Improvement of information security of the physical level based on the model of the advanced NOMA algorithm*

Volodymyr Saiko[1,†], Volodymyr Nakonechnyi[2,†], Oleksandr Pliushch[2,*,†], Serhii Toliupa[2,†], and Bohdan Zhurakovskiy[3,†]

[1] *Kruty Heroes Military Institute of Telecommunications and Information Technology, 45/1 Knyaziv Ostrozkikh str., 01011 Kyiv, Ukraine*
[2] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., 01601 Kyiv, Ukraine*
[3] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," 37 Peremogy ave., 03056 Kyiv, Ukraine*

Abstract

The paper considers the problems of implementing mobile communications in the terahertz spectral range (30-300 GHz), in particular, that of blocking the line-of-sight signal by small objects. Two following approaches to the solution of the problem are proposed: densification of the cellular infrastructure using mobile nodes and multi-cell connection of subscriber terminals. The main attention is paid to the improved M-CO-NOMA algorithm, which combines retransmission and modulated transmission. Its features include clustering of terminal devices by fractal dimension; differentiated modulation of user signals (QPSK: quadrature for distant ones, real component for nearby ones); introduction of orthogonality at the signal formation stage, which reduces interference without spectrum expansion. Comparative analysis showed that M-CO-NOMA outperforms classical NOMA in terms of information efficiency (6.00e-2 vs. 4.50e-2), reduced SER, lower computational complexity, and better noise immunity. Aspects of physical-level information security, including types of threats and methods for their neutralization in M-NOMA and CO-NOMA systems, are also considered.

Keywords

terahertz range, transmission blocking, modulation, retransmission, NOMA, information efficiency, physical security level.

1. General statement of the problem

The deployment of mobile networks in the 30–300 GHz spectral range opens up new opportunities for high-speed data transmission [1, 2], but at the same time it is accompanied by a number of technical challenges, in particular at the level of end subscriber devices [3]. Modern terminals support operation in the 800 MHz–2.7 GHz range; however, for effective operation in the terahertz spectrum, hardware modernization and optimization of antenna systems capable of covering the entire range from 800 MHz to 300 GHz are necessary.

Studies show that short wavelengths in the terahertz range make transmission sensitive to physical interference [4]. Even small objects can block the line-of-sight signal, which leads to a decrease in the power on the receiving side and loss of connection stability. To increase reliability, the following measures are proposed:

- densification of cellular infrastructure thanks to extra mobile nodes;
- multi-cellular connection of terminals to several access points simultaneously.

Signal blocking is random and unpredictable, so the communication system must respond quickly by redirecting the active session to an alternative access point. Such a multi-connection mechanism within the same spectrum is a new functionality of access networks, which differs from the traditional distribution of traffic between different radio access technologies.

* *CSDP'2026: Cyber Security and Data Protection, May 7, 2026, Lviv, Ukraine*

* Corresponding author.
† These authors contributed equally.
pvgsaiko@gmail.com (V. Saiko); volodym.nakonechnyi@knu.ua (V. Nakonechnyi); oleksandr.pliushch@knu.ua (O. Pliushch); tolupa@i.ua (S.Toliupa); zhurakovskybiyu@tk.kpi.ua (B. Zhurakovskiy)
0000-0002-3059-6787 (V. Saiko); 0000-0002-0247-5400 (V. Nakonechnyi); 0000-0001-5310-0660 (O. Pliushch); 0000-0002-1919-9174 (S. Toliupa); 0000-0003-3990-5205 (B. Zhurakovskiy)

In this context, the use of NOMA (Non-Orthogonal Multiple Access) technology [5, 6] is promising, which provides high spectral efficiency due to the joint use of a frequency resource by several users without orthogonal division. Unlike OFDMA, where signals are divided by frequency or time, NOMA allows simultaneous transmission, which increases bandwidth.

The rejection of orthogonality creates interference between signals, which is eliminated using SIC (Successive Interference Cancellation) algorithms. These algorithms gradually decode user signals by power level, subtracting already decoded signals from the received stream. Although SIC effectively reduces interference, increasing the number of users in a NOMA system leads to an increase in computational complexity.

Non-orthogonal multiple access is one of the key technologies that can ensure the efficient operation of wireless networks of the fifth and subsequent generations (5G and B5G). Unlike traditional access methods based on spectrum division (FDMA, TDMA, OFDMA), NOMA allows simultaneous data transmission to several users within the same frequency resource, which significantly increases spectral efficiency.

Modern communication systems use orthogonal spectrum division, which has led to the depletion of the available frequency resource. This limits the possibilities of scaling networks, especially in the conditions of the rapid growth of the number of devices connected to the Internet of Things (IoT), processing of big data (Big Data) and the development of the tactile Internet.

NOMA technology allows:

- To effectively use the spectrum without dividing it between users;
- To provide high data transfer rates, low latency, and reduced downtime;
- To increase energy efficiency and network throughput;
- Ensure system fairness — equal access to the resource for users with different channel conditions;
- Improve the confidentiality and security of transmitted data.

