum of barrage jamming is illustrated in Fig. 1 (a).

The barrage jamming method applies to all anti-jam communication systems because it can cover a large bandwidth, effectively disrupting communication between the drone and its controller. However, the disadvantage of barrage jamming is its high energy consumption, as more energy is required to cover a large bandwidth.

2.2 Tone Jamming

In tone jamming, tones are strategically placed within the spectrum. The effectiveness of the jamming depends on the number and placement of these tones [6]. Single-tone jamming uses a single tone at a key location. When tones are strategically placed, they can effectively suppress target signals. The spectrum of tone jamming is illustrated in Fig. 1 (b).

(a) Barrage *(b) Tone* *(c) Sweep* *(d) Protocol-aware*

Fig. 1. Jamming Types

The effectiveness of tone jamming largely depends on the number of tones used and their distribution. Research has shown that single-tone interference is ineffective against FHSS systems [9]. Therefore, it is more practical to use alternative methods based on fundamental modes to disrupt these systems effectively.

One promising approach to improve jamming effectiveness is to leverage the phenomenon of intermodulation [10]. This happens when two or more signals come together and interact with nonlinear parts in the input circuits of the receiving system. By using multiple tones, the effect of intermodulation can be achieved. This allows jamming techniques to create additional tone signals that disrupt communication, making it a valuable strategy for targeting FHSS systems [11]. This method enables the system to cover a wider spectrum of signals with increased strength while using less energy to cover a broad frequency range.

2.3 Sweep Jamming

Swept jamming involves a relatively narrowband signal, potentially as narrow as a single tone, that is swept or scanned over time across the frequency band of interest [6]. At any given moment, the jammer is focused on a specific frequency, and only a narrow region around this frequency is jammed Fig. 1 (c). However, due to the sweeping motion of the signal, a broad range of frequencies can be effectively jammed within a short period. This technique can also avoid frequency bands that should not be disrupted, allowing for a more focused and effective jamming strategy.

Swept jamming can also be implemented using a multi-tone signal [6]. Multi-tone continuous motion jamming is a sophisticated method that utilizes multiple tones, each changing their frequencies in a predetermined sequence. This method is designed to create interference over a wide frequency range by periodically changing the frequency of the jamming signal. The multi-tone approach enhances the effectiveness of the jamming operation by covering more frequencies simultaneously and reducing the likelihood of the target system adapting to a single-tone jammer.

2.4 Protocol-aware Jamming

Protocol-aware jamming is a technique that interferes with a signal by using the same protocol parameters as the target signal, Fig. 1 (d) such as modulation type and bandwidth [12]. This method does not disrupt other systems that operate on the same frequency. To implement this method effectively, information about the signal is crucial parameters such as modulation type, data rate, and channel bandwidth.

Studies have predominantly explored the feasibility of protocol-aware jamming in IEEE 802.11-based wireless local area network communication systems [13]. It has been established that this form of jamming can be highly effective with minimal energy requirements and a low probability of detection. The low probability of detection is primarily due to its ability to blend in with legitimate traffic. By mimicking the same protocol parameters as the target signal, this method generates interference that is difficult to distinguish from regular network activity. As a result, the jamming

signals can operate under the radar, making it challenging for network security systems to identify and respond to the interference.

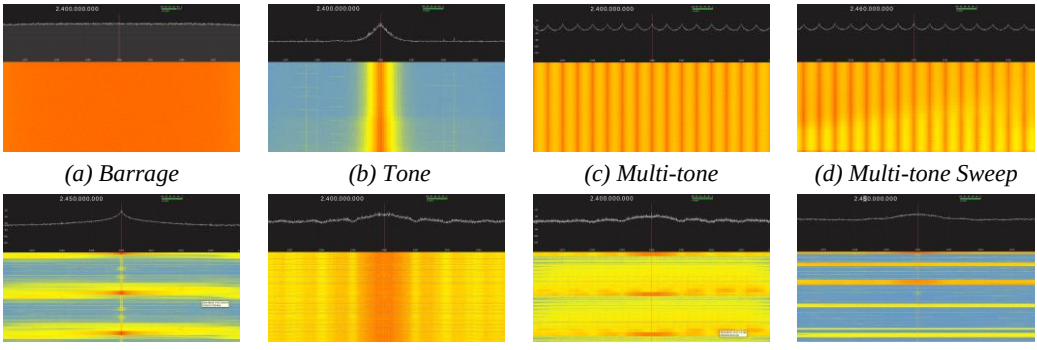
3. Protocol-aware multi-tone sweep jamming

