


Program Współpraca Polska-RPA	RAPORT CZĄSTKOWY z realizacji projektu w ramach programu międzynarodowego Polska-RPA		 Narodowe Centrum Badań i Rozwoju
Nr raportu	IR-RATfor5G-03		
Data aktualizacji raportu:	2022.01.10	Wersja	5
Numer umowy	PL-RPA2/02/RATfor5G+/2019	Akronim	RATfor5G+
Okres realizacji projektu	od 2019.01.01	do	2022.06.30
Tytuł projektu	Technologie dostępu radiowego dla standardu 5G i przyszłych generacji sieci bezprzewodowych		
Tytuł raportu	Przegląd w zakresie bezpieczeństwa systemów opartych o wielodostęp NOMA		

UWAGA: wycinki z przeglądu literatury do dalszej obróbki.

In this section we give an overview of the study of security for NOMA. The overview was performed to give high level understanding of security aspects in NOMA. To fully address the inter-tier and architectural aspects of NOMA, security techniques for NOMA networks have been thoroughly reviewed. The main conclusions of this analysis for the concept of architecture are as follows:

- different types of attacks (passive, active) target the vulnerabilities of the NOMA physical layer,
- the use of jamming / artificial noise and appropriate channel coding techniques allows to reduce the chance of eavesdropping by an unauthorized user (link1, link12, link15, link16),
- appropriate beamforming allows to maintain the correct relationship between the SINR for the NOMA user (legitimate user) and the unauthorized user (eavesdropping user) (link2, link3, link9, link10), as well as beam control in connection with power allocation (link11). The increase in the number of antennas at the base station side has a positive effect on the level of transmission protection against unauthorized users (link17, link21).
- software-defined multi-access techniques have been proposed for NOMA (e.g. SoDeMa) so that it is possible to flexibly switch between different NOMA techniques (power domain, code domain, etc.) - which is important, because of the different computational complexity and spectral efficiency of individual NOMA solutions (link4)
- the use of relay nodes - their configuration and performance are important for the ability to successfully attack infrastructure based on NOMA (link5, link6). The ability to transmit in full-duplex mode can significantly improve the level of transmission security, without consuming transmission resources (link7), similarly, the use of multi-antenna systems and power control in such nodes has a positive effect on the security level (link18). One should consider the effective use of knowledge about their location, inter-layer techniques necessary to increase

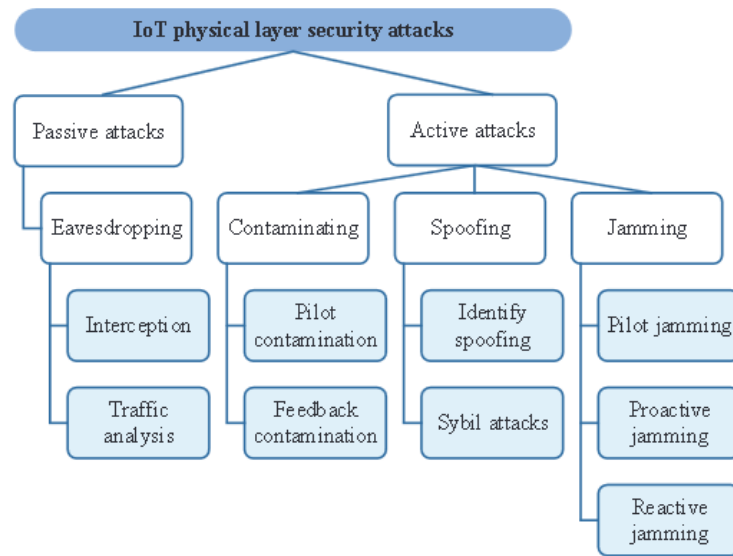
the benefits of using cooperative security techniques. However, hardware aspects may limit the applicability of cooperative techniques (link20).

- appropriate allocation of resources (e.g. joint allocation of power and subcarriers), prevents the implementation of SIC decoding on the side of unauthorized users (link8). For this purpose, game theory techniques are used (link19) or other methods, e.g. application of the chaos theory in modulation techniques (link13, link14) . In particular, the use of quantum security key distribution techniques in NOMA systems is analyzed in (link22).
- authors in [Sec_3] are proposing use of the PLS for power domain NOMA access based HetNet. They are trying to find optimal solution for the optimization problem, by utilizing the monotonic optimization method.

To summarize the energy optimization and task offloading together with the NOMA security aspects – it can be seen that these aspects are very intensively explored by researchers. To fully explore non-functional aspects of NOMA one should consider the complexity dimension of the NOMA related algorithms, and especially the receiver complexity. The promising direction is on one hand to assume more deep-learning networks on the side of receiver (and actually also transmitter) where the need for CSI is decreased by the high prediction/estimation capability of the DL networks. On the other hand MEC based edge servers available in the range of few milliseconds from the NOMA transceiver bring multitude of capabilities to support NOMA processing (task offloading, security support, etc).

NOMA security – state-of-the-art analysis.

- Security for NOMA
 - PHY security in 5G: challenges and opportunities ([link1](#), [link2](#))
 - PHY security
 - PLS solutions of LTE-A require adaptations towards 5G...
 - (mMIMO, NOMA) In the channel training phase, the channel estimation could be compromised by a pilot-contamination attacker, which can imitate and send the same pilot signals as that of legitimate users (LUs)



- Fig. 2. Security threats in 5G IoT physical layer.
- secrecy capacity of a non-orthogonal multiple access system ([link3](#))
 - *secrecy capacity for the transmission of the signal $x_1(t)$ to UE1 is defined as the difference between the channel capacity of the main channel from BS to UE1 and the eavesdropper channel from BS to E*
 - „power allocation for maximizing secrecy rate”
 - problem of maximizing the secrecy sum rate at all users subject to a quality of service (QoS) constraint of the codeword rate at each user was tackled in [21]. Note that the **perfect secrecy rate/capacity considered in [21] can be ensured only when the transmitter has the perfect knowledge on the eavesdropper’s channel state information** (CSI), which is difficult to realize in practice.
 - this motivates us to design the secure NOMA schemes for the practical scenario where the **transmitter does not know the eavesdropper’s instantaneous channel information**. In this scenario, the perfect secrecy rate is usually not achievable, and hence, we do not take it as the secrecy metric. Instead, we use the secrecy outage probability to measure the secrecy performance of the system

- “[...] based on the locations of the users and eavesdropper, the secrecy capacity is analyzed to assess the level of security provided to the legitimate users in the presence of an eavesdropper. Here, the decoding thresholds of legitimate users and eavesdropper are also included in the analysis of the secrecy capacity. Through numerical results, the effects of network parameters on system performance are assessed as well as the the superiority of NOMA in terms of secrecy capacity over traditional orthogonal multiple access”
- high spectral efficiency secure access (HSESA) scheme based on dual nonorthogonal is proposed first in this paper. The scheme which can be recognized as a dual nonorthogonal scheme is designed by the nonorthogonal multiplexing and nonorthogonal multiple access. [\(link4\)](#)
 - high spectral efficiency secure access (HSESA) is proposed based on OFDMA and has more advanced properties;
 - HSESA **jams the reception of the eavesdropper** by using security matrix to improve physical layer security
 - By changing the bandwidth compression factor, HSESA can be **flexibly switched between orthogonality and nonorthogonality** during the multiplexing process
- PHY security enhancements with game-theory “In order to enhance the secrecy performance, a two-phase harvest-and-jam null-steering jamming technique is deployed” [\(link5\)](#)
- Exploiting Inter-User Interference for Secure Massive Non-Orthogonal Multiple Access [\(link6\)](#) – “[...] We first analyze the **secrecy performance** of the considered secure massive access system and derive a closed-form expression for the ergodic **secrecy rate**”
- Secure Transmission to the Strong User in Non-Orthogonal Multiple Access “[...] We aim to maximize the achievable secrecy energy efficiency by **jointly designing the SC assignment, user pair scheduling and power allocation.**” [\(link7\)](#)
- NOMA system, where a transmitter sends confidential messages to multiple users in the presence of an external eavesdropper [...] **optimal designs of decoding order, transmission rates, and power allocated to each user** are investigated [\(link8\)](#)
 - we design the NOMA scheme that **minimizes the total transmit power subject to the QoS constraint and the secrecy constraint**
- Pilot Contamination Attack Detection for NOMA in Mm-Wave and Massive MIMO 5G Communication [\(link9\)](#)
- **Cellular NOMA secrecy**
 - Rank Based Secrecy Rate Improvement using NOMA for Ultra Dense Network [\(link10\)](#) --- CAUTION: interesting channel modeling for different scenarios (Speed, LOS/NLOS,

- Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming ([link11](#))
 - only a few studies have applied jamming techniques in NOMA systems for secrecy consideration
 -
 - Secrecy Outage Performance Analysis for Cooperative NOMA Over Nakagami- m Channel ([link12](#))
- **Secure transmission in NOMA with relays**
 - Trusted relays ([link13](#))
 - Untrusted Relay ([link14](#))
 - Two categories of users trusted/untrusted ([link15](#))
 - Our aim is to maximize the **sum secrecy rate of the network**.
 - SIC Avoidance at Eavesdroppers
 - Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay ([link16](#))
- **SWIPT (power transfer in NOMA) - ([link17](#))**
 - where the legitimate user with a stronger channel condition acts as an energy harvesting relay to help that with a weaker channel condition.
 - Solid and **comprehensive works about PLS and energy harvesting with 5G wireless technologies are still missing**, whereas their specific features have not yet been exploited to improve the secrecy performance and harvested energy.
- **Secure beamforming**
 - beamforming approach may not be successful in dense situations where vehicular users are typically focused...
 - Beamforming can be used to reduce risk of eavesdropping
 - for IoT ([link18](#))
 - for downlink ([link19](#))
 - Secure Downlink Massive MIMO NOMA Network in the Presence of a Multiple-Antenna Eavesdropper ([link20](#))
 - Secure Transmit Antenna Selection Protocol for MIMO NOMA ([link21](#))
 - Downlink MISO Nonorthogonal Multiple Access Systems ([link22](#))
 - Null-Steering Beamforming for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System ([link23](#))
 - On Secure NOMA Systems With Transmit Antenna Selection Schemes ([link24](#))
 -
- **Secure transmission with randomized constellation rotation**
 - For DL and SCMA ([link25](#))
- **Location assisted security in 5G**
 - location distinguishability of transmitters could help 5G IoT networks to mitigate the risk of active attacks, **where the users can effectively distinguish other different users with the location information**, which will be a powerful tool to counter active attack
- **Exploiting Jamming in Secure Cooperative NOMA**
 - Adaptive jamming ([link26](#))
 - Tiered 5G Wireless Networks With Cooperative Jamming ([link27](#))

- Cooperative Relaying and Jamming Strategies for Physical Layer Security ([link28](#))
 - exploiting cooperative communication techniques to further improve the security. Many studies are showing that the cooperation between the legitimate nodes of a network can significantly enhance their secret communications, relative to the non-cooperative case.
- Cooperative relaying and jamming ([link29](#))
- **Legitimate eavesdropper (user pairing – one can eavesdrop the other)**
 - The weak user data can be intercepted by the strong user since the strong user needs to decode the weak user's message for successive interference cancellation operation in NOMA ([link30](#))

SOTA papers – source listing:

1. **Paper1: Enhancing security of SIC algorithm on non-orthogonal multiple access (NOMA) based systems** ([link](#))
 - Non-orthogonal multiple access (NOMA) is a promising candidate among potential nominees for future radio access. NOMA adopts the principle of successive interference cancellation (SIC) algorithm at the receiver's side to segregate user's information. However, during SIC process, information of the user(s) with weaker channel gain is extracted by user(s) with stronger channel gain. It can raise major security concerns, e.g. session hijacking, eavesdropping, identity theft, and others, for users with weaker channel gains. Therefore, this research aims to analyze and verify a secure SIC algorithm for NOMA based systems. This research proposes and demonstrates the SIC scheme to enhance security on the user's side by making use of MAC address and IMEI that are devoted to a smartphone as distinctive keys. This research shown that the proposed scheme can improve security in terms of confidentiality time and secrecy capacity.
2. **Paper2: Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations** ([link](#))
 - Non-Orthogonal Multiple Access (NOMA) has been recognized as one of the most significant enabling technologies for future wireless systems due to its eminent spectral efficiency, ability to provide an additional degree of freedom for Ultra Reliable Low Latency Communications (URLLC) and grant free random access. Meanwhile, Physical Layer Security (PLS) has got much attention for future wireless communication systems due to its capability to provide security without relying on traditional cryptography based algorithms. In this article, security design requirements for NOMA and solutions provided by PLS to fulfill these requirements are discussed. The merits and challenges arising from employing PLS to NOMA are identified. Finally, future recommendations and prospective solutions are also presented
3. **Paper3: Analysis of Security Gaps in 5G Communication using LDPC Codes and NOMA** ([link](#))
 - Advance communication systems such as fifth generation (5G) and 5G+ expect to deploy the security solutions for securing the communication networks. Finding the optimum size of the security gap is a challenging problem in the large scale networks. In this paper, the parity check matrix (H) of low-density parity check (LDPC) considered for determining the security gap is analyzed with the higher rate LDPC coding schemes and different size of frames. Here, optimum LDPC decoding is

considered as a method. Especially, the physical layer is investigated with two different high-rate codes and simulated to find the optimum size of security gaps for better security. Also, non-orthogonal multiple access (NOMA) is employed to enhance the security solution. Thus, optimum security gap is possible when suitable NOMA is employed in the physical layer of the 5G communication system. As expected in this research conclusion, simulation results show that the security gap decreases when frame size is increased

- “[...] Although this paper aims to reduce the security gap (SG) which provides secure communication between sender and receiver, NOMA optimizes the SG and secrecy capacity to improve LDPC based physical layers. The larger frame size of LDPC code provides better SGs and security regions which helps to provide secure communication and transmission. In the 5G physical layer, NOMA and LDPC provide a better secrecy capacity and SG respectively.”

4. **Paper4: Physical Layer Security for Cooperative NOMA Systems** ([link](#))

- In this correspondence, we investigate the physical layer security for cooperative non-orthogonal multiple access (NOMA) systems, where both amplify-and-forward (AF) and decode-and-forward (DF) protocols are considered. More specifically, some analytical expressions are derived for secrecy outage probability (SOP) and strictly positive secrecy capacity (SPSC). Results show that AF and DF almost achieve the same secrecy performance. Moreover, asymptotic results demonstrate that the SOP tends to a constant at high signal-to-noise ratio (SNR). Finally, our results show that the secrecy performance of considered NOMA systems is independent of the channel conditions between the relay and the poor user

5. **Paper5: Device to device comms underlying and uplink SCMA system** ([link](#))

- Device-to-device (D2D) communication has been a potential solution to improve spectral efficiency of cellular systems due to frequency resource sharing. This paper considers D2D communications underlying an uplink cellular system enabling sparse code multiple access (SCMA) technology, where the base station (BS) can decode the signals of cellular users without mutual interference. The demands for high data rate as well as low latency in massive connectivity is the main challenging requirement in D2D communications, along with ensuring the quality of service (QoS) for the on-running cellular user equipment (CUEs). To tackle the problem, the BS is designed to first assign the codewords in a codebook to CUEs based on the lower bound of the achievable CUE rates, so that the sum rate (SR) of CUEs is maximized. With the usage of mutual-interference suppression in the SCMA-enabled system, the BS then attempts to maximize the SR of D2Ds in a transmission block through a joint power and resource allocation subject to the QoS requirements for both CUEs and D2Ds. This task is formulated as a mixed-integer non-convex programming. We propose a low-complexity two-phase algorithm of joint heuristic and inner approximation method to efficiently solve the problem. The numerical results verify that the codebook assignment problem based on the lower bound of SR is easily solved, and the proposed algorithm to maximize the SR of D2Ds outperforms existing methods

6. **Paper6: Securing Downlink Non-Orthogonal Multiple Access Systems by Trusted Relays** ([link](#))

- A downlink single-input single-output non-orthogonal multiple access system is considered in which a base station (BS) is communicating with two legitimate users in the presence of an external eavesdropper. A group of trusted cooperative half-duplex relay nodes, powered by the BS, is employed to assist the BS's transmission. The goal is to design relaying schemes such that the legitimate users' secrecy rate region is maximized subject to a total power constraint on the BS and the relays' transmissions. Three relaying schemes are investigated: cooperative

jamming, decode-and-forward, and amplify-and-forward. Depending on the scheme, secure beamforming signals are carefully designed for the relay nodes that either diminish the eavesdropper's rate without affecting that of the legitimate users, or increase the legitimate users' rates without increasing that of the eavesdropper. The results show that there is no relaying scheme that fits all conditions; the best relaying scheme depends on the system parameters, namely, the relays' and eavesdropper's distances from the BS, and the number of relays. They also show that the relatively simple cooperative jamming scheme outperforms other schemes when the relays are far from the BS and/or close to the eavesdropper

7. **Paper7: Simultaneous Wireless Information and Power Transfer at 5G New Frequencies: Channel Measurement and Network Design** ([link](#))

- Simultaneous wireless information and power transfer (SWIPT) technique offers a potential solution to ease the contradiction between high data rate and long standby time in the fifth generation (5G) mobile communication systems. In this paper, we focus on the SWIPT network design and optimization with 5G new frequencies. To design an efficient SWIPT network, we first investigate the propagation properties of 5G low-frequency (LF) and high-frequency (HF) channels. Specifically, a measurement campaign focusing on 3.5 GHz and 28 GHz is conducted in both outdoor and outdoor-to-indoor scenarios. Motivated by the measurement results, we design a dual-band SWIPT network, where the HF band is used for short-distance information delivery, while the LF band is used for short-distance energy transfer and long-distance information delivery. The designed network has a win-win architecture which can enhance the throughput of cell-edge users and improve the energy-harvesting efficiency of cell-center users. To further boost the network performance, we devise a joint power-and-channel allocation algorithm, which has the advantages of low complexity and fast convergence. Finally, simulation results demonstrate that the designed dual-band network outperforms the conventional single-band network in terms of energy-harvesting efficiency and user fairness, and the proposed algorithm can further upgrade the network performance significantly.

