UDC 004.56 DOI: 10.20535/2411-2976.22025.48-54

PHYSICAL LAYER COMMUNICATION SECURITY IN 5G/6G NETWORKS OF INTELLIGENT TRANSPORT SYSTEMS BASED ON PROBABILISTIC CRYPTOGRAPHIC TRANSFORMATIONS

Viktor M. Gorytsky

Educational and Research Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Background. Ultra-Reliable Low Latency Communication (URLLC) as a service offered by fifth and sixth generation (5G/6G) wireless systems is a technological response to the needs of various mission-critical applications that require reliable data transmission with low latency. These applications also include Intelligent Transportation Systems services, which, among other things, provide connectivity and autonomous vehicle control. The combination of high reliability and low latency requirements in URLLC usage scenarios creates a security problem for URLLC data transmission that cannot be solved using conventional complex cryptographic methods based on a secret key. The article discusses in detail the approach to using physical layer security mechanisms (physical layer security - PLS) as a powerful alternative to classical cryptographic security methods for URLLC, and also proposes the application of the wire-tap channel concept in URLLC with an analysis of the efficiency that can be achieved for physical layer security.

Objective. The aim of the article is to provide an overview of information security solutions in URLLC usage scenarios, as well as to propose a constructive method for information protection for reliable data transmission with low latency without the use of cryptographic mechanisms based on a secret key.

Methods. Theoretical research in the field of the branch channel concept was used to create solutions that allow data protection with information-theoretic stability in URLLC usage scenarios for providing IoT, connected car and autonomous driving services.

Results. The article examines in detail the data security issues in ultra-reliable low latency communication (URLLC) as a service offered by fifth and sixth generation (5G/6G) wireless systems. It is determined that URLLC is a technological response to the needs of various critical applications that require reliable signal transmission with low latency, and among these applications are Intelligent Transportation Systems services, which, among other things, provide connectivity and autonomous vehicle control. It is shown that the combination of high reliability and low latency requirements in URLLC scenarios creates a security problem for URLLC data transmission that cannot be solved using conventional complex cryptographic methods based on a secret key. The feasibility of using physical layer security mechanisms (PLS) as a powerful alternative to classical cryptographic security methods for URLLC is substantiated. The approach to applying the concept of a wire-tap channel in URLLC is considered in detail, as well as the results that can be achieved for physical layer security, and the influence of code parameters for probabilistic cryptographic transformations in accordance with the concept of a wire-tap channel on PLS URLLC. Estimates of the effectiveness of PLS URLLC for finite block length codes are provided.

Conclusions. An effective way to ensure data security for ultra-reliable low-latency physical layer link (PLS URLLC) of fifth-generation 5G wireless systems in the field of connected cars and vehicles of 4-5 levels of automation can be approaches based on the concept of a tapped channel ("wire-tap channel").

Keywords: *IoT; IoT information security; ultra-reliable low-latency communication; intelligent transportation system; connected vehicles; autonomous vehicle security; physical layer protection; tapped channel concept; wire-tap channel.*

Introduction

Problem statement. The market for connected cars and vehicles with SAE J3016 Level 4-5 automation levels is rapidly evolving due to the advancement of network and telecommunications technologies. Among them, 5G technology stands out as a transformative force, and V2X communication plays a significant role in improving road safety and efficiency. 5G/6G technology is driving the connected car revolution due to its high speed (required for real-time communication between vehicles, infrastructure and cloud services, supporting various applications including autonomous driving and intelligent traffic management), low latency (reducing delays in data exchange, which is crucial for applications that require instant response, such as collision avoidance systems and real-time traffic updates), and reliable connectivity (providing stable and secure connectivity, which is vital to maintaining the integrity and security of the connected car ecosystem). As one of the most advanced network technologies available, 5G addresses the critical needs of connected

car applications, ensuring seamless integration and operation. However, the physical properties of the radio technologies applicable to 5G/6G pose a security issue that, if not addressed, calls into question the feasibility of using 5G for these purposes.

Task statement. Thus, the task is to comprehensively study the ways and mechanisms of information protection when using network technologies and telecommunications technologies based on 5G/6G for the needs of connected cars, as one of the security-critical examples of IoT, and to create recommendations for the selection of effective and acceptable data protection technologies. As a result, the ultimate goal of this task is to propose constructive approaches to solving security issues of the communication connection of cars to 5G-based networks.