It should be noted that NOMA technology, although designed primarily to improve spectral efficiency in 5G/6G wireless networks, has built-in features that can help improve the confidentiality and security of transmitted data — especially at the physical level. The key security mechanisms in NOMA, which are relevant for solving the stated problem, are as follows:

1. Superposition coding and Successive Interference Cancellation (SIC) that implements the technique in which data from multiple users is transmitted simultaneously on the same frequency, but with different power. This makes interception difficult: the attacker needs to know the exact power configuration and decoding algorithm. At the same time, SIC allows a legitimate user to distinguish their signal while an outside observer sees only a mixture of signals.
2. Physical Layer Security that is designed to use channel fluctuations (e.g., multipath, fading) to generate keys or mask the signal. NOMA allows the transmission to be adapted to the channel conditions, which makes interception less effective.
3. Asymmetric access to information in which users with better channel conditions can decode the signals of others, but not vice versa. This creates an access hierarchy that can be used to control confidentiality.
4. Selective coding and encryption that means that in NOMA, it is possible to implement dynamic encryption depending on the power and the channel. For example, weaker users can receive additional encryption to compensate for the risk of interception.

Practical scenarios for using NOMA are shown in Table 1.

NOMA can be integrated with existing access algorithms, making it a universal solution for heterogeneous networks.

To differentiate users, NOMA uses power distribution: users with better channel conditions are assigned less power, and those who are further away are assigned more power. This allows receivers to use SIC algorithms to decode signals in stages. However, this scheme creates a high level of interference, which complicates the system architecture; increases computational complexity; and creates security and privacy risks, especially if the power is set incorrectly.

Before transmission, user signals can be pre-divided by time (TDMA) or frequency (FDMA), which partially compensates for interference, but reduces the benefits of NOMA.

Table 1
Practical scenarios for using NOMA

Scenario	How NOMA improves security
IoT Systems	Makes mass interception of sensor data more difficult
5G/6G Mobile Networks	Provides multi-level access to data
Military/Government Communications	Hides message structure at the physical layer
Smart City/eHealth	Minimizes the risk of confidential information leakage

To differentiate users, NOMA allocates different amounts of power to different users, which increases the level of interference and security concerns between signals, as is shown in Figure 1.

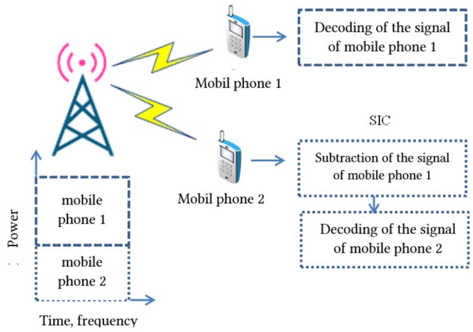

Figure 1: The process of operating mobile communications with NOMA technology

In NOMA systems, each user receives a superposition signal that contains both its own message and interference components from other users. To correctly decode its own signal, it is necessary to apply the SIC algorithm — stepwise suppression of interference arising from the signals of other subscribers.

As the number of simultaneously active users increases, the amount of interference increases, which leads to an increase in the computational complexity of the SIC procedure. This creates an additional load on the receiver and can affect the delay and power consumption of the system.

Despite these challenges, research into NOMA technology in the context of next-generation wireless networks is actively ongoing. The main focus is on optimizing SIC algorithms, adapting to dynamic channel conditions, and ensuring scalability for a large number of users.

2. Analysis of publications by research topic

In traditional orthogonal multiple access (OMA) systems, users with worse channel conditions often receive limited access to the resources, which negatively affects the overall spectral efficiency. NOMA is proposed as a future candidate for 6G technology and allows simultaneous service to all users, regardless of channel quality, through flexible power allocation [7–9]. This provides equal service, high connectivity and low latency [10].

Methods for improving spectral efficiency, in particular MIMO-NOMA, as well as the relationship between cognitive radio and NOMA, are considered in [10–12]. Simulations confirm the advantages of NOMA over OMA (including OFDMA), although trade-offs between bandwidth and energy efficiency are also identified.

Among the latest developments one can list the following:

- Joint NOMA using distributed space-time block coding [13];
- New spectrum sharing methods for 5G [14], [19];
- Performance failure analysis [15];
- Spatial modulation in NOMA [16–18];

- Modern information protection approaches based on artificial intelligence and blockchain technologies for strengthening cybersecurity systems [20];
- Impact of randomly distributed users on system performance [21].

Of particular interest is the concept of VP-NOMA (Virtual Pairing NOMA) [22], which allows combining a central user with several peripheral OMA users. Simulations have shown that VP-NOMA outperforms both classical NOMA and OMA in terms of performance.

3. Problem statement

Based on the analysis of literature sources, the research goal is formulated as to develop an algorithm to improve the efficiency of NOMA technology, which takes into account the following:

- interference between user signals;
- computational complexity of SIC algorithms;
- reliability of functioning of decentralized 5G mobile networks;
- dynamic blocking of line-of-sight connections by moving obstacles during transmission in the terahertz frequency range;
- increasing information security of the physical layer.