We propose a protocol-aware multi-tone sweep jamming method aimed at disrupting specific target signals. This method combines protocol-aware jamming with multi-tone sweep jamming to enhance effectiveness and efficiency. Multiple tones create interference through intermodulation effects, generating signals that disrupt communication. Additionally, the jamming signal is swept across a range of frequencies, ensuring that a broad spectrum is covered over time and increasing the likelihood of disrupting the target signal. This approach ensures high efficiency by effectively targeting communication with minimal energy requirements, and its low probability of detection enhances its stealthiness. The sweeping motion across frequencies further broadens the coverage, making protocol-aware multi-tone sweep jamming a powerful technique for disrupting target communications.

3.1 GnuRadio Based Implementation

We implemented the mentioned jamming methods using GnuRadio [15]. GnuRadio is a universal toolkit that offers pre-built blocks to facilitate the creation of custom flow graphs, which are essential for designing and testing various signal processing applications. Additionally, GnuRadio supports the development of custom blocks, allowing for greater flexibility and customization to meet specific requirements.

The barrage jamming was implemented using basic blocks for Gaussian noise generation and signal transmission. The generated signal has a 20 MHz bandwidth and an adjustable central frequency, spectrogram illustrated in Fig. 2 (a).



(a) Barrage *(b) Tone* *(c) Multi-tone* *(d) Multi-tone Sweep*

(e) Sweep *(f) OFDM* *(g) OFDM Sweep* *(h) MT OFDM Sweep*

Fig. 2. Spectrograms of Jamming methods

For the tone jamming implementation, we utilized a block capable of generating waves in either sinusoidal or cosinusoidal form and a signal transmission block with an adjustable central frequency, as shown in Fig. 2 (b). A multi-tone jamming system was implemented using multiple sources to generate three distinct tones, each at a different frequency. By generating signals across multiple frequency channels simultaneously, it creates interference over a broader spectrum.For the experiments, we generated three tones with a separation of 5 MHz, specifically at frequencies of 2410 MHz, 2415 MHz, and 2420 MHz. As shown in Fig. 2 (b), (c), the spectrum exhibits notable changes when a single tone is generated compared to when three.

We used the “Probe Signal” and “Function Probe” blocks to implement the sweep method [16]. Since GNURadio allows you to create your blocks in Python, we developed a custom block for the continuous movement of the signal. The custom module also regulates the signal's step size and range by setting variables for the start and end frequencies.

To implement a protocol-aware method, we used parameters obtained during spectrum scanning. We developed a specialized module capable of extracting OFDM parameters from target signals, such as those emitted by drones. This module extracted key characteristics of the OFDM signal, including the number of subcarriers, the cyclic prefix length, the number of occupied carriers, and the placement of pilot symbols.

Once these parameters are extracted, the generated tone signal is processed through the OFDM Transmitter block. This block is responsible for modulating the signal by the extracted parameters.