8. **Paper8: Secure Beamforming Design in Relay-Assisted Internet of Things** ([link](#))

- A secure downlink transmission system which is exposed to multiple eavesdroppers and is appropriate for Internet of Things (IoT) applications is considered. A worst case scenario is assumed, in the sense that, in order to enhance their interception ability all eavesdroppers are located close to each other, near the controller and collude to form joint receive beamforming. For such a system, a novel cooperative nonorthogonal multiple access (NOMA) secure transmission scheme for which an IoT device with a stronger channel condition acts as an energy harvesting relay in order to assist a second IoT device operating under weaker channel conditions, is proposed and its performance is analyzed and evaluated. A secrecy sum rate (SSR) maximization problem is formulated and solved under three constraints: 1) transmit power; 2) successive interference cancellation; and 3) quality of service. By considering both passive and active eavesdroppers scenarios, two optimization schemes are proposed to improve the overall system SSR. On the one hand, for the passive eavesdropper scenario, an artificial noise-aided secure beamforming scheme is proposed. Since this optimization problem is nonconvex, instead of using traditional but highly complex, brute-force 2-D search, it is conveniently transformed into a convex one by using an epigraph reformulation. On the other hand, for the active multi-antennas eavesdroppers' scenario, the orthogonal-projection-based beamforming scheme is considered, and by employing the successive convex approximation method, a suboptimal solution is proposed. Furthermore, since for single antenna transmission the orthogonal-projection-based scheme may not be applicable a simple power control scheme is proposed. Various performance evaluation results obtained by means

of computer simulations have verified that the proposed schemes outperform other benchmark schemes in terms of SSR performance.

9. **Paper9: Secure Transmission With Randomized Constellation Rotation for Downlink Sparse Code Multiple Access System ([link](#))**

- Sparse code multiple access (SCMA) is a promising candidate air interface of next-generation mobile networks. In this paper, we focus on a downlink SCMA system where a transmitter sends confidential messages to multiple users in the presence of external eavesdroppers. Consequently, we develop a novel secure transmission approach over physical layer based on a highly structured SCMA codebook design. In our proposed scheme, we rotate the base constellations (BCs) with random angles by extracting channel phases from the channel state information. By employing randomized constellation rotation, the security of downlink SCMA can be ensured. In addition, a tight SCMA upper bound is introduced to guide the design of the encrypted codebook. As a result, we propose an approach to avoid the significant error rate performance loss caused by using codebooks that are designed using our method. The proposed upper-bound-aided codebook design scheme can select relatively good codebooks with low complexity. By combining SCMA codebook design and secure communication, our scheme ensures security for massive quantities of users with low encrypted and decrypted complexity at the cost of transmission rate and possible error rate performance loss. Moreover, the proposed scheme can achieve robustness against channel estimation errors. Analyses and Monte Carlo simulations confirm the effectiveness of our scheme.

10. **Paper10: Physical Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities ([link](#))**

- The fifth generation (5G) wireless technologies serve as a key propellant to meet the increasing demands of the future Internet-of-Thing (IoT) networks. For wireless communication security in 5G IoT networks, physical layer security (PLS) has recently received growing interest. This article aims to provide a comprehensive survey of the PLS techniques in 5G IoT communication systems. The investigation consists of four hierarchical parts. In the first part, we review the characteristics of 5G IoT under typical application scenarios. We then introduce the security threats from the 5G IoT physical layer and categorize them according to the different purposes of the attacker. In the third part, we examine the 5G communication technologies in 5G IoT systems and discuss their challenges and opportunities when coping with physical-layer threats, including massive multiple-input-multiple-output (MIMO), millimeter wave (mmWave) communications, non-orthogonal multiple access (NOMA), full-duplex technology, energy harvesting (EH), visible light communication (VLC) and unmanned aerial vehicle (UAV) communications. Finally, we discuss open research problems and future works about PLS in the IoT system with technologies of 5G and beyond.

11. **Paper11: Exploiting Adaptive Jamming in Secure Cooperative NOMA with an Untrusted Relay ([link](#))**

- We study secure communications with an untrusted relay for a cooperative non-orthogonal multiple access (NOMA) system, where a base station (BS) serves a near user (NU) and a far user (FU) by the NOMA principle, and transmission between BS and FU is aided by an untrusted relay. We propose an adaptive jamming scheme to enhance transmission security, in which FU is asked to adaptively emit a jamming signal to confuse the untrusted relay. The transmission rate for jamming is designed to ensure that only NU can decode the jamming signal correctly, and the jamming power is optimized for maximizing the secrecy sum rate. We analyze the security performance of the proposed scheme and derive the ergodic secrecy sum rate and its scaling law. Simulation results are presented to validate the effectiveness of the proposed adaptive jamming scheme.

12. **Paper12: Non-Orthogonal Multiple Access: A Unified Perspective ([link](#))**

- Non-orthogonal multiple access (NOMA) is a promising technique for future mobile communication systems, which can approach multiuser channel capacity by sharing the same time-frequency resources with multiple users. In this article, we provide a unified framework for NOMA and review the principles of various NOMA schemes in different domains with the objective of creating a unified framework. A systematic performance comparison of different NOMA schemes regarding their peak-to-average power ratio, receiver complexity, latency, grant-free access, user load, and peak throughput is also provided for different application scenarios. Relying on our unified framework, we generalize the current understanding of the NOMA principle from the conventional code and power domains to the spatial domain as well as to their hybrids and to the networking domain. Finally, the challenges in terms of resource allocation, channel estimation, security, system flexibility, and implementation issues are also discussed

13. **Paper13: Secure Transmission in Non-Orthogonal Multiple Access Networks With an Untrusted Relay** ([link](#))

- This letter investigates secure transmission in non-orthogonal multiple access networks with an untrusted amplify-and-forward relay. In order to enhance secrecy performance, a cooperative jamming strategy is designed to confuse the relay. The new exact and asymptotic expressions for effective secrecy throughput (EST) are derived over Nakagami-m fading channels, which demonstrates that jamming plays an important role for obtaining nonzero EST and should be carefully designed for achieving better secrecy performance. In addition, simulations are presented to provide some insights into parameters, i.e., transmit powers and fading parameters, on the secrecy performance.

14. **Paper14 Robust Physical Layer Security for Power Domain Non-orthogonal Multiple Access-Based HetNets and HUDNs: SIC Avoidance at Eavesdroppers** ([link](#))

- In this paper, we investigate the physical layer security in downlink of Power Domain Non-Orthogonal Multiple Access (PD-NOMA)-based heterogeneous cellular network (HetNet). In this paper, we assume two categories of users are available: 1) Trusted users, 2) untrusted users (eavesdroppers) at which transparency of users is not clear for the BSs, i.e., they are potential eavesdroppers. Our aim is to maximize the sum secrecy rate of the network. To this end, we formulate joint subcarrier and power allocation optimization problems to increase sum secrecy rate. Moreover, we propose a novel scheme at which the eavesdroppers are prevented from doing Successive Interference Cancellation (SIC), while legitimate users are able to do it. In practical systems, perfectly availability of all eavesdroppers' Channel State Information (CSI) at legitimate transmitters are impractical. Also CSIs of legitimate users may be also imperfect due to the error of channel estimation. Hence, we study two cases of CSI availability, 1) Perfect CSI of nodes (legitimate users and eavesdroppers) are available at the BSs, 2) imperfect CSI of nodes are available at the BSs. Since the proposed optimization problems are non-convex, we adopt the well-known iterative algorithm called Alternative Search Method (ASM). In this algorithm, the optimization problems are converted to two subproblems, power allocation and subcarrier allocation. We solve the power allocation problem by the Successive Convex Approximation approach and solve the subcarrier allocation subproblem, by exploiting the Mesh Adaptive Direct Search algorithm (MADS). Moreover, in order to study the optimality gap of the proposed solution method, we apply the monotonic optimization method. Moreover, we evaluate the proposed scheme for secure massive connectivity in Heterogeneous Ultra Dense Networks (HUDNs). Furthermore, we investigate multiple antennas base stations scenario in this literature. Finally, we numerically compare the proposed ...