4. General principle of operation of the proposed NOMA algorithm

The proposed improved Modulation-Cooperative-NOMA (M-CO-NOMA) algorithm for the downlink communication channel is focused on servicing two groups of subscribers using relay and phase modulation mechanisms.

The algorithm is implemented in the following five sequential steps:

Step 1: A common NOMA transport signal is formed at the base station, which combines data for all terminal devices in the service area.

Step 2: The generated signal is transmitted into the air in the first time slot and is received by the terminal device of the first subscriber.

Step 3: The first subscriber performs signal demodulation, selects the component intended for the second subscriber, and stores it in memory. The own signal is decoded using the SIC algorithm.

Step 4: In the second time slot, the stored signal is retransmitted from the first to the second terminal device.

Step 5: The second subscriber receives the retransmitted signal and performs flexible demodulation of both components — direct and retransmitted.

Unlike known solutions [8–18], the M-CO-NOMA algorithm includes the following additional technological operations that increase its efficiency:

- Clustering of terminal devices in the service area of the base station before signal transmission. For this, a fractal dimension estimation algorithm is used, which allows adaptively grouping devices according to the network topology.
- Differential modulation: when forming the transport signal, the signals of nearest users are modulated by the real component of the complex symbols of the QPSK constellation, and the signals of distant ones by the imaginary component. This allows reducing mutual interference and improving signal separation at the receiver.
- Intelligent cyber defence systems that use artificial intelligence technologies for attack detection, ransomware counteraction, and protection of wireless networks [23].

5. Mobile terminals clustering algorithm for implementing the improved M-CO-NOMA algorithm

Mobile terminals clustering is based on the fractal dimension analysis method [24]. The main stages of the method are the following:

- Determination of the increment of the number of nodes in the cluster (Qr).

- When the increment threshold value (Q_0) is reached, the cluster is considered complete.
- Nodes of the first cluster are excluded from further analysis.
- The process is repeated from a random starting position until the entire service area is fully covered.

This approach allows for effective localization of terminal groups for optimal power distribution and modulation within the framework of the M-CO-NOMA algorithm. The algorithm of the clustering method is shown in Figure 2.

The network is described by a matrix Q of size $n \times n$

$$Q = \begin{bmatrix} d_{11} & Z & d \\ W & d_{ij} & W \\ d_{n1} & Z & d_{nn} \end{bmatrix}$$

The elements of the matrix d_{ij} are a metric that characterizes the reachability of node j from node i. As mentioned above, such a metric can be distance or other metrics obtained based on the signal power level or signal-to-noise ratio, attenuation.

In the proposed algorithm d_{ij} is the signal power level that can be measured for a real network, and in the model it is calculated taking into account the attenuation model and transmitter power:

$$d_{ij} = p_j - \infty_{ij},$$

where p_j — the transmitter power level of the j th node (dB), $\propto_{ij}$ — is the signal attenuation between nodes i and j (dB).

Data collection on key parameters of network infrastructure functioning is traditionally carried out using centralized monitoring systems managed by mobile operators. However, within the framework of the 5G standard, such systems are limited to the domain of a single operator, which complicates the coordination of results between different providers and the creation of a single consensus database.

The proposed approach involves decentralized monitoring, in which subscriber end terminals act as active agents for collecting data on network efficiency. This model allows obtaining more accurate and localized information that is not available in centralized systems.

To process the collected data, a clustering algorithm based on the Cluster-growth method using fractal metrics is used. The algorithm is implemented in several sequential stages presented below.

Step 1: Initialization. Input data:

- number of network nodes n;
- metric matrix Q;
- metric change step Δr;
- cluster counter $z = 0$.

Step 2: Starting node selection. A node is randomly selected to serve as the starting point for cluster construction.

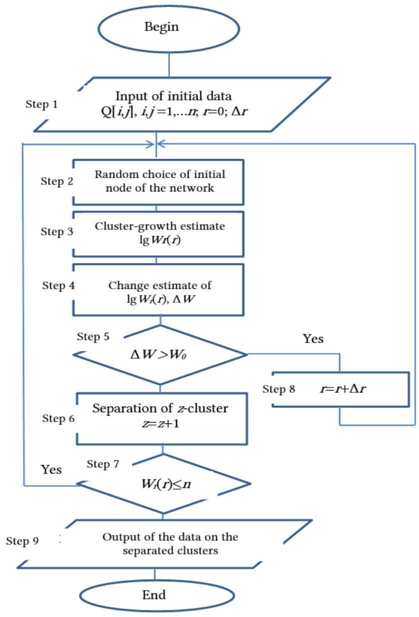

Figure 2: Algorithm of network clustering method

Step 3: Cluster formation

- New nodes are added to the starting node if the metric value is not less than the threshold value *r*.
- Construction can be carried out according to the principle of depth-first search [25].
- The result is the logarithm of the number of nodes in the cluster, which can take values from 0 to lg(n).

Step 4: Growth estimation:

- The number of nodes in the cluster is compared with the previous cycle.
- The change is random and depends on Δr and the distribution of metrics in the matrix **R**.