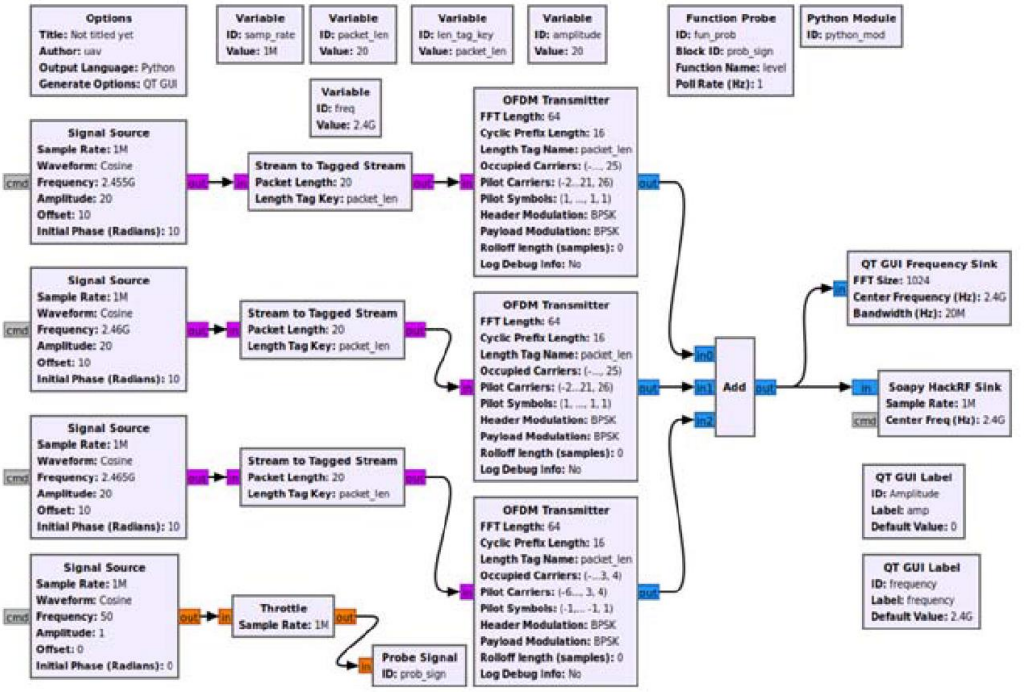


Fig. 3. GNURadio Flow graph

The implementation of the protocol-aware multi-tone sweep jamming method involves integrating sweep, multi-tone, and protocol-aware jamming techniques. Using the GnuRadio toolkit, we created a custom flow graph that combines these methods into a cohesive jamming strategy. We do spectrum analysis to identify and extract the OFDM parameters from the target signal; these parameters are then used to construct an OFDM signal.

Next, based on the multi-tone jamming method, we generate multiple OFDM signals spaced apart at predetermined intervals. These signals are strategically chosen to create intermodulation effects, significantly disrupting the communication signal. We then combine this with the sweep jamming technique. This module enables the multi-tone OFDM signal to be swept across a wide range of frequencies over time. The GNURadio flow graph and spectrogram are illustrated in Fig. 3 and Fig. 2 (h).

4. Experiments and Results

All described jamming methods were tested using the programs we implemented in GNU Radio.

We assembled a system for the experiments consisting of a HackRF One, an amplifier, a preamplifier, a Yagi antenna, and a computer. A Yagi antenna operates at 2.4 GHz.

The jamming target was an FPV drone with an SIYI FT24 remote control and an SIYI mini receiver [17]. The drone also had telemetry to maintain communication with the operator. The experiments

were conducted both in the field and in the laboratory. In the laboratory, the distance between the drone and the remote controller was 15 meters, and between the jamming system and the drone was 2 meters. During the field experiments, the distance between the remote control and the jammer was approximately 1 km, while the distance between the drone and the jammer ranged from 20 to 30 meters.

We also considered energy consumption when comparing methods. The measurements were taken at 10-minute intervals for each type of jamming, as shown in Table 1.

We analyzed the RSSI (Received Signal Strength Indicator) parameter to evaluate the results [18]. RSSI measures the strength of the signal received by the receiver and is typically used to evaluate the quality of communication between the transmitter and receiver. A high RSSI value indicates a strong received signal, whereas a low value indicates a weak signal. RSSI values were recorded and presented in Table 2 during the experiments.

Following the experiments, some parameters from the drone log files were used for analysis. Drone log files contain information about various aspects of the drone's flight and operation. We focused on radio parameters such as RSSI and noise for our purposes. Noise analysis was necessary to evaluate the system's effectiveness using another method.

One key parameter is the SNR. Since the purpose of the jamming system is to increase the noise in the target receiver, the SNR should be as low as possible to ensure the effective operation of such a system.

