**Noname manuscript No.**
(will be inserted by the editor)

# Survey on Physical Layer Security for 5G Wireless Networks

**José David Vega Sánchez**[1] · **Luis Urquiza-Aguiar**[1] · **Martha Cecilia Paredes Paredes**[1] · **Diana Pamela Moya Osorio**[2]

Received: date / Accepted: date

**Abstract** Physical layer security is a promising approach that can benefit traditional encryption methods. The idea of physical layer security is to take advantage of the propagation medium's features and impairments to ensure secure communication in the physical layer. This work introduces a comprehensive review of the main information-theoretic metrics used to measure the secrecy performance in physical layer security. Furthermore, a theoretical framework related to the most commonly used physical layer security techniques to improve secrecy performance is provided. Finally, our work surveys physical layer security research over several enabling 5G technologies, such as massive multiple-input multiple-output, millimeter-wave communications, heterogeneous networks, non-orthogonal multiple access, and full-duplex. We also include the key concepts of each of the technologies mentioned above. Also identified are future fields of research, and technical challenges of physical layer security.

**Keywords** 5G systems · full-duplex · heterogeneous networks · massive MIMO · millimeter-Wave · non-orthogonal multiple access · physical layer security techniques

José David Vega Sánchez
jose.vega01@ epn.edu.ec

Luis Urquiza-Aguiar
luis.urquiza@epn.edu.ec

Martha Cecilia Paredes Paredes
cecilia.paredes@epn.edu.ec

Diana Pamela Moya Osorio
diana.moyaosorio@oulu.fi

[1]Departamento de Electrónica, Telecomunicaciones y Redes de Información, Escuela Politécnica Nacional (EPN), Quito, 170525, Ecuador. The authors gratefully acknowledge the financial support provided by the Escuela Politécnica Nacional, for the development of the project PIGR-19-06. José David Vega Sánchez is the recipient of a teaching assistant fellowship from Escuela Politécnica Nacional for doctoral studies in Electrical Engineering.
[2]Centre for Wireless Communications (CWC), University of Oulu, Oulu, 90014, Finland. The work of Diana Pamela Moya Osorio was funded by the Academy of Finland 6Genesis Flagship under Grant 318927 and FAITH project under Grant 334280.

## 1 Introduction

The increasing demands for wireless applications and the rapid growth of connected users have saturated the capacity of current wireless communication systems. These fundamental problems motivate researchers and network designers to provide novel solutions that guarantee ultra-high data rates, ultra-wide radio coverage, a massive number of efficiently connected devices, ultra-low latency, and efficient energy consumption. In this sense, the fifth generation of wireless networks (5G) foresees great advances in solutions that satisfy these stringent requirements by employing intelligent and efficient technologies [1]. Accordingly, 5G must be prepared to tackle major challenges concerning the reliability, security, and efficiency of the network. Specifically, the security paradigm protecting the confidentiality of wireless communication is one of the core problems to be considered in 5G networks [2]. Due to the propagation medium's broadcast nature, wireless transmissions are exposed to both jamming and eavesdropping attacks. The former, also known as a denial of service (DoS) is a usual attack against security in the physical layer of wireless networks. To mitigate the interference generated by the DoS, researchers devote their efforts

in ($i$) spread spectrum communications that are a common defense against DoS in wireless systems, and ($ii$) receiver filters that attenuate the jamming signals in the legitimate user [3]. In the latter, non-authorized users attempt to intercept the confidential information by decoding its received signal. To face this issue, physical layer security (PLS) emerges as a promising approach to provide secure wireless communications against eavesdropping by exploiting the physical characteristics of the wireless channels [4].

Based on the preceding, the goal of this work is to provide a comprehensive survey of PLS on enabling technologies for 5G. Firstly, we review the two main types of attacks against security at the physical layer of wireless systems. Next, the main PLS performance metrics are introduced, including secrecy capacity, secrecy outage probability (SOP), alternative secrecy outage formulation, fractional equivocation, average information leakage rate, intercept probability, probability of strictly positive secrecy capacity (SPSC), and the secrecy throughput (ST). Then, a theoretical framework on the PLS techniques commonly used to improve the secrecy performance is revisited. Next, we review the basic concepts of emerging 5G technologies. In particular, we focus on the following: massive MIMO, millimeter-wave (mm-Wave) communications, heterogeneous networks (HetNets), non-orthogonal multiple access (NOMA), and full-duplex (FD). Subsequently, we summarize the latest PLS research advances on the aforementioned 5G technologies.