Step 5: Decision making:

- If the increment in the network size does not exceed the threshold value W_0, the cluster is considered complete.
- Otherwise, the metric r is increased by Δr (step 8), and the algorithm returns to Step 2.

Step 6: Cluster fixation:

- Nodes of the localized cluster are excluded from further analysis.
- The cluster counter z is increased by one.

Step 7: Completion check:

- If there are nodes remaining that are not assigned to any cluster, the process is repeated from Step 2.
- Otherwise, the clustering is completed.

Step 9: Output of results:

- A final cluster structure is formed, which can be used for further analysis of network performance.

A comparison of the proposed algorithm with the Formal Element (FOREL) and *k*-means algorithms [26] in terms of input data requirements is given in Table 2.

Table 1
A comparison of the proposed algorithm with the FOREL and *k*-means algorithms

Algorithm	Number of clusters	Cluster size	Node density in the cluster
FOREL	-	-	-
k-means	-	-	-
Proposed algorithm	-	-	-

From the above table it is clear that the proposed algorithm requires the least amount of input data, which allows it to be used in cases with an unknown number of clusters, their sizes and shapes, as well as with different node densities in clusters. The closest to the proposed algorithms can be considered FOREL; however, for use in conditions of different node densities in clusters, its modification is required.

6. Features of the implementation of the CO-NOMA and M-NOMA methods

6.1. CO-NOMA method

The Cooperative Non-Orthogonal Multiple Access (CO-NOMA) method involves the use of a signal relay mechanism between subscribers within the framework of NOMA technology. In the literature, CO-NOMA is considered a promising approach to increasing communication reliability, especially in unstable channel conditions. The main idea is that one subscriber (for example, MP1 (mobile phone 1)) relays a signal to another subscriber (MP2) if there is a favorable communication channel between them. The relay procedure is carried out in an additional frequency-time resource, in particular in the second time slot, after the initial transmission of the NOMA group signal from the base station. In the first time slot, the signal arrives simultaneously to MP1 and MP2. In the second slot, MP1 relays the signal to MP2. On the MP2 side, flexible demodulation of the two received signals is performed — direct signal from the base station and the relayed one from another subscriber. This allows to increase the signal-to-noise ratio (SNR) at the demodulator input and improve the communication quality.

Unlike traditional technologies such as OFDMA, CO-NOMA does not require the allocation of a separate resource for transmitting the retransmitted signal, since the NOMA group signal already contains information for all subscribers.

CO-NOMA technology is relatively new and is of considerable interest for modeling and experimental research, especially in the context of increasing noise immunity. From this point of view, combined multiple access methods that use several resource spaces (frequency, time, power, space) to separate users and provide multidimensional access to the radio air are promising.

Such methods should be dynamic and adaptive, with the possibility of flexible selection of resource space depending on the following:

- the number of active users;
- the level of interference;
- signal propagation conditions;
- equirements for quality of service.

In this context, the study of integrated solutions combining CO-NOMA with modulation-oriented NOMA (M-NOMA) methods, which implement bit division based on phase or amplitude modulation, is particularly relevant. This approach allows optimizing spectrum usage and improving service efficiency in complex radio environments.

6.2. M-NOMA method

The M-NOMA method implements the principle of modulation separation of users, which allows to create orthogonality between signals without using additional spectral resources. This approach not only simplifies the system architecture, but also increases its performance compared to classical NOMA implementations.

In M-NOMA, the base station performs clustering of users by distance to the transmitter in the following ways:

- near users are modulated by the real component of complex symbols of the QPSK constellation;
- distant users by the imaginary component.

This ensures spatial orthogonality between groups of users, which allows one to avoid mutual interference between near and distant terminals. As a result, near users receive signals without interference from distant ones, which improves the reception quality.

The M-NOMA method demonstrates the following advantages:

- reduction of the symbol error rate (SER);
- reduction of inter-cell and inter-cluster interference;
- reduction of delay and computational complexity;
- increased data transfer rate compared to traditional NOMA.

To combat residual interference at the receiver, the SIC algorithm is used. However, it is worth noting that SIC can reduce the Signal-to-Interference-plus-Noise Ratio (SINR) due to the effect of close proximity of or uneven power distribution between users.

In M-NOMA, SIC operations are performed only within one cluster — near or far users. This allows reducing the number of SIC operations for near terminals by $N/2t$ times compared to classic NOMA, while the processing volume for far users remains unchanged.

7. System model of the improved M-CO-NOMA algorithm

7.1. Architecture and operating principle

A model of a mobile network with one cell is considered, at the center of which there is a base station (BS) serving four users. To generalize the algorithm, it is assumed that there are N users, who are divided into two groups:

- near users — $N/2$,
- far users — $N/2$.

The users are divided into two clusters according to the distance to the BS and the signal level. Cluster 1 has a higher SNR compared to cluster 2. The BS performs signal modulation:

- for users of cluster 1 — on the real component of the QPSK constellation;
- for users of cluster 2 — on the imaginary component.

