BASIC TECHNOLOGIES AND TECHNIQUES *ML/AI* FOR IMPROVING PHYSICAL LAYER SECURITY FOR *5G/6G* COMMUNICATIONS SYSTEMS

Oleksandr TSOPA,
DS., Professor
Kharkiv National University of Radio Electronics,
oleksandr.tsopa@nure.ua

Oleksandra DUDKA
Ph.D., Associate Professor
Kharkiv National University of Radio Electronics,
oleksandra.dudka@nure.ua

Anatolii Merzlikin
Ph.D student
Kharkiv National University of Radio Electronics,
anatolii.merzlikin@nure.ua

ABSTRACT

One of the main features of using the millimeter wave band in the deployment of 5G/6G technologies is that these waves have a narrower range and less ability to penetrate obstacles such as buildings and trees [1,2]. Therefore, millimeter waves require a larger number of communication nodes located closer to each other to ensure network coverage. In addition, due to the high frequency of millimeter waves, they are subject to greater signal scattering and absorption from surfaces such as building walls and other obstacles, which can result in reduced data transmission range. Therefore, it is necessary to consider engineering solutions and technologies of artificial intelligence (IA) and machine learning (ML), which will allow ensuring high-quality communication between communication nodes, taking into account the peculiarities of the millimeter range of radio waves.

However, thanks to the high bandwidth of the millimeter wave band, 5G/6G technology can provide high-speed transmission of large amounts of data, enabling new applications and services such as virtual reality (VR), augmented reality (AR), augmented reality (XR), Internet of Things (IoT) and others. Therefore, using the millimeter range of radio waves is an important element of 5G/6G technology that requires specific solutions to ensure reliability and security at the physical level of the network.

Keywords: Physical layer security, Future communication systems 5G/6G, Artificial intelligence, Machine learning.

INTRODUCTION

The deployment of 5G/6G technologies may lead to certain information security threats, including [3-5]:

1. Increase in the number of connected devices: significantly more devices can be connected to a 5G/6G network, which increases the potential number of vulnerable points in the network and increases the risk of cyber-attacks.

2. Increased data throughput: 5G/6G network can transmit significantly more data, leading to an increased risk of losing sensitive information if any part of the network becomes compromised.

3. Use of new technologies: 5G/6G networks use new technologies, such as network virtualization and feature scaling, which may create new vulnerabilities.

4. Increasing number of network access points: With the deployment of 5G/6G networks, new access points such as small base stations will appear, which can become the target of attacks.

5. Expanding network geography: 5G/6G technologies can create networks that cover much larger areas, which can increase the risk of outages or attacks spreading.

6. Dependence on service providers: the deployment of 5G/6G networks requires cooperation with many service providers, which may increase information security risk.

In this regard, it is important to pay attention to ensuring network security and applying measures to counter cyber threats, such as data encryption, network access control, network monitoring, disaster recovery, etc.

Table 1.

Comparison of 4G, 5G, and 6G networks.

Technology	4G	5G	6G
Applications	3GPP LTE Advanced (LTE-A) Frequency aggregation, Advanced antennas, MIMO technology, Relay transmission, Work optimization, Heterogeneous networks (SRVCC, eMBMS, CoMP)	Enhanced Mobile, Broadband, Communications (eMBB), Ultrareliable Low Latency Communications (URLLC), Massive Machine Type Communications (mMTC)	Holographic-Type Communication (HTC), Tactile Internet, Intelligent Transport and Logistics, Intelligent and automated machines, Virtual Reality (VR), Augmented Reality (AR), Extended reality (XR)
Peak data rate	1 Gbps	10 Gbps	1 Tbps
Frequency	6 GHz	3–300 GHz	1000 GHz
Latency	(20 -30) ms	10 ms	<1 ms
Mobility support	Up to 120 km/h	Up to 500 km/h	Up to 1000 km/h
Spectral efficiency	5 bps/Hz	30 bps/Hz	100 bps/Hz
Reliability	99.999%	99.9999%	99.99999%

MAIN PART

Traditionally, high-level cryptography techniques to resolve any information privacy disagreements include data authentication, secret key establishment, and secret distribution. However, with the increasing computing power of eavesdropping devices, the aforementioned methods may be insufficient or even unusable if an

additional secure channel is required to generate the secret key. Physical layer security (PLS) has emerged as a promising solution to the computational eavesdropping challenges of secure transmission. Compared with complex cryptographic methods, PLS does not depend on the computing power of eavesdropping devices and has the advantage of reducing computational costs and resource consumption. From the perspective of information-theoretic frameworks, it has been found that PLS can achieve secure and reliable communication even when network attackers have very powerful computing capabilities. This approach to information security is particularly effective because it does not rely on underlying computing power, but rather on characteristics of the transmission environment, such as noise, fading, and interference, and provides security guarantees that are independent of the computing power of the eavesdropper. Overall, the PLS approach has clear advantages and is well-suited for distributed processing systems and dynamic network configurations. Therefore, the PLS approach can be used as an alternative complement to computationally demanding high-level techniques to further ensure data security.