The remainder of this paper is organized as follows. Section 2 introduces the key concepts of both jamming and eavesdropping attacks. Section 3 presents some fundamentals for PLS and reviews the main secrecy performance metrics. The PLS techniques are introduced in Section 4. Section 5 summarizes concepts of promising 5G technologies and presents the recent advances in PLS research on these key 5G technologies. Section 6 presents some of the open challenges in wireless security communications, and provides some concluding remarks.

## 2 Wireless Security Attacks and Countermeasures

In this section, we focus on discussing wireless security attacks and their countermeasures. Although the slope of this paper is how to face eavesdropping attacks through PLS, we briefly summarize the pivotal aspects of jamming attacks.

### 2.1 Jamming Attacks

DoS attack occurs when a malicious node tries to block legitimate communication by causing intentional interference in the main channel[1]. In a successful DoS attack, network services are not available to legitimate users, causing the system to stop working correctly. Generally, jamming begins during the transmission of either data or pilot signals [5]. Different classifications of DoS attack strategies based on their functionality are available in the literature. Basically, the DoS attack can be divided into constant jammer, deceptive jammer, random jammer, and reactive jammer[2] [7]. In order to counteract the DoS attacks, the research community has proposed several mitigation techniques. Among these defense mechanisms stand out spread spectrum techniques and jamming filtering at the receiver [5]. In the first one, the original signal is expanded into a wider frequency band. This process prevents unauthorized users from knowing that communication between the legitimate pair is in progress. The most widely used spread spectrum approaches in wireless communications are direct sequence extended-spectrum (DSSS) and frequency hopping spread spectrum (FHSS) [6]. However, both DSSS and FHSS are spectrally inefficient, since the spread spectrum-based techniques require a wideband spectrum. Hence, these approaches have to overcome various challenges to be candidate techniques that provide security in 5G networks. Concerning the Jamming filtering at the receiver, the main idea is to use a special receiver filter that separates the desired signal from interference signals [5]. The essential drawback of this approach is that the filter order must be high to perform successfully. This fact renders high computational complexity. To circumvent such limitations, many techniques have been proposed as defense schemes against DoS attacks, such as machine learning, compressing sensing, and estimation based detection method [8]. To be specific, learning technology achieves the desirable security through repeated trial-and-error exploration in a random network environment with different jamming models. In Table 1, we list the latest papers on jamming mitigation techniques.

### 2.2 Eavesdropping Attacks

As mentioned above, wireless communications are vulnerable to eavesdropping due to the broadcast nature of

[1] It is worth mentioning that each layer of the wireless protocol stack is vulnerable to different types of DoS attacks. In this section, we focus on the DoS attack in the physical layer.

[2] A complete information of different types of jammers can be found in [6].

| Reference | System Model | Jamming Defence Mechanism |
|---|---|---|
| F. Wang et al. [9] | SISO channel in the presence of a jammer | Deep Reinforcement Learning |
| A. Alagil et al. [10] | SISO channel in the presence of a jammer | Randomized Positioning DSSS |
| N. Van Huynh et al. [11] | SISO channel in the presence of a jammer | Deep Reinforcement Learning |
| W. Li et al. [12] | SISO channel in the presence of a jammer | Q Learning Algorithm |
| Z. Valkova-Jarvis et al. [13] | SISO channel in the presence of a jammer | First-Order Notch Adaptive Filter |

**Table 1** Mitigation techniques against jamming attacks.

radio propagation. Traditionally, cryptographic methods have been used for protecting confidential information against eavesdroppers [14]. The main cryptographic approaches are symmetric-key cryptography and public-key cryptography. The basic idea of the symmetric-key encryption is that the plain-text to be transmitted is first encrypted using a secret key that is previously shared with the legitimate receiver. In this scenario, even if the eavesdropper intercepts the encrypted plain-text, it cannot recover the plain-text without knowing the secret key. The main issue in this scheme is the secret key distribution between the legitimate parties. Conversely, public-key cryptography does not have to distribute secret keys, but the generation of such keys relies on mathematical cryptographic algorithms. In this system, the security is compromised when (*i*) any person discovers an efficient method to solve the mathematical problem, (*ii*) the public-key is deciphered using a brute-force attack [15]. Unlike these security systems based on higher layer cryptographic mechanisms [16], PLS uses the inherent randomness (e.g., noise and fading) of the wireless channel to ensure secure communications in the physical layer [2]. In particular, PLS offers a significant advantage comparing cryptographic algorithms, since it does not rely on computational complexity. Therefore, the security level achieved will not be affected even if the eavesdropper has unlimited computing capabilities. These features contrast with encryption-based approaches, which are based on the idea that eavesdropper has reduced computational capabilities to solve hard mathematical problems in limited periods [17]. Based on the above considerations, the integration of PLS with cryptographic techniques (e.g., authentication and key generation) is envisioned as a powerful approach to secure confidential communications in future wireless networks [18]. In this context, the pioneering idea of physical layer authentication (PLA) was introduced in [19]. These results were extended in different topologies, including, vehicular ad hoc networks (VANETs) [20], ultra-reliable low-latency communications (URLLC) [21], and wireless sensor communications [22]. Recently, in [23], the authors design PLA protocols based on machine learning techniques. In [24], the researchers provide useful insights concerning the authentication and key generation at the physical layer for the internet of things (IoT).