Each terminal knows on which component its message is placed, which ensures orthogonality between clusters.

In cluster 1, user terminal W1 receives the group signal in the first time slot, performs SIC decoding to extract its own message, and also stores the signal of user W2. In the second time slot, W1 retransmits the signal to W2. In the case of line-of-sight blocking in the terahertz range, W2 receives two signals — from the BS and from W1, which are processed using Maximum Ratio Combining (MRC).

A similar procedure is implemented in cluster 2: user W3 decodes the signal of user W4 and retransmits it in the second time slot.

The proposed model provides resilience to dynamic line-of-sight blocking by using the time-frequency and energy resources of mobile terminals within clusters, which is critically important for decentralized 5G/6G networks.

7.2. Evaluation of the effectiveness of the M-CO-NOMA algorithm

In the setup mode, the BS performs the following modulation:

- for remote users — on the quadrature QPSK component;
- for near users — on the real component.

This ensures orthogonality of the signals, which allows avoiding interference between user groups.

As a result, near users do not receive interference from the signals of remote users, and SIC operations are performed only for near signals.

Thus, each user needs to perform *N*/2-1 SIC operations, which significantly reduces the computational complexity compared to classical NOMA, where the number of SIC operations is *N*-1.

For example, with four users in NOMA the near user performs 3 SIC operations, in M-CO-NOMA — only 1 operation, that is three times less.

Remote users in both algorithms perform the same number of SIC operations, but in NOMA they encounter additional interference from near users, which is difficult to compensate for due to the low signal power. In M-CO-NOMA, these interferences are eliminated due to orthogonality, which allows reducing interference for remote users by a factor of *N*/2.

In the general case, in NOMA, each user encounters *N*-1 sources of interference, and in M-CO-NOMA — only *N*/2-1, which reduces the total system interference by a factor of 6 for four users.

Figure 3 shows the simulation result of the CO-NOMA-M algorithm.

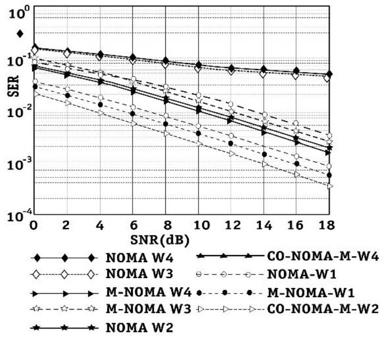

Figure 3: Comparison of SER efficiency for NOMA, M-NOMA and the proposed M-CO-NOMA algorithms

Figure 3 illustrates the comparative curves of the symbol error rate (SER) for three algorithms: classical NOMA algorithm, modulation-oriented M-NOMA algorithm and the proposed M-CO-NOMA one.

MATLAB 2021a environment was used for simulation with the following parameters:

- channel model — Rayleigh fading channel;
- signal loss — 2 units;
- total transmission power — 1 W;
- power distribution coefficients according to the distance to each user:

$a_1 = 0.15$, $a_2 = 0.20$, $a_3 = 0.25$, $a_4 = 0.40$.

The simulation results demonstrate the following:

- user W4 in the CO-NOMA-M system shows better SER performance compared to users W3 in M-NOMA and W4 in M-NOMA;
- user W2 in CO-NOMA-M outperforms W3 in NOMA in decoding accuracy.

Overall, CO-NOMA-M demonstrates superior performance compared to traditional NOMA methods, especially in dynamic environments with high levels of interference. This confirms the feasibility of using CO-NOMA-M to improve interference immunity and reduce SER in promising 5G/6G mobile networks.

8. Information security analysis in NOMA systems

NOMA technology is considered one of the key components of next-generation mobile networks (5G/6G) due to its ability to provide high spectral efficiency and massive simultaneous service to users. However, the implementation of NOMA is accompanied by new challenges in the field of information security, due to the features of the access architecture — in particular, superposition coding and resource sharing.

One of the main threats is signal interception (eavesdropping), which arises due to the open nature of transmission in NOMA. In addition, there is a risk of message substitution, reduced data confidentiality, as well as unauthorized access to information at the physical layer.

Traditional security mechanisms are focused mainly on higher layers of the network model (for example, encryption at the application or network level). However, in the case of NOMA, it is advisable to use technical means of protection at the physical layer, which allow one to neutralize threats at the signal transmission stage. This also corresponds to AI-oriented approaches to radio channel security, where intelligent analysis of signal characteristics and threat conditions supports the design of more resilient wireless communication mechanisms [27].

Effective physical layer security (PLS) solutions include the following:

- Artificial Noise (AN) — creating interference for a potential interceptor without degrading the quality of communication for a legitimate user;
- Dynamic Beamforming — directional signal transmission taking into account the spatial position of users;
- Optimization of power distribution between users with different channel characteristics;
- Coordinated coding and use of multi-user MIMO systems, which allows to increase transmission selectivity and reduce the risk of interception.