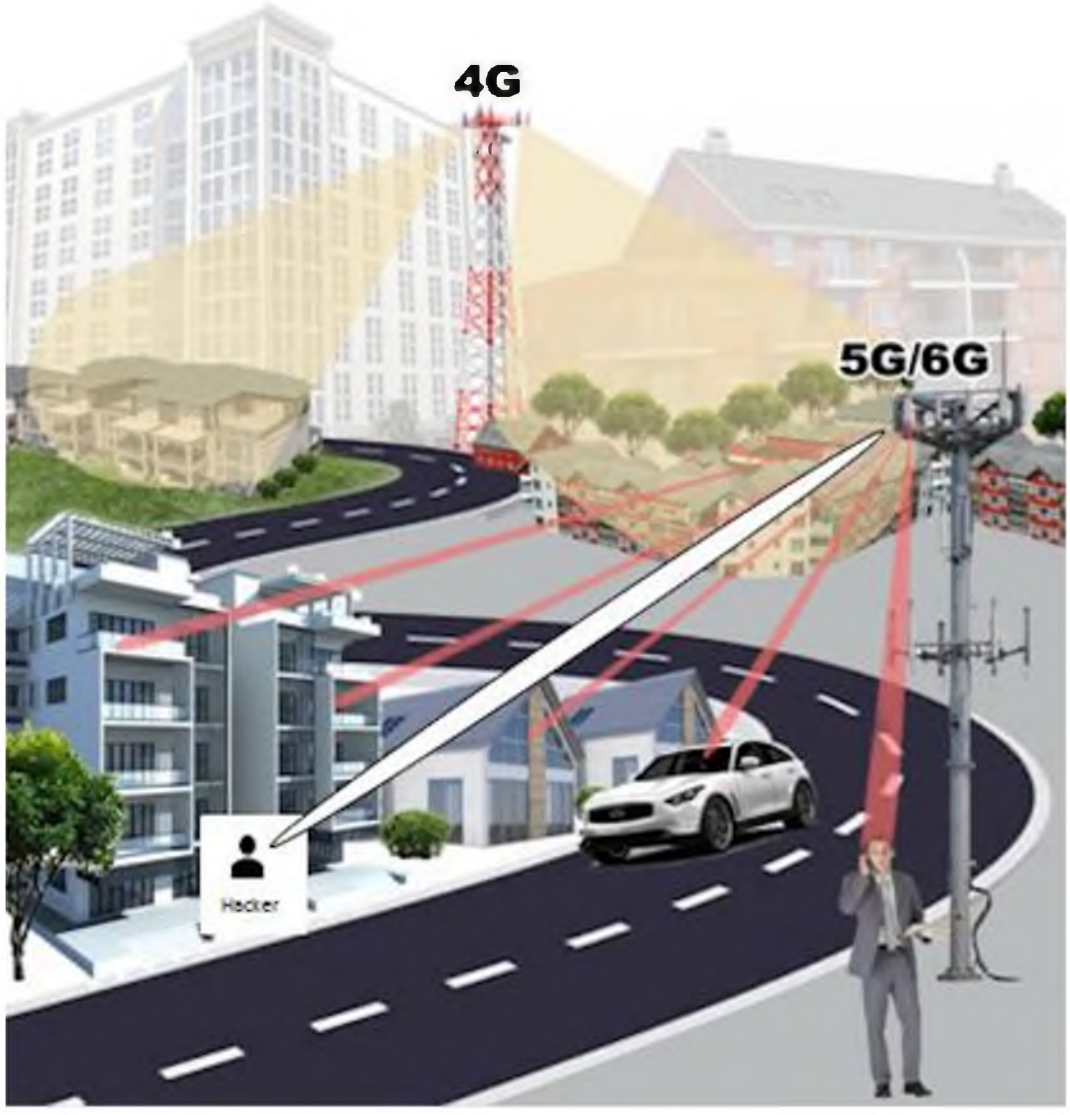

Figure 1. Wiretap channel and beamforming system 5G/6G

Although PLS can be accurately evaluated using popular performance metrics such as secrecy capacity, secrecy rate, secrecy bandwidth, etc., which are discussed in detail in the literature, the security performance is quantified by maximizing the performance difference between legitimate channels and listening channels.