15. **Paper15: Outage probability and secrecy capacity of a non-orthogonal multiple access system** ([link](#))
 - In this paper, we analyze the outage probability and secrecy capacity of a non-orthogonal multiple access (NOMA) system in the presence of an eavesdropper. In order to enhance spectral efficiency, a base station communicates with two users simultaneously in the same frequency band by superimposing the transmit signals to the users in the power domain. Specifically, the user with the worse channel conditions is allocated higher power such that it is able to directly decode its signal from the received superimposed signal. At the user with the better channel conditions, the interference due to NOMA is processed by successive interference cancellation. Given these system settings and accounting for decoding thresholds, we analyze the outage probability of the NOMA system over Rayleigh fading channels. Furthermore, based on the locations of the users and eavesdropper, the secrecy capacity is analyzed to assess the level of security provided to the legitimate users in the presence of an eavesdropper. Here, the decoding thresholds of legitimate users and eavesdropper are also included in the analysis of the secrecy capacity. Through numerical results, the effects of network parameters on system performance are assessed as well as the superiority of NOMA in terms of secrecy capacity over traditional orthogonal multiple access.
16. **Paper16: Secure Downlink Massive MIMO NOMA Network in the Presence of a Multiple-Antenna Eavesdropper** ([link](#))
 - In this paper, the secrecy performance of a massive multiple-input multiple-output (MIMO) non-orthogonal multiple access (NOMA) network is studied in the presence of a multiple-antenna eavesdropper. The ergodic secrecy rates for the downlink transmission in the considered system are derived to provide important insights. Then, by using these results, a joint power allocation scheme is proposed for both uplink training and downlink data transmission phases to maximize the sum ergodic secrecy rates. Because the utility function of interest is non-concave and the involved constraints are non-convex, a new iterative algorithm is proposed, which can find at least a local optimum. The obtained results reveal that the secrecy performance of NOMA networks benefits from deploying massive MIMO techniques. They also indicate that the proposed optimization algorithm enhances the secrecy performance of the considered system.
17. **Paper17: On the Secrecy Capacity of 5G MmWave Small Cell Networks** ([link](#))
 - In the next generation 5G millimeter-wave (mmWave) small cell networks, mmWave communication will play a critical role, as there is a lot more open bandwidth in high frequencies. The rapid growth of mmWave systems poses a variety of challenges in PHY security. This article investigates those challenges in the context of several 5G mmWave small cell communication technologies, including MIMO, NOMA, and so on. In particular, we introduce an RT-based 5G mmWave small cell communication channel model, and reveal that the secrecy capacity in mmWave band widely depends on the richness of the RF environment through numerical experiments.
18. **Paper18: High-throughput, cyber-secure multiuser superposition covert avionics system** ([link](#))
 - With the ever-growing attention on advanced cyber threats to aerospace systems, research activities on cyber resiliency have accelerated in both academic and industrial communities. For example, in mobile wireless devices, machine-to-machine architectures, as well as broadband transport computing technology, protection and security are a shared responsibility and liability across both government and commercial sectors [1]. Airborne networks are envisioned as an infrastructure consisting of Internet protocol-based airborne nodes and onboard platforms that provide interconnectivity between terrestrial and space networks [2]. The airborne networks will be critical for avionics systems communication,

navigation, display, and control [3]. As a consequence, airborne systems, as well as satellite communication (SATCOM) systems, require fast and robust data transfer in a hostile action or adverse conditions.

19. **Paper19: Secure Communications in Tiered 5G Wireless Networks With Cooperative Jamming** ([link](#))

- Cooperative jamming is deemed as a promising physical layer-based approach to secure wireless transmissions in the presence of eavesdroppers. In this paper, we investigate cooperative jamming in a two-tier 5G heterogeneous network (HetNet), where the macrobase stations (MBSs) at the macrocell tier are equipped with large-scale antenna arrays to provide space diversity and the local base stations (LBSs) at the local cell tier adopt non-orthogonal multiple access (NOMA) to accommodate dense local users (LUs). In the presence of imperfect channel state information, we propose three robust secrecy transmission algorithms that can be applied to various scenarios with different security requirements. The first algorithm employs robust beamforming (RBA) that aims to optimize the secrecy rate of a macro user (MU) in a macrocell. The second algorithm provides robust power allocation (RPA) that can optimize the secrecy rate of an LU in a local cell. The third algorithm tackles a robust joint optimization (RJO) problem across tiers that seek the maximum secrecy sum rate of a target MU and a target LU robustly. We employ convex optimization techniques to find feasible solutions to these highly non-convex problems. The numerical results demonstrate that the proposed algorithms are highly effective in improving the secrecy performance of a two-tier HetNet

20. **Paper20: A Zero-Sum Game Approach for Non-Orthogonal Multiple Access Systems: Legitimate Eavesdropper Case** ([link](#))

- In this paper, secure communication in non-orthogonal multiple access (NOMA) downlink system is considered wherein two NOMA users with channel gain difference are paired in each transmission slot. The user with poor channel condition (weak user) is entrusted, while the user with good channel condition (strong user) is a potential eavesdropper. The weak user data can be intercepted by the strong user since the strong user needs to decode the weak user's message for successive interference cancellation operation in NOMA. To impair strong user's eavesdropping capability, weak user's information-bearing signal is merged with an artificial signal (AS). Thus, the eavesdropping process requires extra decoding step at higher power level. The secrecy outage probability of the weak user is derived and provided in closed-form expression. The weak user faces a choice between transmitting the information-bearing signal with the total power and the deploying the AS technique, whereas the strong user can choose whether to eavesdrop the weak user's message or not. To investigate users' power-secrecy tradeoffs, their interactions are modeled as a non-cooperative zero-sum game. The existence of Nash equilibria (NEs) of the proposed game is first analyzed, and pure and mixed-strategy NE profiles are provided. In addition, numerical simulations are conducted to validate the analytical results and to prove that AS-Aided proposed scheme enhances the secrecy performance of NOMA systems while maintaining the NOMA superiority over OMA systems.

21. **Paper21 A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security** ([link](#))

- Physical layer security (PLS) has been extensively explored as an alternative to conventional cryptographic schemes for securing wireless links. Of late, the research community is actively working towards exploiting cooperative communication techniques to further improve the security. Many studies are showing that the cooperation between the legitimate nodes of a network can significantly enhance their secret communications, relative to the non-cooperative case. Motivated by the importance of this class of PLS systems, this paper provides

a comprehensive survey of the recent works on cooperative relaying and jamming techniques for securing wireless transmissions against eavesdropping nodes which attempt to intercept the transmissions. First, it provides a in-depth overview of various secure relaying strategies and schemes. Next, a review of recently proposed solutions for cooperative jamming techniques has been provided with an emphasis on power allocation and beamforming techniques. Then, the latest developments in hybrid techniques, that use both cooperative relaying and jamming, are elaborated. Finally, several key challenges in the domain of cooperative security are presented along with an extensive discussion on the applications of cooperative security in key enablers for 5G communications, such as non-orthogonal multiple access (NOMA), device-to-device (D2D) communications, and massive multiple-input multiple-output (MIMO) systems.