Ultra-reliable low latency communication.

Ultra-reliable low latency communication (URLLC) is an innovative service offered by fifth-generation (5G) wireless systems. 5G technology introduces new services such as enhanced mobile broadband (eMBB), ultra-reliable low latency communication (URLLC), and massive machine-type communication (mMTC) to meet the growing demand for services to create intelligent applications.

URLLC enables various mission-critical applications by facilitating reliable low-latency signal transmission. URLLC is one of the promising new services offered by 5G. URLLC brings significant innovation to 5G, introducing qualitative differences from the previous generation of mobile services (4G, LTE), while expanding functionality and going beyond the scope of new-generation 5G applications. In addition, URLLC enables seamless connectivity to a vast number of low-power smart devices in Internet of Things (IoT) applications through transformative technologies that rely on real-time, low-latency, and highly reliable communication.

The application scope of Ultra-Reliable Low-Latency Communication (URLLC) is constantly growing and is becoming a cornerstone of cyber-physical systems. URLLC service is capable of providing high reliability (99.999%) and low latency ($\leq$ 1 ms) signal transmission to support a variety of mission-critical applications, such as: industrial automation (Industry 5.0), autonomous driving (Intelligent Transportation Systems), smart grid, haptic Internet, intelligent healthcare systems, etc.

Intelligent Transport Systems (ITS) and 5G URLLC

The introduction of URLLC has revolutionised current ITS applications such as autonomous driving, vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication: IoT enables data exchange in V2V (vehicle-to-vehicle), V2I (infrastructure-to-infrastructure), V2P (pedestrian-to-pedestrian), V2N (network-to-network) formats, supporting extreme quality of service requirements in high mobility environments.

Automotive connectivity has opened up new opportunities for improved road safety and efficient routing in autonomous driving with 5G services. V2X communication provides extraordinary ITS benefits by efficiently transmitting latency-sensitive data, multimedia streams and critical control information between vehicles, roadside units, sensor nodes and cellular base stations using 5G URLLC. This allows vehicle users to exchange real-time information about traffic congestion, road conditions, route data, location information, vehicle speed, breakdown status, and sensor data over a wireless environment using the 5G URLLC service. However, broadcasting this latency-sensitive control information over an open wireless environment is highly vulnerable to security attacks and eavesdropping. Therefore, maintaining the confidentiality and security of this information is vital to avoid unwanted accidents and security breaches.

Information Security Problem for URLLC

Thus, in addition to high data transmission reliability and low data transmission latency, ensuring data transmission security for URLLC is an important issue. This is because most of the critical 5G applications use URLLC service to transmit confidential and high-priority control information to improve operation efficiency. With the emergence of smart applications (including intelligent transportation systems, autonomous driving, etc.), the demand for URLLC service has increased many times.

To ensure strict quality of service (QoS) requirements, URLLC uses short packet signals of finite block length, tens to hundreds of bits, for data transmission, which greatly complicates (eliminates) the use of conventional complex cryptographic methods based on secret keys.

As the URLLC service scales to meet the exponential demand for the service, ensuring information security of critical short packet communication (SPC) in URLLC becomes crucial from the perspective of reliable and secure communication.

URLLC Information Security Issues

URLLC is an innovative class of 5G services. According to 5G standards, URLLC is a type of service that provides high signal transmission reliability, keeping the packet loss probability within 10−5 to 10−7 and faster response time with low communication latency (≤ 1 ms).

However, the model parameters for URLLC packets must consider a trade-off between latency (measured in terms of coding block length) and packet error probability (which indicates the reliability of data transmission), which ultimately requires that the packet size be short enough for URLLC. On the other hand, such a short packet transmission causes an inevitable non-zero decoding error, which degrades the reliability of signal transmission.

The conventional (original) wireless communication system (1G, 2G) was specifically designed for signals of infinite block length. Thus, the throughput becomes achievable for these systems while reducing the decoding error probability to zero. Meanwhile, the payload size of URLLC signals is small with a finite block length. Due to the finite block length, the usual bandwidth-based asymptotic analysis is not applicable to URLLC.