PLS technology aims to improve the quality of the received signal at the intended receiver or to reduce the performance of the listening channel compared to the legal channel. Under these circumstances, there is a need to allocate transmit power based on the states of the legitimate and eavesdropping channels to improve PLS, since the transmit power affects the signal quality at the intended receiver and eavesdropper. However, the distribution of power in PLS is a complex task. It depends heavily on the prior information the transmitter has about the Channel State Information (CSI) of the intended receiver and eavesdropper (Fig.1).

Basic studies of PLS as a method for characterizing achievable anti-eavesdropping performance have been extensively investigated from fundamental information theory perspectives for various communication scenarios and channel types and under various CSI knowledge assumptions. These studies have inspired the development of many signal processing design methods. In this context, a large number of research works have been carried out, which have contributed insightful thoughts and opportunities to understand practical security designs, optimization methods, state of the art, etc.

Key technologies, technical challenges, and countermeasures were reviewed from the fundamental perspectives of design strategies involving physical layer authentication, secret key generation, eavesdropping coding, and multi-antenna techniques and relay interactions. In addition, some authors have presented an extensive study of multi-antenna techniques in multi-user wireless networks using different assumptions about the availability of CSI. Securing multi-antenna methods is an efficient and powerful approach in PLS that can offer higher spatial degrees of freedom. It can also be seen that the interferences and interferences encountered by PLS arise from different assumptions about wireless channel characteristics and interceptor models. Naturally, the concept of optimization methods in PLS plays a key role in practical security design, so it has attracted considerable attention from the research community.

To overcome the limitations associated with existing optimization problems, machine learning (ML) and artificial intelligence (AI) technologies must be effectively integrated into 5G/6G networks to provide better security and resource management (Fig. 2). The use of ML and AI technologies in the field of mobile communication infrastructure has made significant progress in ensuring security, reliability and resource allocation in a dynamic, reliable and trustworthy manner.

The main studies of PLS system design can be generally summarized in two main approaches. The first is related to secrecy functions, which in particular focus on the characterization of security and eavesdropping capabilities, or more generally, the trade-off between achievable secrecy capability and privacy distrust based on information-theoretic framework concepts. The second approach is related to security system design, which mainly focuses on designing and optimizing secure transmission strategies using signal processing techniques.