Methods for detecting radio signals by estimating their parameters are relevant for identifying abnormal physical-layer conditions in radio channels and supporting further security analysis of wireless communication systems [26]. At the system level, these threats should also be considered within the broader context of socio-cyber-physical systems security, where communication, computation, control, and cybersecurity mechanisms interact within one protected environment [28]. In addition, vulnerability-checking methods for corporate networks are important for assessing weak points in the surrounding infrastructure that may affect the reliability and security of NOMA-based communication systems [29].

Analysis of the proposed NOMA model from the point of view of information security allows one to:

- Identify critical vulnerabilities in the transmission process;
- Assess the effectiveness of technical protection measures;
- Develop directions for improving the system architecture to increase its stability and reliability.

Particular attention should be paid to the integration of PLS solutions into the structure of NOMA systems, which will ensure a balance between performance and security in the conditions of high user density and complex radio environment.

Let us pay some additional attention to physical layer security threats in NOMA systems and methods for their neutralization

In traditional multiple access systems with orthogonal resource allocation (e. g., FDMA, TDMA, OFDMA), there was physical isolation between users, which significantly complicated the possibility of direct data interception. This approach provided a basic level of protection at the physical layer by dividing the frequency, time-frequency or code space.

In contrast, the technology of non-orthogonal multiple access NOMA, which is based on superimposing signals with different power levels for simultaneous data transmission to several users, creates new challenges for physical layer security. The sharing of the spectrum and superposition coding lead to potential system vulnerabilities, in particular the following:

- the possibility of unauthorized signal interception;
- a decrease in the confidentiality of the transmitted information;
- eavesdropping attacks;
- the risk of message substitution or interference in the decoding process.

These threats require specialized solutions focused on physical layer security, which allows ensuring security at the signal transmission stage, supplementing or replacing traditional cryptographic methods that operate at higher levels of the network model.

Table 3 and Table 4 below show the main types of threats and methods for improving physical layer security in NOMA.

Table 3
Main types of threats

Threat Types	Description
Eavesdropping	The use of signal superposition in NOMA means that the weaker user is forced to decode the stronger user's signal first. This increases the risk that an attacker who impersonates the weaker user or has access to the channel will gain unauthorized access to the strong user's data.
Interference Attacks	Vulnerability to targeted jamming by attackers increases because NOMA relies on precise signal power balancing. Intentional jamming of even a portion of the channel can lead to significant errors in multi-user decoding.
Threats from erroneous decoding in SIC	Since SIC is a key mechanism in NOMA receivers, an attacker may attempt to disrupt the process of sequential signal subtraction, leading to data leakage or information substitution.
Exploiting power distribution weaknesses	If the power parameters are incorrectly determined or transmitted without protection, an attacker can use this information to increase the effectiveness of attacks on the channel or organize unauthorized access.
Replay Attacks	An attacker can record the superposition signal and retransmit it to the network, creating a threat to the authenticity and integrity of the information.

Table 4
Methods for improving physical security in NOMA

Methods	Description
Beamforming	The use of multi-beam antenna arrays allows you to focus the signal energy in the direction of legitimate users and minimize the likelihood of its interception. Adaptive beamforming taking into account the location of subscribers reduces the effectiveness of eavesdropping attacks.
Secure Power Allocation	The use of chaotic mappings, pseudo-random symbol permutations, or dynamic modulation parameter changes creates an additional layer of protection. The advantage is the absence of significant computational costs compared to classical cryptographic encryption.
Artificial Noise addition	Optimizing power factors for different users reduces information leakage. The use of machine learning algorithms makes it possible to dynamically adjust parameters to channel conditions and potential threats.
Integration with 6G technologies	The use of intelligent reflective surfaces (IRS) allows one to change the structure of the radio channel to improve the signal-to-noise ratio for a legitimate user and worsen it for an attacker. The synergy of NOMA and quantum-resistant protocols opens up new horizons of physical-level security.

Thus, despite the obvious advantages of NOMA technology — in particular, high spectral efficiency and the ability to mass serve users — it reveals vulnerabilities inherent in its multi-user nature. Resource sharing and superposition coding create conditions for potential threats at the physical level, requiring specialized solutions.

Further development of NOMA systems requires the development of innovative approaches to ensuring information security, in particular the following:

- implementation of physical layer encryption technologies;
- application of dynamic resource management in accordance with channel conditions and threat level;
- integration of adaptive signal processing algorithms capable of responding to changes in network topology and behavior of potential attackers.

These areas are critically important for increasing the stability and reliability of NOMA systems in the context of future generations of mobile communications.

9. Modeling the transmission process in the M-CO-NOMA system

As part of the study, computer modeling of the data transmission process in the proposed M-CO-NOMA system and comparative modeling for classical NOMA were conducted. The main goal was to determine the dependence of the secrecy coefficient, Secrecy Spectral Rate (SSR), on the signal level at the receiver SNR.