22. **Paper22:** SWIPT-Aided Secure Beamforming Design for Downlink Cooperative NOMA Systems

[\(link\)](#)

- In this paper, we consider a downlink non-orthogonal multiple access system, in which base station emits secret messages to two legitimate users in the presence of multiple eavesdroppers, and all the eavesdroppers collude to form joint receive beamforming, in an attempt to enhance their interceptions. In light of this, a cooperative simultaneous wireless information and power transfer non-orthogonal multiple access secure transmission protocol is proposed, where the legitimate user with a stronger channel condition acts as an energy harvesting relay to help that with a weaker channel condition. Following this, a secrecy sum rate maximization problem is formulated, under the constraints of transmit power and quality of service requirements. By taking both the single-antenna and multiple-antenna scenarios into account, two different optimization schemes, i.e., the power control scheme, and the null-space beamforming design scheme, are presented to maximize the secrecy sum rate. Numerical results verify the superiority of our proposed schemes over the benchmarks

23. **Paper23:** Secure Transmit Antenna Selection Protocol for MIMO NOMA Networks Over Nakagami-m Channels [\(link\)](#)

- In this paper, we consider a multi-input multioutput (MIMO) nonorthogonal multiple access (NOMA) network consisting of one source and two legitimate users (LUs), so-called near and far users according to their distances to the source, and one passive eavesdropper, over Nakagami-m fading channels. Specifically, we investigate the cases where the signals of the far user might or might not be successfully decoded at the eavesdropper and the near user. Thus, we aim to design a transmit antenna selection (TAS) secure communication protocol for the network; where, two TAS solutions, namely Solutions I and II, are proposed. Specifically, Solutions I and II focus on maximizing the received signal power between the source and the near user, and between the source and the far user, respectively. Accordingly, exact and asymptotic closed-form expressions for the secrecy outage probability of the LUs and the overall system are derived. Our analytical results corroborated by the Monte Carlo simulation indicate that the secrecy performance could be significantly improved by properly selecting the power allocation coefficients and increasing the number of antennas at the source and the LUs. Interestingly, solution II is shown to provide a better overall secrecy performance over solution I.

24. **Paper24:** On Fair Secure Rate Maximization for NOMA Downlinks using Quantum Key Distribution

[\(link\)](#)

- Quantum key distribution (QKD) ensures two individuals to establish a secret key by exchanging photon quantum states, which ensures the security and can be promising to assist future wireless communications. In this paper, we investigate a quantum-assisted wireless communication system, where QKD is first performed to generate secure key, and wireless

communication is conducted for data transmission via nonorthogonal multiple access (NOMA). To guarantee user fairness, the aim is to maximize the minimal secure rate among all users. To solve this nonconvex problem, an iterative algorithm with low complexity is proposed, where the closed-form solution is obtained in each iteration. Simulation results are illustrated to show the superiority of the proposed algorithm.

25. **Paper25: High Spectral Efficiency Secure Communications With Nonorthogonal Physical and Multiple Access Layers** ([link](#))

- Internet of Things as an essential integrated part of the future wireless communication system provides ubiquitous connectivity and information exchange to enable a range of applications and services, which has triggered spectrum resource pressure, multiple access, bandwidth efficiency, and security issues. Focusing on these issues, a high spectral efficiency secure access (HSESA) scheme based on dual nonorthogonal is proposed first in this paper. The scheme which can be recognized as a dual nonorthogonal scheme is designed by the nonorthogonal multiplexing and nonorthogonal multiple access. Particularly, HSESA scheme is equipped with secure multiplexing by using security matrix to improve physical layer security. Moreover, spectral efficiency analysis is given and the throughput of HSESA has been derived. Moreover, iterative detection (ID) and maximum likelihood (ML) are, respectively, combined with message passing algorithm (MPA) as detection schemes, and their respective performance advantages are analyzed. Simulation results show that the detection scheme using ID combined with MPA has lower complexity, while ML combined with MPA has better bit error rate performance, and the spectral efficiency is also enhanced by the proposed HSESA.

26. **Paper26: Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems** ([link](#))

- In this paper, we consider a cellular downlink multiple-input-single-output (MISO) nonorthogonal multiple access (NOMA) secure transmission system, where users are grouped as multiple clusters. Each cluster consists of a central user and a cell-edge user. The central user is an entrusted user, and the cell-edge user is a potential eavesdropper. We focus on the secure beamforming and power allocation design optimization problem which maximizes the sum achievable secrecy rate of central users subject to the transmit power constraint at the base station and transmission rate requirements at cell-edge users. The problem is nonconvex because of coupling optimization variables in the considered fractional quadratically constrained quadratic programming. We propose an alternating optimization-based solution and a constrained concave-convex procedure-based solution to the considered problem. Simulation results demonstrate that our proposed NOMA schemes outperform the conventional orthogonal multiple access scheme.

27. **Paper27: NOMA-Based Resource Allocation and Mobility Enhancement Framework for IoT in Next Generation Cellular Networks** ([link](#))

- With the unprecedented technological advances witnessed in the last two decades, more devices are connected to the Internet, forming what is called the Internet of Things (IoT). The IoT devices with heterogeneous characteristics and the quality of experience (QoE) requirements may engage in the dynamic spectrum market due to the scarcity of radio resources. We propose a framework to efficiently quantify and supply radio resources to the IoT devices by developing intelligent systems. The primary goal of this paper is to study the characteristics of the next generation of cellular networks with non-orthogonal multiple access (NOMA) to enable connectivity to clustered IoT devices. First, we demonstrate how the distribution and QoE requirements of IoT devices impact the required number of radio resources in real time. Second, we prove that using an extended auction algorithm by implementing a series of complementary functions enhance the radio resource utilization efficiency. The results show a substantial reduction in the number of sub-carriers required

when compared with conventional OMA and the intelligent clustering is scalable and adaptable to the cellular environment. Ability to move spectrum usages from one cluster to other clusters after borrowing when a cluster has fewer users or move out of the boundary is another soft feature that contributes to the reported radio resource utilization efficiency. Moreover, the proposed framework provides IoT service providers cost estimation to control their spectrum acquisition to achieve the required quality of service with a guaranteed bit rate (GBR) and non-GBR

28. **Paper28: A Game-Theoretical Modelling Approach for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System** ([link](#))

- This paper investigates the physical layer security of a downlink non-orthogonal multiple access (NOMA) communication system, wherein a base station is communicating with two paired active users in the presence of an eavesdropper and multiple idle nodes (helpers). In order to enhance the secrecy performance, a two-phase harvest-and-jam null-steering jamming technique is deployed. In the first phase, the base station provides the helper with power in addition to active users and eavesdropper's information via simultaneous wireless information and power transfer technique. The helpers exploit the harvested energy and the information received in the first phase to build a null-steering beamformer and jam the eavesdropper, during the information exchange between the base station and the legitimate users in the second phase. A game theory is introduced to the proposed scheme, and the base station-helpers interactions are modeled as a Stackelberg game, where the helpers play the leader role and the base station is the follower. The utility functions of both the leader and follower are formed, and the Stackelberg equilibrium is reached by means of the backward induction technique. The proposed scheme demonstrates better secrecy performance when compared with the artificial noise-aided secure NOMA system.

29. **Paper29: Exploiting Inter-User Interference for Secure Massive Non-Orthogonal Multiple Access** ([link](#))

- This paper considers the security issue of the fifth-generation wireless networks with massive connections, where multiple eavesdroppers aim to intercept the confidential messages through active eavesdropping. To realize secure massive access, non-orthogonal channel estimation and non-orthogonal multiple access techniques are combined to enhance the signal quality at legitimate users, while the inter-user interference is harnessed to deliberately confuse the eavesdroppers even without exploiting artificial noise. We first analyze the secrecy performance of the considered secure massive access system and derive a closed-form expression for the ergodic secrecy rate. In particular, we reveal the impact of some key system parameters on the ergodic secrecy rate via asymptotic analysis with respect to a large number of antennas and a high transmit power at the base station. Then, to fully exploit the inter-user interference for security enhancement, we propose to optimize the transmit powers in the stages of channel estimation and multiple access. Finally, extensive simulation results validate the effectiveness of the proposed secure massive access scheme.

30. **Paper30: Physically Securing Energy-Based Massive MIMO MAC via Joint Alignment of Multi-User Constellations and Artificial Noise** ([link](#))

- This paper investigates the artificial noise (AN) aided physical layer security (PLS) for energy-based massive multi-input multi-output multi-access channels with finite-alphabet data inputs, where both the legitimate base station (Bob) and the passive eavesdropper (Eve) are equipped with large antenna arrays and each user has multiple antennas. For such system, the main challenge is how to allocate power between the transmitted constellation of finite size and AN for both interference management and PLS enhancement. To this end, we first characterize a distance-optimal (DO) constellation structure that maximizes the minimum

Euclidean distance of the received signals with energy detection. It turns out that the DO multiuser constellations constitute a commonly-used pulse amplitude modulation (PAM) constellation at the receiver side. Then, we specifically design an energy-efficient PAM-constellation alignment to form a received sizeable PAM constellation by adaptively aligning the power of multi-users' PAM sub-constellations. This design provides us with a new finite-alphabet non-orthogonal multi-access scheme as well as with a stepped water filling (SWF) power allocation between the constellation and AN for each user, which can provide the power-domain freedom for PLS. To spatially exploit this freedom, a SWF-based product-constant AN generation algorithm is developed such that the product of Bob's channel and the AN is a constant which can be inferred by Bob, and the channel-noise product for Eve cannot be uniquely determined, even for noise-free channels. Simulations indicate that for SWF, Bob's error rate will vanish when the number of the receiver antennas goes to large, but Eve's error rate has a non-vanishing lower-bound, even with an unlimited number of antennas. In addition, PAMA, as a new finite-alphabet NOMA scheme, has significant advantages in both security and communication error performance over the time division multi-access.