From Table 3, it can be concluded that the data obtained in laboratory conditions (at short distances) demonstrate the effectiveness of the jamming algorithms. However, in field conditions (at long distances), these same algorithms are practically ineffective, likely due to the limited power of the system.

Table 1. Voltage loss for different jamming methods

Jamming Method	Voltage loss (volt)
Barrage	0.08
Tone	0.005
Multi-tone	0.09
Sweep	0.07
Multi-tone Sweep	0.12
OFDM Sweep	0.06
Multi-tone OFDM Sweep	0.07

Table 2. The value of the RSSI for different types of jamming

Jamming Type	Working Frequency (GHz)	RSSI value (%)	
		Laboratory	Field
Barrage	2.45	25	70
Tone	2.45	75	97
Multi-tone	2.445, 2.450, 2.455	14	73
Sweep	2.4–2.5	20	75
Multi-tone Sweep	2.445, 2.450, 2.455	10	65
OFDM Sweep	2.4–2.5	8	70
Multi-tone OFDM Sweep	2.455, 2.460, 2.465	3	50

Table 3. The value of the SNR for different types of jamming

Jamming Type	SNR (dB)	
	Laboratory	Field
Barrage	-29	48
Tone	55	82
Multi-tone	-34	51

Jamming Type	SNR (dB)	
	Laboratory	Field
Sweep	-12	61
Multi-tone Sweep	-43	41
OFDM Sweep	-40	45
Multi-tone OFDM Sweep	-41	31

5. Conclusion

In this paper, we implemented and tested basic jamming methods and developed a new method to jam the radio signals controlling drones. Our experiments revealed that the system performs exceptionally well in laboratory settings but is less effective in real-world conditions, primarily due to the limited power of our devices. Despite these power constraints, our new jamming methods significantly outperformed existing techniques. Future research could focus on enhancing the system's power efficiency and adapting it for a wide range of real-world applications.

References

[1]. Adamy D. EW 101: A first course in electronic warfare. Artech House, Boston, 2001, 352 p.
[2]. Litwin L., Pugel M. The principles of OFDM. RF signal processing, 2001, vol. 2, pp. 30—48.
[3]. Great Scott Gadgets. HackRF One. Available at: https://greatscottgadgets.com/hackrf/one/ (accessed 02.08.2024).
[4]. Reis A. L. G., de Oliveira R. E., Bego A. S., Teixeira M. C. Introduction to the software-defined radio approach. IEEE Latin America Transactions, 2012, vol. 10, no. 1, pp. 1156—1161.
[5]. Grover K., Lim A., Yang Q. Jamming and anti-jamming techniques in wireless networks: a survey. International Journal of Ad Hoc and Ubiquitous Computing, 2014, vol. 17, no. 4, pp. 197—215.
[6]. Poisel R. Modern communications jamming principles and techniques. Artech House, Boston, 2011, 508 p.
[7]. Shannon C. E. A mathematical theory of communication. The Bell System Technical Journal, 1948, vol. 27, no. 3, pp. 379—423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.
[8]. Johnson D. H. Signal-to-noise ratio. Scholarpedia, 2006, vol. 1, no. 12, p. 2088.
[9]. Pärlin K. Jamming of spread spectrum communications used in UAV remote control systems. Tallinn University of Technology, School of Information Technologies, Thomas Johann Seebeck Department of Electronics, 2017.
[10]. Джуринский К. Интермодуляции в радиочастотных соединителях для мобильной и сотовой связи. Компоненты и технологии, 2010, no. 107, pp. 26—30.
[11]. Матюшков А.Л., Сенюк В.О., Ступин К.В. Алгоритм радиоэлектронного подавления радиостанций с псевдослучайной перестройкой рабочей частоты. Доклады Белорусского государственного университета информатики и радиоэлектроники, 2019, no. 1(119), pp. 5—10.
[12]. Brito A., Sebastião P., Souto N. Jamming for Unauthorized UAV Operations-Communications Link. 2019 International Young Engineers Forum (YEF-ECE), 2019, pp. 94—98. DOI: 10.1109/YEF-ECE.2019.8740828.
[13]. Hussain A., Hoque M. M., Shahriar N., Ahmed M. Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks. Journal of Communications and Networks, 2014, vol. 16, no. 4, pp. 397—406. DOI: 10.1109/JCN.2014.000069.
[14]. GNURadio. The Free and Open-Source Toolkit for Software Radio. Available at: https://www.gnuradio.org (accessed 02.08.2024).
[15]. GNURadio. Function Probe. Available at: https://wiki.gnuradio.org/index.php?title=Function_Probe (accessed 02.08.2024).
[16]. Siyi. FT24 User Manual. Version v1.1. Available at: https://siyi.biz/siyi_file/FT24/FT24_User_Manual_en_v1.1.pdf (accessed 02.08.2024).
[17]. Mohsin H., Abdulameer K., Khudhair Z. N. Study and performance analysis of received signal strength indicator (RSSI) in wireless communication systems. International Journal of Engineering and Technology, 2017, vol. 6, no. 1, pp. 195—200.