In the computer experiment, the following initial modeling parameters were used:

- SSR was defined as $SSR = \max\{0, \log_2(1+SNR_{leg}) - \log_2(1+SNR_{eve})\}$ (bits/s/Hz);
- the SNR range from −10dB to 30dB was modeled and small channel fluctuations were taken into account (Monte Carlo, 200 trials for each SNR);
- for M-CO-NOMA, practical improvements were introduced: amplification of the legitimate channel $G_{leg}=1.5$ (use of retransmission/orthogonality) and attenuation of the channel of the possible interceptor $A_{eve}=0.5$ (beamforming, masking). For the reference NOMA $SNR_{eve} = 0.8 \cdot SNR_{leg}$;
- the average SSR over iterations was calculated for each SNR and a graph was constructed.

For each SNR value, the average SSR value was calculated based on the iteration results, and on the basis of which a graph of dependence was constructed.

Figure 4 presents a graphical comparison of SSR for two systems: classical NOMA and proposed M-CO-NOMA.

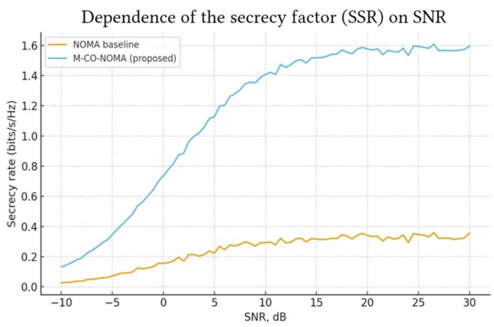

Figure 4: Dependence of the SSR secrecy coefficient on SNR.

The obtained results confirm the significant advantage of the M-CO-NOMA scheme in terms of ensuring the confidentiality of the transmission: the secret transmission rate (SSR) factor in the proposed configuration demonstrates significantly higher values SSR in the entire range of SNR. In particular, at SNR≈10 dB, SSR for M-CO-NOMA is approximately 1.4 bit/s/Hz, while for the basic NOMA it is only about 0.3 bit/s/Hz. This increase is due to the synergy of several key mechanisms: retransmission allows to amplify the legitimate signal, orthogonalization reduces mutual interference, and spatial methods contribute to the attenuation of the signal available for a potential interceptor.

In general, the integration of these technologies in combination with analytical modeling provides a significant increase in the level of physical security of NOMA systems, reducing the risks associated with unauthorized access at the physical transmission layer.

10. Conclusions

In this paper, an improved M-CO-NOMA algorithm is proposed, aimed at increasing the reliability of functioning of decentralized 5G mobile networks in conditions of dynamic blocking of direct visibility during transmission in the terahertz frequency range. Unlike known solutions, the proposed approach combines relaying, modulation and clustering of terminals, which is implemented in two key stages:

- before transmitting the signal into the air, clustering of terminal devices is carried out using the fractal dimension estimation algorithm;

- while forming the general transport signal, the base station modulates the signals of nearby users using the real components of the QPSK constellation, while the signals of distant users — on the quadrature component. This approach ensures orthogonality between groups and reduces the level of interference.

The simulation results confirmed the effectiveness of the algorithm according to the following criteria:

- reduction of the symbol error rate;
- reduction of computational complexity;
- reduction of interference compared to the classical NOMA.
- integration of solutions based on M-NOMA and CO-NOMA opens up new opportunities for stable data transmission in conditions of blocking direct transmission, thanks to auxiliary signal retransmission between subscribers.

In addition, the use of the proposed methods in combination with analytical security models allows to significantly increase the level of security of NOMA systems and reduce the risks of attacks at the physical level, which is critically important for next-generation networks

11. Directions of further scientific work

Further work should be aimed at developing adaptive signal processing algorithms taking into account inter-user interference, improving physical security mechanisms, optimizing energy efficiency and increasing data transfer speed and reducing latency in conditions of high user density.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] 3GPP TS 37.340 V15.2.0: NR: Multi-connectivity; Overall description, Rel. 15, 2018.

[2] D. Moltchanov, A. Samuylov, V. Petrov, et al. Improving Session Continuity with Bandwidth Reservation in mmWave Communications, In: IEEE Wireless Communications Letters, no. 7. 2018. pp. 1-4.

[3] V. Saiko, R. et al., Merezhy mobylnogo zviyazku novogo pokoliniya 4G/5G/6G, Pro format, Kyiv, 2021.

[4] V. Saiko, T. Narytnyk. Model pobudovy bezdrotovoiy teragerzovoiy merezhy z pidvyshchenoyu nadiynistiu zvyazku. Int. Sci. J. Eng. Agric., 2(2), 2023, pp. 166-181. doi:10.46299/j.isjea.20230202.16.

[5] M. Bakulyn, Technologiya NOMA z kodovym rozdylenniyam u 3GPP: 5G abo 6G. T-Comm: Telekomunikaciy i transport, vol. 16, 2022. pp. 4-14.

[6] U. Arachchillage, D. Jayakody, S. Biswash, R. Dinis, Recent Advances and Future Challenges in Non-Orthogonal Multiple Access (NOMA), In: Proceedings of the IEEE 87th Vehicular Technology Conference (WS). Porto. Portugal. 2018.

[7] T. Rappaport, 6G and beyond: Terahertz communications and sensing. Brooklyn 5G Summit Keynote, 2019.