31. **Paper31: Secure Transmission to the Strong User in Non-Orthogonal Multiple Access** ([link](#))

- With non-orthogonal multiple access (NOMA) in a passive eavesdropping scenario, we tackle the maximization of the secrecy rate for the strong user subject to a maximum allowable secrecy outage probability while guaranteeing a constraint on the transmission rate to the weak user. For the first time, the dependence between the eavesdropper's ability to conduct successive interference cancellation and her channel quality is considered. We determine the exact optimal power allocation and redundancy rate, based on which the cost of security in terms of the reduction in the strong user's secrecy rate is examined, and the benefits of NOMA for secure transmissions are revealed.

32. **Paper32: Energy Efficient Resource Allocation for Secure NOMA Networks** ([link](#))

- In this paper, we investigate the joint subcarrier (SC) assignment and power allocation problem for non-orthogonal multiple access (NOMA) amplify-and-forward two-way relay wireless networks. We aim to maximize the achievable secrecy energy efficiency by jointly designing the SC assignment, user pair scheduling and power allocation. Assuming the perfect knowledge of the channel state information (CSI) at the relay station, we propose a low-complexity subcarrier assignment scheme (SCAS-1), which is equivalent to many-to-many matching games, and then SCAS-2 is formulated as a secrecy energy efficiency maximization problem. The secure power allocation problem is modeled as a convex geometric programming (GP) problem, and then solved by interior point methods. Simulation results demonstrate that the effectiveness of the proposed SSPA algorithms.

33. **Paper33: On the Design of Secure Non-Orthogonal Multiple Access Systems** ([link](#))

- This paper proposes a new design of non-orthogonal multiple access (NOMA) under secrecy considerations. We focus on a NOMA system, where a transmitter sends confidential messages to multiple users in the presence of an external eavesdropper. The optimal designs of decoding order, transmission rates, and power allocated to each user are investigated. Considering the practical passive eavesdropping scenario where the instantaneous channel state of the eavesdropper is unknown, we adopt the secrecy outage probability as the secrecy metric. We first consider the problem of minimizing the transmit power subject to the secrecy outage and quality of service constraints, and derive the closed-form solution to this problem. We then explore the problem of maximizing the minimum confidential information rate among users subject to the secrecy outage and transmit power constraints, and provide an iterative algorithm to solve this problem. We find that the secrecy outage constraint in the studied problems does not change the optimal decoding order for NOMA, and one should increase the

power allocated to the user whose channel is relatively bad when the secrecy constraint becomes more stringent. Finally, we show the advantage of NOMA over orthogonal multiple access in the studied problems both analytically and numerically.

34. **Paper34: Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay** ([link](#))

- In a downlink non-orthogonal multiple access (NOMA) system, the reliable transmission of cell-edge users cannot be guaranteed due to severe channel fading. On the other hand, the presence of eavesdroppers can severely threaten the secure transmission due to the open nature of wireless channel. Thus, a two-user NOMA system assisted by a multi-antenna decode-and-forward relay is considered in this paper, and a two-stage jamming scheme, full-duplex-jamming (FDJam), is proposed to ensure the secure transmission of NOMA users. In the FDJam scheme, using full-duplex, the relay transmits the jamming signal to the eavesdropper while receiving confidential messages in the first stage, and the base station generates the jamming signal in the second stage. Furthermore, we eliminate the self-interference and the jamming signal at the relay and the legitimate node, respectively, through relay beamforming. To measure the secrecy performance, analytical expressions for secrecy outage probability (SOP) are derived for both the cellcenter and cell-edge users, and the asymptotic SOP analysis at high transmit power is presented as well. Moreover, two benchmark schemes, half-duplex-jamming and full-duplex-nojamming, are also considered. Simulation results are presented to show the accuracy of the analytical expressions and the effectiveness of the proposed scheme.

35. **Paper35: Transmit Beamforming for Layered Physical Layer Security** ([link](#))

- In this paper, we propose a novel layered physical layer security model, which is the extension of the traditional physical layer security to the domain of multiple-layer information security. It has a hierarchical information security structure that every transmitted message has a security level, while every user has a security clearance. Users can only decode the messages with security levels lower than or equal to their clearance, otherwise they will be deemed as eavesdroppers. Based on the framework of the layered information security and assuming perfect channel state information of all users, an artificial-noise-aided optimal beamforming scheme is proposed to minimize the total transmit power at the base station, while satisfying the minimum secrecy rate requirements of all secret messages. Due to the intrinsic complexity of the formulated nonconvex problem, a safe and convex reformulation based on the first-order Taylor series expansion method is proposed to generate a tractable approximation. A successive convex approximation-based algorithm is then proposed, which solves a series of second-order cone problems with convergence to the stationary point of the original problem. We also consider the imperfect channel state information case, and then propose a worst-case robust design to overcome the influence of channel uncertainties. Semi-definite relaxation method and S-procedure are utilized to get a computationally efficient lower bound of the intractable power minimization problem. Moreover, we investigate the application of the suboptimal zero-forcing-based beamforming scheme in the system to tradeoff the achievable performance and the computational complexity. Simulation results are provided to demonstrate the effectiveness of our proposed schemes.

36. **Paper36: Rank Based Secrecy Rate Improvement using NOMA for Ultra Dense Network** ([link](#))

- Non-orthogonal multiple access (NOMA) has emerged as an integral component for the future cellular networks. The purpose to install more small cells in the vicinity of macrocell is to provide seamless and ubiquitous coverage to a huge density of users. Hence, security becomes an important aspect which needs to resolve for users under critically acclaimed applications. The conventional encryption techniques and physical layer security measures may not be feasible always in Ultra Dense Network due to limited resources. Thus, NOMA based multiple

access (MA) technique is emphasized to ensure reliability and confidentiality to users under dense picocells deployment. This paper sheds light on the security challenges of vehicular users and examines the impact of NOMA-based MA technique on overall performance in comparison to the conventional approach. We design a training model to determine the density of vehicular users in a given picocell, before assigning power and resources. However, the proposed approach takes care of low mobile vehicular users as the eavesdropper tends to impact them more. The operation of NOMA enabled users under the influence of intracellular and intercellular interference is also discussed. The results demonstrate that NOMA is successful in achieving a high sum rate for vehicular users by efficiently exploiting the resources in the power domain. To end this, we also compare the NOMA based solution for the same scenario with the conventional approaches.

37. **Paper37: Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming** ([link](#))

- This paper analyzes the secrecy capacity of a cooperative relaying system using non-orthogonal multiple access (NOMA). A new cooperative NOMA scheme is proposed, where the source actively sends jamming signals while the relay is forwarding, thereby enhancing the security of intended communication links. Closed-form expressions for the ergodic secrecy rate are derived in the presence of an eavesdropper. Asymptotic approximate expressions for the ergodic secrecy rate are established in high signal-to-noise ratio (SNR) regime, which provides insights on secure NOMA transmission. Numerical results reveal the critical condition, under which NOMA is able to outperform orthogonal multiple access (OMA) in terms of secrecy rate. The proposed NOMA scheme can improve the secrecy rate by about 78.1%.

38. **Paper38: Secrecy Outage Performance Analysis for Cooperative NOMA Over Nakagami- m Channel** ([link](#))

- In this paper, we investigate the secrecy outage performance of a typical cooperative downlink non-orthogonal multiple access (NOMA) system over Nakagami-m fading channel, in which the base station transmits a superimposed signal to two users via a relay. First, the secrecy outage behavior of the considered system over Nakagami-m fading channel under three wiretapping cases, e.g., one eavesdropper (Eve), non-colluding and colluding eavesdroppers, are studied, and both analytical and asymptotic expressions for the secrecy outage probability are derived. Next, by considering the availability of Eves' channel state information, we adopt the two-stage relay selection (RS) strategy to improve the system's secrecy outage performance. Finally, simulation results are provided to corroborate the accuracy of our derived expressions. The results show that: 1) there exists secrecy performance floor for cooperative NOMA system, and it was determined by the weak user's secrecy requirement and the channel conditions of the Eves; 2) the two-stage RS scheme can increase the secrecy outage performance significantly under three wiretapping cases; 3) the secrecy performance of cooperative NOMA network is superior to that of orthogonal multiple access network on the condition of low and medium signal-to-noise ratio regions.