The problem of cryptographic approaches for URLLC security

Traditionally, the development of security enhancement schemes in a drone-free environment revolves around approaches based on information theory, and cryptographic methods are used to control the flow of information and establish security linking in dartless systems. However, the decision for URLLC may have some shortcomings, since they create strong savings and high additional costs for the merchandising at the least, maintain the additional processing time, and pay invoices. The alarm is suitable for signals with a larger voltage block. On the other hand, the end of the block, the non-zero reliability of decoding and the benefits of QoS URLLC create additional incentives for the development of security enhancement schemes. Therefore, to transmit the URLLC signal, low-complexity security schemes are used instead of foldable cryptographic methods. New approaches to security come from the fundamentals of information theory and focus on the security channel of radio broadcasting, and are called physical layer security (PLS) [1].

Physical Layer Security (PLS) for URLLC Security

Meanwhile, to address these issues, an approach known as “physical layer security (PLS)” has emerged as a potential method for securing URLLC signaling, an alternative to cryptographic methods for information protection. PLS uses the randomness of the wireless channel characteristics to provide secure communication, making it difficult for eavesdroppers to intercept the transmitted data.

In this way, PLS provides flexible and simple security improvements compared to complex cryptographic methods.

PLS also provides secure message transmission without the need for additional secret keys and complex encryption/decryption methods.

In addition, PLS technologies can adapt to dynamic wireless channel conditions, making them suitable for time-varying environments such as high mobility scenarios in transportation communication (connected cars). Simple and achievable security mechanisms, such as physical layer security (PLS), have emerged as a powerful alternative to complex cryptographic security methods for URLLC, exploiting the randomness of the wireless channel (i.e., the randomness of the characteristics of a discrete transmission channel built on top of the wireless access).

Compared to higher-level cryptographic solutions, PLS generates less signalling overhead, reducing additional bandwidth requirements, while using less computational resources and processing power.

This is especially useful for IoT applications in ITS, which contain resource-constrained devices that need to preserve system resources while ensuring secure data transmission.

Developing new approaches to PLS that can be used to organise secure URLLC in 5G and future sixth-generation wireless networks (in 6G - Hyper Reliable Low Latency Communication (HRLLC)) is currently a relevant scientific task.

Security of PLS URLLC based on the concept of "wire-tap channel"

Effective methods for improving PLS URLLC can be approaches based on the concept of a channel with a tap ("wire-tap channel"), proposed by A.D. Wyner [2] and developed later in other works [4-7]. Its essence lies in the fact that many physical models of unauthorised access to information in real information and communication systems (both wired and wireless) can be mapped to a mathematical model containing two channels: the *main channel* - from the source of information to the recipient and the *tap channel* (wire-tap channel) - from the source to the illegal user.

Wyner suggested that ideal secrecy can be achieved in the presence of eavesdroppers if the quality of the

listening channel becomes worse than the quality of the legal channel.

The proposed scheme is a so-called degraded broadcast channel (DBC) with one input and two outputs. However, unlike the usual task of maximising the transmission rate to both recipients, traditional for the DBC, here the task is to minimise the amount of information received by the illegal user, while maintaining the maximum possible speed of information transmission to the legitimate user. For this purpose, it is proposed to perform random encoding on transmission and the corresponding (non-random) decoding on reception. Below is a formal description of the model shown in Fig. 1.

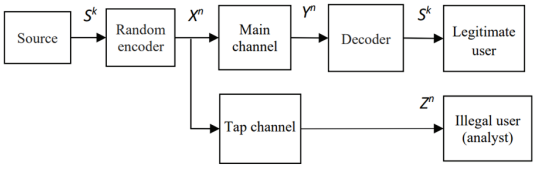

Fig. 1. Model of the concept of "wire-tap channel"

The channel for transmitting information from the source to the recipient is called the *main channel*; the channel for diverting to the illegal user (analyst) is called the *tap channel*.

The source is a device that generates one of the symbols belonging to the discrete set *S* at each unit of time. At this stage, we will limit ourselves to representing the source as a sequence of independent, identically distributed random variables belonging to *S*. We will denote the entropy of the source by H_S.

The main channel is a discrete memoryless channel {X, p(y/x), Y} with the input alphabet *X*, the output alphabet *Y* and the transition probability matrix |p(y/x)|.

A random encoder is a mapping of k-blocks of the source *S* into n-blocks of the encoder *X*, i.e. x = f (s,t), where f is the coding function, t is a random number. The encoding function is constrained to have $f(s_i, t) \neq f(s_j, t')$ for any t, t ' and $s_i \neq s_j$.