Информация об авторах / Information about authors

Егине ГРИГОРЯН получила степень бакалавра в области информатики и прикладной математики в Национальном Политехническом Университете Армении, Армения, в 2022 году. В 2024 году она получила степень магистра в области интеллектуальных систем и робототехники в Российско-Армянском Университете, Армения. Она также является исследователем в Центре Передовых Программных Технологий (CAST). Ее исследовательские интересы включают связи для БПЛА, системы беспроводной связи.

Heghine GRIGORYAN received her Bachelor's degree in Computer Science and Applied Mathematics from the National Polytechnic University of Armenia in 2022. She earned her Master's degree in Intelligent Systems and Robotics from the Russian-Armenian University in 2024. She is also a researcher at the Center for Advanced Software Technologies (CAST). Her research interests include UAV communications and wireless communication systems.

Лиалиа КИРАКОСЯН получила степень бакалавра в области информатики и прикладной математики в Российско-Армянском Университете в 2021 году. В 2023 году она получила степень магистра в области интеллектуальных систем и робототехники в Российско-Армянском Университете. В настоящее время она занимается аспирантурой по математическому и программному обеспечению вычислительных машин, комплексов и компьютерных сетей в Российско-Армянском Университете. Она также является исследователем в Центре Передовых Программных Технологий (CAST). Её исследовательские интересы включают БПЛА, системы радиосвязи, системы связи для БПЛА, программно-определяемые радиосистемы.

Lilia KIRAKOSYAN received her Bachelor's degree in Computer Science and Applied Mathematics from the Russian-Armenian University in 2021. In 2023, she earned her Master's degree in Intelligent Systems and Robotics from the Russian-Armenian University. She is currently pursuing a Ph.D. in Mathematical and Software Support for Computing Machines, Complexes, and Computer Networks at the Russian-Armenian University. She is also a researcher at the Center for Advanced Software Technologies (CAST). Her research interests include UAVs, radio communication systems, communication systems for UAVs, and software-defined radio systems.

Севак САРГСЯН получил степени бакалавра и магистра в области информатики и прикладной математики в Ереванском Государственном Университете, Армения, в 2010 и 2012 годах соответственно. Позже, в 2016 году, он получил степень кандидата физ.-мат. наук в области математического и программного обеспечения вычислительных машин, комплексов и компьютерных сетей в Институте системного программирования имени Иванникова Российской академии наук. В настоящее время он является заведующим кафедрой Системного Программирования в Российско-Армянском Университете, Армения. Его исследовательские интересы включают технологии компиляторов, безопасность программного обеспечения и тестирование программного обеспечения.

Sevak SARGSYAN received his B. Sci. and M. Sci. degrees in informatics and applied mathematics from Yerevan State University, Armenia, in 2010 and 2012, respectively. He later in 2016 obtained his Cand. Sci. (Phys.-Math.) degree in mathematical and software support for computing machines, complexes, and computer networks from the Ivannikov Institute for System Programming of the Russian Academy of Sciences. Presently he serves as the head of the system programming department at Russian-Armenian University, Armenia. His research interests include compiler technologies, software security, and software testing.