39. **Paper39 : Null-Steering Beamforming for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System** ([link](#))

- This paper addresses enhancing the physical layer security of a downlink non-orthogonal multiple access systems. The proposed scheme consists of a base station, multiple legitimate users, and an eavesdropper. In each transmission slot, the base station communicates with two paired users, under the malicious attempts of the eavesdropper to intercept the information messages. In order to impair the eavesdropper's channel without affecting the legitimate paired users, a jamming signal is injected into the system by means of null-steering beamforming. In null-steering precoding, the jamming signal is directed toward the malicious

node while being suppressed in the legitimate users' directions. Null-steering jamming is exploited in two different mainstreams, namely, self-cooperative and nonself-cooperative jamming. In the self-cooperative strategy, the base station implements the null-steering beamformer to transmit the jamming signal during the information exchange with the legitimate users, whereas in the nonself-cooperative jamming scheme, idle legitimate users (helpers) utilize the harvested energy in the first phase to transmit the jamming signal toward the eavesdropper in the second phase during the base station communication with the legitimate users. The outage behavior in the two considered scenarios is investigated, and the secrecy outage probability for both paired users is derived and provided in closed-form expressions. Numerical simulations are performed to validate the derived analytical results and to compare the two considered strategies secrecy performance. Comparisons yield that self-cooperative jamming has better outage behavior unless the number of helpers in the system is large enough.

40. **Paper40** : On Secure NOMA Systems With Transmit Antenna Selection Schemes ([link](#))

- This paper investigates the secrecy performance of a two-user downlink non-orthogonal multiple access systems. Both single-input and single-output and multiple-input and single-output systems with different transmit antenna selection (TAS) strategies are considered. Depending on whether the base station has the global channel state information of both the main and wiretap channels, the exact closed-form expressions for the secrecy outage probability (SOP) with suboptimal antenna selection and optimal antenna selection schemes are obtained and compared with the traditional space-time transmission scheme. To obtain further insights, the asymptotic analysis of the SOP in high average channel power gains regime is presented and it is found that the secrecy diversity order for all the TAS schemes with fixed power allocation is zero. Furthermore, an effective power allocation scheme is proposed to obtain the non-zero diversity order with all the TAS scheme

41. **Paper41** : Pilot Contamination Attack Detection for NOMA in Mm-Wave and Massive MIMO 5G Communication ([link](#))

- Power non-orthogonal multiple access (NOMA) has been considered as a key technology in 5G communication. In this paper, we introduce the problem of pilot contamination attack (PCA) on NOMA in millimeter-wave (mmWave) and massive MIMO 5G communication. Due to the new characteristics of NO-MA such as superposed signals with multi-users, PCA detection face new challenges. By harnessing the sparseness and statistics of mmWave and massive MIMO virtual channel, we propose two simple but effective PCA detection schemes for NOMA tackling static and dynamic environments, respectively. For the static environment, the problem of PCA detection is formulated as a binary hypothesis test of virtual channel sparseness. For the dynamic environment, the statistic of the peak in virtual channel is leveraged to distinguish the contamination state from the normal state. A peak estimation algorithm and a machine learning based detection scheme are proposed to achieve high detection performance. Simulation results evaluate and confirm the effectiveness of the proposed detection schemes. The detection rate can approach 100% with 10^{-3} false alarm rate in static environment and above 95% in dynamic environment under various system parameters.

42. **Paper42** : Enhancing Physical Layer Security for NOMA Transmission in mmWave Drone Networks ([link](#))

- Physical layer security (PLS) is critically important for emerging wireless communication networks to maintain the confidentiality of the information of legitimate users. In this paper, we investigate enhancing PLS in an unmanned aerial vehicle (UAV) based communication network where a UAV acting as an aerial base station (BS) provides coverage in a densely

packed user area (such as a stadium or a concert area). In particular, non-orthogonal multiple access (NOMA) together with highly-directional multi-antenna transmission techniques in mmWave frequency bands are utilized for improving spectral efficiency. In order to achieve PLS against potential eavesdropper attacks, we introduce a protected zone around the user region. However, limited resource availability refrain protected zone being extended to cover the entire eavesdropper region. Hence, we propose an approach to optimize the protected zone shape (for fixed area) at each UAV-BS hovering altitude. The associated secrecy performance is evaluated considering the secrecy outage and sum secrecy rates. Numerical results reveal the importance of protected zone shape optimization at each altitude to maximize NOMA secrecy rates

43. **Paper43** :Improving Physical Layer Security of NOMA Networks by Using Opportunistic Scheduling ([link](#))

- In this paper, we study how to improve physical layer security capability of multiple near users and multiple far users non-orthogonal multiple access (NOMA) networks. To this end, we propose an opportunistic user scheduling scheme, named the best-secure-near-user best-secure-far-user (BSNBSF) scheme. The BSNBSF aims to select the best near-far user pair, whose data transmission is the most robust against the interception of an eavesdropper. In order to facilitate the performance analysis of the proposed user scheduling scheme in terms of secrecy outage probability (SOP), we derive an exact closed-form expression and a tight approximate closed-form expression for the SOP of the selected near and far users, respectively. Numerical results show that the BSNBSF scheme significantly improves the secrecy outage performance NOMA networks compared to that of the random near user and random far user selection scheme. Additionally, discussions on the complicate convex characteristic of the total SOP with respect to the power allocation coefficients and the impact the number of near and/or far users are provided.

Physical Layer Security Approaches in 5G Wireless Communication Networks

0. NOMA: Physical layer security for 5G non-orthogonal multiple access in large-scale networks
 - In this paper, the physical layer security of applying non-orthogonal multiple access (NOMA) in large-scale networks is investigated. In the considered scenario, both the NOMA users and eavesdroppers are spatially randomly deployed
1. Beam forming: Privacy Preservation via Beamforming for NOMA
 - In this paper, we propose two schemes based on beamforming optimization for NOMA that can enhance the security of a specific private user while guaranteeing the other users' quality of service (QoS).
2. Artificial-Noise-Aided Optimal Beamforming in Layered Physical Layer Security
 - Focusing on the basic two-layer unicast system, we propose an artificial-noise-aided optimal beamforming scheme to maximize the higher level information security performance while adhering to the low-level information secrecy rate constraint.
3. Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT
 - In order to improve the security of the primary network, an artificial-noise-aided cooperative jamming scheme is proposed. Our simulation results show that the proposed cooperative jamming scheme succeeds in establishing secure communications and NOMA is capable of outperforming the conventional orthogonal multiple access in terms of its power efficiency.
4. Transmit Beamforming for Layered Physical Layer Security

- Based on the framework of the layered information security and assuming perfect channel state information of all users, an artificial noise aided optimal beamforming scheme is proposed to minimize the total transmit power at the base station, while satisfying the minimum secrecy rate requirements of all secret messages.
5. Beamforming Design and Power Allocation for Secure Transmission With NOMA
 - novel beamforming design to enhance physical layer security of a non-orthogonal multiple access (NOMA) system with the aid of artificial noise (AN). The proposed design uses two factors to balance the useful signal strength and interference at the strong and weak users, which is a generalized version of the existing beamforming designs in the context of physical layer security for NOMA.
 6. Secure Beamforming Design in Relay-Assisted Internet of Things
 - A secure downlink transmission system which is exposed to multiple eavesdroppers and is appropriate for Internet of Things (IoT) applications is considered.
 7. Secure Beamforming for MIMO-NOMA-Based Cognitive Radio Network
 - In this letter, a down-link cascaded transmitting zero-forcing-beamforming (ZFBF) technique is proposed to secure communications in a two-cell multiple-input multiple-output (MIMO) NOMA-based CRN. The proposed technique protects the information from illegitimate users (eavesdroppers) within the same and adjacent cells.
 8. Secure Beamforming in Downlink MIMO Nonorthogonal Multiple Access Networks
 - we consider a cellular downlink multiple-input-multiple-output nonorthogonal multiple access (NOMA) secure transmission network, which consists of a base station, a central user, and a cell-edge user. The base station and two users are all equipped with multiple antennas. The central user is an entrusted user and the cell-edge user is a potential eavesdropper. We focus on secure beamforming optimization problem, which maximizes achievable secrecy rate of the central user subject to transmit power constraint at the base station and transmission rate requirement at the cell-edge user.
 9. Inter-beam Interference Cancellation and Physical Layer Security Constraints by 3D Polarized Beamforming in Power Domain NOMA Systems
 - The security in the physical (PHY) layer in order to achieve confidential and authentic communication is also an important consideration. The proposed scheme checks the PHY layer security constraints on the number of users served per beam. In simulations, the robustness of the proposed scheme allows the average half power beam-width (HPBW) to be brought to about 20° for different steps in HPBW and for different user densities.
 10. Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems
 - In this paper, we consider a cellular downlink multiple-input-single-output (MISO) nonorthogonal multiple access (NOMA) secure transmission system, where users are grouped as multiple clusters. Each cluster consists of a central user and a cell-edge user. The central user is an entrusted user, and the cell-edge user is a potential eavesdropper. We focus on the secure beamforming and power allocation design optimization problem which maximizes the sum achievable secrecy rate of central users subject to the transmit power constraint at the base station and transmission rate requirements at cell-edge users.
 11. Privacy Protection via Beamforming Optimization in MISO NOMA Networks

- In this paper, we propose a scheme based on beamforming optimization for the downlink NOMA that can enhance the security of a specific private user while guaranteeing other users' quality of service (QoS).