The decoder in the main channel is a non-random mapping of n-blocks *y* into k-blocks s', s' = ψ(y), where ψ is the decoding function.

According to the concept, the source produces a sequence of equally probable and independent binary symbols

$$S_1, S_2, \dots, S_i \quad (1)$$

The encoder combines the input symbols into blocks of k symbols

$$S^k = (S_1, S_2, \dots, S_k) \quad (2)$$

and encodes each block into a binary n-dimensional vector

$$X^n = (X_1, X_2, \dots, X_n), \quad (3)$$

which in the main channel is converted into a vector

$$Y^n = (Y_1, Y_2, \dots, Y_n) \quad (4)$$

and is fed to the decoder, where it is decoded into a vector

$$\hat{S}^k = (\hat{S}_1, \hat{S}_2, \dots, \hat{S}_k) \quad (5)$$

A tap channel (wire-tap channel) is connected in series with the main channel, at the output of which the vector

$$Z^n = (Z_1, Z_2, \dots, Z_n) \quad (6)$$

In the case when the main binary channel has no interference, and the tap channel is a discrete symmetric channel with error probability *p*, i.e.

$$Y^n = X^n \text{ and } Z^n = X^n \oplus \mathrm{E}^n \quad (7)$$

where $\oplus$ - is the component-wise summation of vectors modulo two;

E^n – is the binary vector of errors in the diverted channel, which are independent, the probability of a unit appearing in each of the positions is *p*, and of a zero is *1- p*.

In this case, the *task of probabilistic coding is to maximise the uncertainty*

$$\Delta = k^{-1} H(S^k | Z^n) \quad (8)$$

in the diverted channel with respect to the transmitted S^k messages during the observation of Z^n.

The main transmission parameters in this model are:

- information transmission rate – k/n;
- probability of an error per symbol in the main channel

$$P_e = \frac{1}{K}\sum_{i=1}^{K} p(s_i \neq s_{j'}); \quad (9)$$

- information uncertainty

$$\Delta = H(S^k | Z^n)/k \quad (10)$$

The parameter Δ characterises the security of information with respect to the diverted channel. Indeed, using the well-known relation for the amount of information transmitted over the channel [1], we can write as (11)

$$I(S^k; Z^n) = H(S^k) - H(S^k \mid Z^n), \qquad (11)$$

where $H(S^k)$ - is the entropy of the k-blocks of the source;

$H(S^k \mid Z^n)$ - is the conditional entropy of the source given the n-blocks at the channel output;

$I(S^k; Z^n)$ - is the average mutual information between the k-blocks at the input and the n-blocks at the channel output.

Then it is obvious that if $H(S^k \mid Z^n) = H(S^k)$, then $I(S^k; Z^n) = 0$ and no information is transmitted to the illegal user. If $H(S^k \mid Z^n) = 0$, then $I(S^k; Z^n) = H(S^k)$ and the illegal user receives complete information from the source. In the intermediate case, the illegal user receives some non-zero amount of information, but it is incomplete.

The main conclusion established in [2] is to prove the existence of an encoding-decoding method for the region of finite transmission rates $0 \le R \le R_S$, in which high security $\Delta \to H_S$ can be ensured in the downlink channel, if $n \to \infty$.

Constructive methods of implementing the concept of "wire-tap channel"

Constructive methods of implementing the concept of "wire-tap channel", which were called "code protection" (CP) and the corresponding non-asymptotic estimates of its effectiveness were formulated in [4].

The essence of the CP method is that by using special redundant coding, which functionally reflects random coding based on a codebook, it is possible to transmit information in the main channel (the channel of the legitimate recipient) practically without errors, and in the interception channel ("wire-tap channel") at the same time ensure that the error probability approaches unity not at the cost of energy suppression of the intercepted signals, but at the cost of complexity of coding and some deterioration in the quality of the interception channel compared to the recipient channel (this approach assumes that the illegal user knows the same a priori set of information as the legitimate user, i.e. no secret data is used here). If the main channel is of sufficiently high quality, then redundancy in such coding is not used to increase the reliability of information transmission, but, on the contrary, to exclude the possibility of information interception by the interception channel (the quality of the main channel is practically not reduced or is reduced slightly).