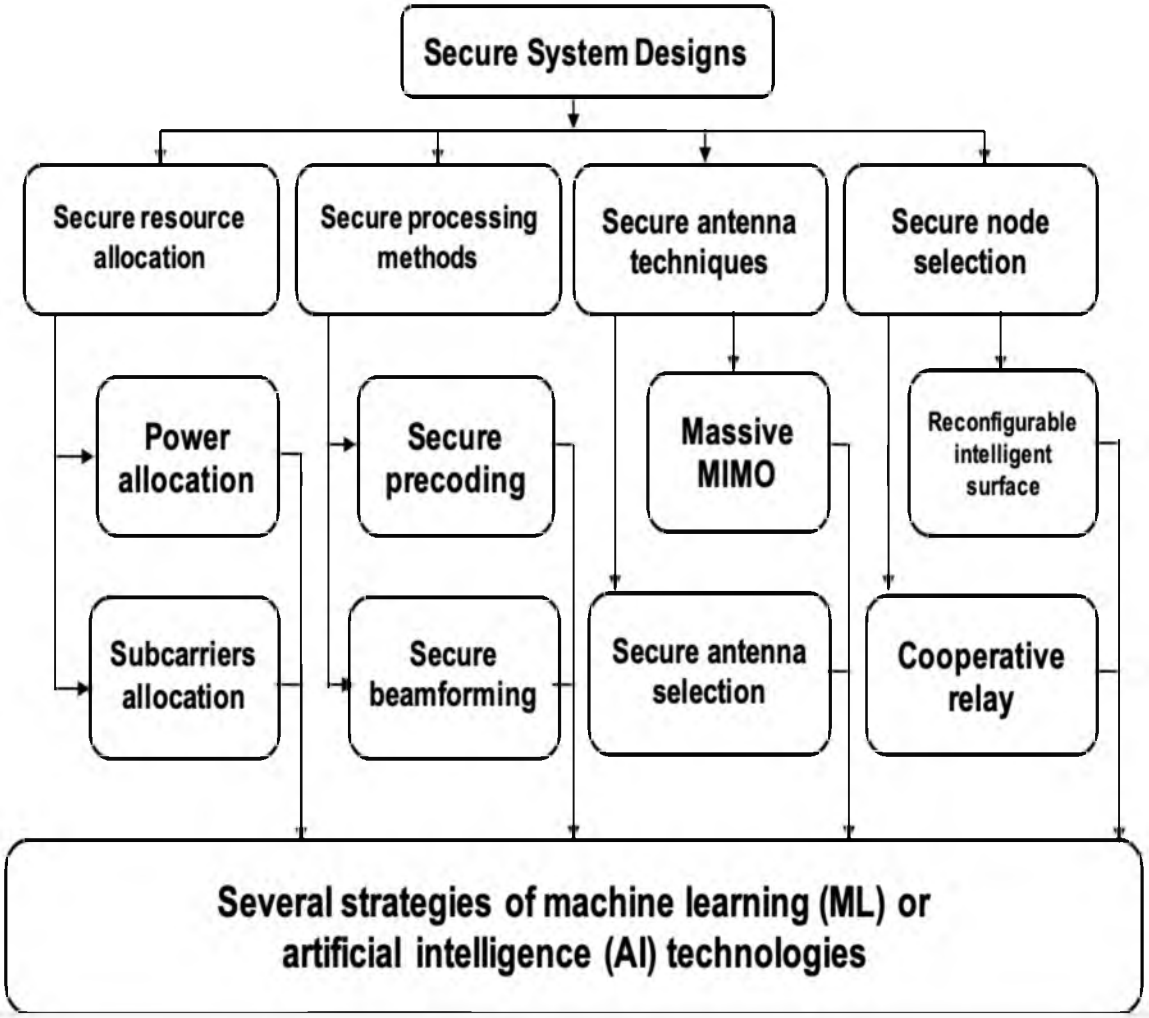

Figure 2. Secure transmission strategies to improve the security and robustness of physical layer designs.

Many conventional physical-layer security technologies without regard to communication secrecy can be retrofitted for secure data transmission in the fundamental PLS framework. To realize the main optimization problems and PLS performance measures, the main research questions and directions are expected to include three candidate secure design strategies, as shown in Figure 2. These research topics are signal processing techniques, secure resource allocation, and secure antenna selection/cooperative nodes. Signal processing techniques use secure precoding and beamforming to achieve the development of effective secure communication strategies. The secure precoding and beamforming designs take full advantage of the characteristics of multi-node and multi-antenna scenarios that can form virtual or massive MIMO networks. Allocation of resources, which is usually adopted in traditional communication systems, includes the allocation of power and subcarriers. It mainly focuses on resource management systems that use multifaceted wireless resources, including power, time slots, and frequency. Shared nodes or safe antenna selection, such as interference source selection, relay node selection, and user selection, which are widely used in multi-node scenarios, have been fully explored as promising methods to improve PLS design. Such methods attempt to select

appropriate cooperative nodes or antennas from a set of candidates to improve the effectiveness of secure design strategies.

CONCLUSION

Physical layer security has evolved as a new dominant alternative that can complement or even replace the traditional approach to security. The stringent requirements of new wireless networks create new challenges for PLS. Recently, the integration of ML/AI and PLS has attracted some interest from researchers. In this article, we have introduced the main directions and techniques of intelligent PLS, classifying existing PLS methods in an easy-to-understand way.

References:

1. Prediction model of energy security for the systems of subscriber radio access with branched street and corridor communications channels // A.A. Strelnitskiy, A.E. Strelnitskiy, O.I. Tsopa, V.M. Shokalo / Radioelectronics and Communications Systems - Springer - 2011.
https://link.springer.com/article/10.3103/S0735272711020014

2. The project of joint investigations of millimeters waves propagations for Ukrainian advanced 5G communication lines // V.I. Leonidov, N.V. Ruzhentsev, A.I. Tsopa, A.A. Zarudniy / *2016 9th International Kharkiv Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW).*
https://ieeexplore.ieee.org/abstract/document/7538185

3. Millimeter-range radiometric system for perspective problems of meteorology and telecommunication // V.V. Pavlikov, N.V. Ruzhentsev, A.D. Sobkolov, A.I. Tsopa… / *2017 XI International Conference on Antenna Theory and Techniques (ICATT).*
https://ieeexplore.ieee.org/abstract/document/7972583

4. Estimation of the Bandwidth of the Communication Channel of 5G Networks Based on Small Cells // O. Tsopa, O. Dudka, A. Merzlikin, N. Ruzhentsev / *IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, pp.525-529, 2021. https://ieeexplore.ieee.org/abstract/document/9575330

5. Security analysis of wireless communication systems of the millimeter waves band // D. Salnykov, A. Dudka, A. Tsopa / *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT).*
https://ieeexplore.ieee.org/abstract/document/8409211