Jamming/chaos/modulation

12. Exploiting Adaptive Jamming in Secure Cooperative NOMA with an Untrusted Relay
 - We propose an adaptive jamming scheme to enhance transmission security, in which FU is asked to adaptively emit a jamming signal to confuse the untrusted relay.
13. An Uplink Non-Orthogonal Multiple Access Scheme Having Physical Layer Security Based on Chaos Modulation
 - Non-orthogonal multiple access (NOMA) scheme is a typical core technology for 5G. On the other hand, we had proposed earlier a chaos multiple-input multiple-output (C-MIMO) transmission scheme that harnesses the strengths of the chaos communication system. C-MIMO exhibits channel coding effect and physical layer security based on a common key encryption that helps realize a secure wireless transmission. Furthermore, based on the C-MIMO, we had proposed a downlink chaos NOMA transmission scheme that realizes physical layer security in NOMA. However, in the conventional studies, an uplink transmission is not considered yet. Therefore, in this paper, we propose an uplink chaos NOMA transmission scheme using C-MIMO to realize a secure and large- capacity uplink transmission. The performance of the proposed scheme is evaluated through numerical simulation
14. Chaos MIMO-based Downlink Non-orthogonal Multiple Access Scheme With Physical Layer Security
 - To meet these requirements, we propose a chaos multiple-input multiple output (C-MIMO) scheme that realizes both physical layer security and channel coding gain. In this paper, we apply the principle of C-MIMO to the NOMA scheme, and propose a chaos NOMA scheme that achieves higher-capacity, enabling a secure downlink wireless communication system
15. Artificial Jamming Assisted Secure Transmission for MISO-NOMA Networks
 - In the scheme, the transmit power of artificial jamming is maximized, with its received power at each receiver higher than that of other users. Thus, the jamming signal can be eliminated via successive interference cancellation before others, and the eavesdropping can be disrupted effectively.
16. Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming
 - A new cooperative NOMA scheme is proposed, where the source actively sends jamming signals while the relay is forwarding, thereby enhancing the security of intended communication links. Closed-form expressions for the ergodic secrecy rate are derived in the presence of an eavesdropper. Asymptotic approximate expressions for the ergodic secrecy rate are established in high signal-to-noise ratio (SNR) regime, which provides insights on secure NOMA transmission.
17. Chaos MIMO-based Downlink Non-orthogonal Multiple Access Scheme With Physical Layer Security
 - To meet these requirements, we propose a chaos multiple-input multiple output (C-MIMO) scheme that realizes both physical layer security and channel coding gain. In this paper, we apply the principle of C-MIMO to the NOMA scheme, and propose a chaos NOMA scheme that achieves higher-capacity, enabling a secure downlink wireless communication system

18. Securing Downlink Massive MIMO-NOMA Networks With Artificial Noise
 - In this paper, we focus on securing the confidential information of massive multiple-input multiple-output (MIMO) non-orthogonal multiple access (NOMA) networks by exploiting artificial noise (AN).
19. Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex
 - In this paper, we develop a non-orthogonal multiple access (NOMA)-based two-way relay network with secrecy considerations, in which two users wish to exchange their NOMA signals via a trusted relay in the presence of single and multiple eavesdroppers. To ensure secure communications, the relay not only forwards confidential information to the legitimate users but also keeps emitting jamming signals all the time to degrade the performance of any potential eavesdropper
20. Secure Communications in Tiered 5G Wireless Networks With Cooperative Jamming
 - In this paper, we investigate cooperative jamming in a two-tier 5G heterogeneous network (HetNet), where the macrobase stations (MBSs) at the microcell tier are equipped with large-scale antenna arrays to provide space diversity and the local base stations (LBSs) at the local cell tier adopt non-orthogonal multiple access (NOMA) to accommodate dense local users (LUs).
21. Physically Securing Energy-Based Massive MIMO MAC via Joint Alignment of Multi-User Constellations and Artificial Noise
 - This paper investigates the artificial noise (AN) aided physical layer security (PLS) for energy-based massive multi-input multi-output multi-access channels with finite-alphabet data inputs, where both the legitimate base station (Bob) and the passive eavesdropper (Eve) are equipped with large antenna arrays and each user has multiple antennas.
22. Jammer-aided Secure Communications for Cooperative NOMA Systems
 - This letter investigates a jammer-aided cooperative nonorthogonal multiple access (NOMA) system, where one relay is used to deliver information and other relays are acted as jammers. Two simple relay selection (RS) strategies, e.g., random RS and max-min RS, are considered in this paper.
23. NOMA Aided Interference Management for Full-Duplex Self-Backhauling HetNets
 - In this letter, we address this issue by developing a two-tier non-orthogonal multiple access (NOMA) scheme together with efficient power control to enable aggressive frequency reuse and alleviate co-channel interference. For the considered multi-tier and multi-cell NOMA scenario, we formulate a power minimization problem, and develop an efficient algorithm with guaranteed convergence to enable optimal power control, such that users' data demand is satisfied and backhauling bottleneck is avoided.

SWIPT

24. Resource Allocation for Secure MISO-NOMA Cognitive Radios Relying on SWIPT
 - Cognitive radio (CR) and non-orthogonal multiple access (NOMA) are two promising technologies in the next generation wireless communication systems. The security of a NOMA CR network (CRN) is important but lacks of study. In this paper, a multiple-input single-output NOMA CRN relying on simultaneous wireless information and power transfer is studied. In order to improve the security of both the primary and secondary network, an artificial noise-aided cooperative jamming scheme is proposed.
25. Secrecy Analysis and Learning-Based Optimization of Cooperative NOMA SWIPT Systems

- This paper considers the link security aspect of energy harvesting cooperative NOMA users. In particular, the near user applies the decode-and-forward (DF) protocol for relaying the message of the source node to the far user in the presence of an eavesdropper.
26. SWIPT-Aided Secure Beamforming Design for Downlink Cooperative NOMA Systems
- In this paper, we consider a downlink non-orthogonal multiple access system, in which base station emits secret messages to two legitimate users in the presence of multiple eavesdroppers, and all the eavesdroppers collude to form joint receive beamforming, in an attempt to enhance their interceptions
27. Optimization for Maximizing Sum Secrecy Rate in SWIPT-Enabled NOMA Systems
- In this paper, we study secrecy simultaneous wireless information and power transfer (SWIPT) in downlink non-orthogonal multiple access (NOMA) systems comprising a base station (BS), multiple information receivers (IRs), and multiple energy receivers (ERs) that have potential to wiretap the IRs
28. Two-Stage Relay Selection for Enhancing Physical Layer Security in Non-Orthogonal Multiple Access
- To safeguard the legitimate communications against eavesdropping, we propose a novel two-stage secure relay selection (TSSRS) with a non-orthogonal multiple access (NOMA) scheme to maximize the capacity of one source-destination pair, while guaranteeing the successful communication of the other source-destination pair.
29. Analysis of Uplink NOMA in Cellular IoT: A Physical Layer Security Perspective
- this paper mainly studies the physical layer security problem in the non-orthogonal multiple access (NOMA) system of simultaneous wireless information and power transfer (SWIPT) in the downlink channel.
30. Downlink Non-Orthogonal Multiple Access Systems With an Untrusted Relay
- A downlink single-input single-output (SISO) non-orthogonal multiple access (NOMA) system in which a base station (BS) is communicating with two users is considered. An untrusted half-duplex relay node is available to assist with the BS's transmission. The BS uses superposition coding to transmit messages, and the relay employs either a compress-and-forward or an amplify-and-forward scheme to communicate with the users.