Physical interpretation of the effectiveness of probabilistic cryptographic transformations for PLS URLLC

When considering the capabilities of an illegal user to intercept information, it is first necessary to assess the reduction of the physical zones of possible interception (with different requirements for information security), which is achieved by using probabilistic cryptographic transformations for PLS URLLC. The physical-spatial model of the “wire-tap channel” concept for PLS URLLC looks like in Fig. 2.

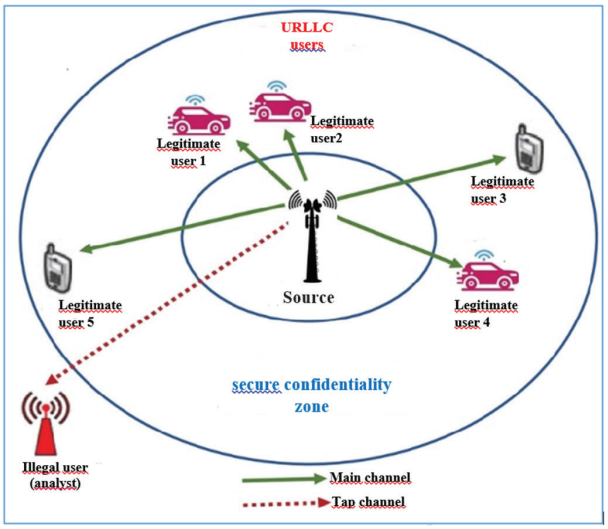

Fig. 2. Physical-spatial model of the “wire-tap channel” concept for the connected car

This physical-spatial model of the "wire-tap channel" concept for *URLLC recipients* solves the problem of ensuring non-cryptographically protected exchange of information between the source and legal recipients (via the main channel) within the *secure confidentiality zone* while simultaneously preventing the *illegal user* from obtaining this information outside the *secure confidentiality zone (via the tap channel)*. The inability of an illegal user to obtain information outside the secure confidentiality zone can be assessed using various indicators and standardised criteria. Since using probabilistic cryptographic transformations, with the same signal/noise ratio (without coding) at the input of the receiver of an illegal user, it is possible to obtain a worse quality of reproduction of the transmitted message, the criterion of the quality of the communication channel (both the diverted channel and the main channel) can be, for example, its *bandwidth C*. By calculating the *bandwidth C* for cases of application or non-application of probabilistic cryptographic data transformations, it is possible to estimate the gain in the

size (reduction) of the information availability zone for an illegal user. Accordingly, this gain will depend on the parameters of the block code, the structure of its adjacent classes, etc.

Conclusion

5G technology with the innovative 5G URLLC service is the driver of the connected car revolution thanks to its ultra-reliable low latency communication.

The implementation of 5G URLLC has revolutionized current ITS applications such as autonomous driving, vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication, which enables data exchange in V2V (vehicle-to-vehicle), V2I (infrastructure), V2P (pedestrian), V2N (network) formats, supporting extreme quality of service requirements in high mobility environments.

To ensure strict quality of service (QoS) requirements, URLLC uses short, finite block-length packet signals for data transmission, which greatly complicates (eliminates) the use of conventional complex cryptographic methods for secret-key-based information security.

Effective methods for improving PLS URLLC can be approaches built on the concept of a wire-tap channel, which limits the information availability of illegal (unauthorised) users to a spatially secure confidentiality zone created through probabilistic-cryptographic transformations of URLLC commands.

References

1. Yongpeng Wu; Ashish Khisti; Chengshan Xiao; Giuseppe Caire; Kai-Kit Wong; Xiqi Gao «A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead». IEEE Journal on Selected Areas in Communications, Volume: 36 (2018), Issue: 4, pp 679 -695

2. *Wyner A.D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355-1387.

3. *Csisz´ar I., K¨orner J.* Broadcast Channels with Confidential Messages // IEEE Trans. Inform. Theory. – 1978. –Vol. 24, № 3. – pp. 339–348, May 1978.

4. Korzhik V.I., Yakovlev V.A. Non-asymptotic estimations of the effectiveness of the code noise of one channel // Problemy peredachi information. – 1981. – Volume 17, Issue 4. – pp. 11–18.

5. Korzhik V.I., Goritsky V.M., Otsenki effektivnosti metodov kodovogo zashumleniya [Assessment of the efficacy of code noise reduction techniques] // Specialized communication equipment. - Series: TPS. - Issue 1. - 1983. - pp. 74-83.