[8] N. Zhang, J. Wang, G. Kang, Y. Liu, Uplink Non-orthogonal Multiple Access in 5G Systems, In: IEEE Communications Letters, vol. 20, no. 3. Mar. 2016, pp. 458-461.

[9] M. El-Sayed, A. Ibrahim, M. Khairy, Power allocation strategies for Non-Orthogonal Multiple Access, In: Proceedings of the International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Cairo. 2016.

[10] Z. Ding, et al., Application of Non-Orthogonal Multiple Access in LTE and 5G Networks, In: IEEE Communications Magazine. vol. 55, no. 2. Feb. 2017, pp. 185-191.

[11] A. Benjebbour, K. Saito, A. Li, Y. Kishiyama, T. Nakamura, Non-orthogonal multiple access (NOMA): Concept, performance evaluation and experimental trials, In: Proceedings of the International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakech. 2015.

[12] S. Islam, N. Avazov, O. Dobre, K. Kwak, Power-Domain Non-Orthogonal Multiple Access (NOMA) 5G Systems: Potentials and Challenges, In: IEEE Communications Surveys and Tutorials, vol. 19, no. 2. Second quarter 2017. pp. 721-742.

[13] M. Jamal, S. Hassan, D. Jayakody, A New Approach to Cooperative NOMA Using Distributed Space Time Block Coding, In: Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Montreal. 2017.

[14] S. Qureshi, S. Hassan, D. Jayakody, Divide-and-Allocate: An Uplink Successive Bandwidth Division NOMA System, Trans. emerg. telecommun. technol., vol. 2. no. 10, 19 Jun. 2012.

[15] P. Xu, Y. Yuan, Z. Ding, X. Dai, R. Schober, On the Outage Performance of Non-Orthogonal Multiple Access with 1-bit Feedback, IEEE Trans. Wirel. Commun., vol. 15, no. 10, Oct. 2016. pp. 6716-6730.

[16] Z. Wang, J. Cao, NOMA-Based Spatial Modulation, IEEE Access, vol. 5. 2017, pp. 3790-3800.

[17] C. Zhong, X. Hu, X. Chen, D. Ng, Z. Zhang, Spatial Modulation Assisted Multi-Antenna Non-Orthogonal Multiple Access, IEEE Wirel. Commun., vol. 25, no. 2. April 2018, pp. 61-67.

[18] X. Wang, J. Wang, L. He, J. Song, Spectral Efficiency Analysis for Downlink NOMA Aided Spatial Modulation with Finite Alphabet Inputs, IEEE Trans. Veh. Technol., vol. 66, no. 11. Nov. 2017, pp. 10562-10566.

[19] Z. Ding, et al., A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends, IEEE J. Sel. Areas Commun., vol. 35, no. 10. Oct. 2017, pp. 2181-2195.

[20] O. Harasymchuk, I. Opirskyy, et al. (2025) Mod. Methods Ensuring Inf. Prot. Cybersecur. Syst. Using Artif. Intell. Blockchain Technol., Kharkiv: Technology Center PC, 132 p. doi:10.15587/978-617-8360-12-2.

[21] Z. Ding, Z. Yang, P. Fan, H. Poor, On the Performance of Non-Orthogonal Multiple Access in 5G Systems with Randomly Deployed Users. IEEE Signal Process. Lett., vol. 21, no. 12. Dec. 2014, pp. 1501-1505.

[22] M. Shahab, S. Shin, On the Performance of a Virtual User-pairing Scheme to Efficiently Utilize the Spectrum of Unpaired Users in NOMA, Phys. Commun., vol. 25, Dec. 2017, pp. 492-501.

[23] O. Harasymchuk, I. Opirskyy, et al. (2025) Intell. Cyber Def. Syst. Detect. Ransomware Prot. Wirel. Netw. Based Artif. Intell. Technol. Kharkiv: Technology Center PC, 182 p. doi:10.15587/978-617-8360-22-1.

[24] A. Morozov, Vvedeniya v teoriyu fraktaliv. M.: Instytut kompyuternych doslidzhein, 2002.

[25] K. Berzh, Teoriya grafiv ta yy zastosuvanniya. M.: Vydavnytstvo inozemnoyi literatury, 1962.

[26] N. Lukova-Chuiko, et al., The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. In: 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 — Proceedings, 67-70. doi:10.1109/ATIT54053.2021.9678856.

[27] O. Partyka, A. Imoize, AI for Radio Channel Security. Handb. Cybersecur. Chall. Solut. Emerg. Technol., 2026. doi:10.1201/9781003640790-16.

[28] S. Yevseiev, Y. Khokhlachova, S. Ostapov, O. Laptiev et al, Models of socio-cyber-physical systems security, Monographs, PC technology center, 2023. doi:10.15587/978-617-7319-72-5.

[29] R. Kyrychok, O. Laptiev, R. Lisnevsky, V. Kozlovsky, V. Klobukov, Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. East. Eur. j. enterp. technol., vol.1№9 (115), 2022, p. 93-101. doi:10.15587/1729-4061.2022.253530.