6. V.Y. Korzhik, V.M. Goritsky, Evaluation of the effectiveness of code noise methods // Specialized communication equipment. - Sir TPS - Issue 1. - 1983. - pp. 74-83.

7. Goritsky V.M. Probabilistic cryptography in information security systems: code protection // Electronics and Communications. - Issue 5. - 1998. - pp. 140-145.

Горицький В.М.

Безпека зв'язку фізичного рівня в мережах 5G/6G інтелектуальних транспортних систем на основі імовірнісно-криптографічних перетворень

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, м. Київ, Україна

Проблематика. Наднадійний зв'язок із низькою затримкою URLLC (Ultra-Reliable Low Latency Communication) як послуга, яку пропонують бездротові системи п'ятого та шостого покоління (5G/6G) є технологічною відповіддю на потреби різних критично важливих застосунків, які вимагають надійної передачі даних з низькою затримкою. До цих застосунків відносяться також послуги Інтелектуальних транспортних систем, які серед іншого забезпечують підключеність та автономне керування транспортними засобами. Поєднання вимог до високої надійності та низької затримки у сценаріях використання URLLC створює проблему безпеки передачі даних URLLC як таку, що не може бути вирішена використанням звичайних складних криптографічних методів на основі секретного ключа. У статті детально розлядається підхід з використання механізмів безпеки фізичного рівня (physical layer Security - PLS), як потужної альтеранативи класичним методам криптографічної безпеки для URLLC, а також пропонується застосування концепції каналу із відведенням («wire-tap channel») в URLLC з аналізом ефективності, яка може бути досяжна при цьому для безпеки фізичного рівня.

Мета досліджень. Мета статті – надати огляд рішень інформаційної безпеки у сценаріях використання URLLC, а також запропонувати конструктивний метод захисту інформації для надійної передачі даних з низькою затримкою без застосування криптографічних механізмів на основі секретного ключа.

Методика реалізації. Використано теоретичні дослідження в галузі концепції відвідного каналу для створення рішень, які дозволяють забезпечити захист даних з інформаційно-теоретичною стійкістю у сценаріях використання URLLC для надання послуг IoT, підключеного автомобіля та автономного водіння.

Результати досліджень. У статті детально розглянуто проблеми безпеки даних у наднадійному зв'язку із низькою затримкою URLLC (Ultra-reliable low latency communication) як послузі, яку пропонують бездротові системи п'ятого та шостого покоління (5G/6G). Визначено, що URLLC є технологічною відповіддю на потреби різних критично важливих застосунків, які вимагають надійної передачі сигналу з низькою затримкою, а серед цих застосунків мають місце послуги Інтелектуальних транспортних систем, які серед іншого забезпечують підключеність та автономне керування транспортними засобами. Показано, що поєднання вимог до високої надійності та низької затримки у сценаріях використання URLLC створює проблему безпеки передачі даних URLLC як таку, що не може бути вирішена використанням звичайних складних криптографічних методів на основі секретного ключа. Обгрунтовано доцільність використання механізми безпеки фізичного рівня (physical layer Security - PLS) як потужної альтернативи класичним методам криптографічної безпеки для URLLC. Детально розглянуто підхід з застосування концепції каналу із відведенням («wire-tap channel») в URLLC, а також результати, які можуть бути досяжні при цьому для безпеки фізичного рівня, вплив параметрів кодів для імовірнісно-криптографічних перетворень у відповідності до концепції каналу із відведенням на PLS URLLC. Надано оцінки ефективності PLS URLLC для кодів кінцевої довжини блоку.

Висновки. Ефективним шляхом забезпечення безпеки даних для наднадійного зв'язку із низькою затримкою на фізичному рівні (PLS URLLC) бездротових систем п'ятого покоління 5G у сфері підключених автомобілів та транспортних засобів 4-5 рівнів автоматизації можуть бути підходи, побудовані на концепції каналу із відведенням («wire-tap channel»).

***Ключові слова**: IoT; інформаційна безпека IoT; наднадійний зв'язок із низькою затримкою; інтелектуальна транспортна система; підключені транспортні засоби; безпека автономного керування транспортними засобами; захист фізичного рівня; концепція каналу із відведенням; канал із відведенням.*

Received by the Editorial Office
August 18, 2025

Accepted for publication
September 30, 2025