On the other hand, the first ideas of PLS are from the seminal paper of Shannon, who laid the basis of secrecy systems [25]. Later, the wiretap channel was presented by Wyner in 1975 [26]. In that work, Wyner established that secret messages could be transmitted when the wiretap channel is a degraded (much noisier) version of the legitimate link. Thus, the secrecy capacity is the maximum data rate that can be safely transmitted without being decoded by an eavesdropper. In practice, due to the intrinsic randomness of the medium, the signal-to-noise ratio (SNR) of the eavesdropper can be similar or even better than the legitimate channel. Specifically, when the eavesdropper is closer to the source than the legitimate receiver. So, Wyner's ideas become impracticable in such environments. Inspired by Wyner's work, investigations of the attainable secrecy capacity against eavesdropping were addressed in [27] for the broadcast channel, and the Gaussian channel in [28]. These approaches have inspired an important amount of recent research activities from the information-theoretic point of view for different fading channels. Specifically, we survey the fading channel models that have proven to characterize mm-Wave scenarios in 5G accurately. We can mention the following: 1) $\kappa$-$\mu$ shadowed: In this fading model, the received power signal is structured by a finite sum of multipath clusters. Each cluster is modeled by a dominant component and scattered diffuse waves. All the specular components are subject to the shadowing fluctuation caused by obstacles or human body movements [29]. 2) $\alpha$-$\eta$-$\kappa$-$\mu$: As pointed out in [30], this is a rather complex fading model that encompasses virtually all the fading channel models proposed in the literature based on a power envelope formulation. Such a model incorporates the relevant short-term propagation factors, viz., non-linearity of the medium, scattered waves, specular components, and multipath clustering. 3) Fluctuating Two-Ray [31]: In this channel model, the receiver signal can be expressed as a superposition of two dominant waves, plus additional waves associated with diffuse scattering. Also, a fluctuation in the amplitude of the dominant rays is assumed. This fact is due to blockage by obstacles or by various electromagnetic

disturbances. 4) Fisher-Snedecor $\mathcal{F}$: In this composite fading proposed in [32], the received signal is modeled by jointly combining the effects of shadowing and small-scale fading. The secrecy performance over the fading channels models described above is given in Table 2.

Finally, the PLS testbed is a paramount aspect of verifying the novel security designs proposed in the vast body of literature. These experimental hardware-based results allow detecting potential security threats not considered in the preliminary studies. In Table 3, we list interesting works on PLS testbed.

## 3 Fundamentals of Physical Layer Security

Here, we introduce essential concepts to understand PLS in wireless communications systems.

### 3.1 General System Model

The general PLS model is made up of three main communication nodes as shown in Fig. 1.

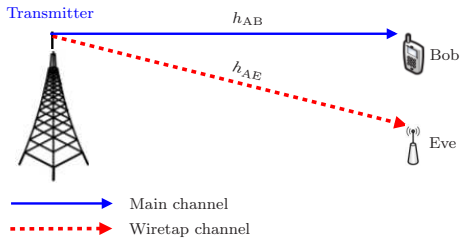


**Fig. 1** The wiretap channel model consisting of two legitimate nodes and an eavesdropper.

The first node is the legitimate transmitter (also known as Alice in network security jargon), the second node is the intended receiver (also known as Bob), and the third node is the eavesdropper (also known as Eve). The channel between Alice and Bob is known as the legitimate channel, while the path between Alice and Eve is named the wiretap channel (also known as Eavesdropper channel). In this setup, Alice transmits confidential information to Bob, while Eve receives the signal and intends to decode it. Therefore, Alice's goal is to use a transmission approach that can deliver the secret information to Bob while making sure that Eve cannot intercept the transmitted data. To attain secrecy in wireless systems, PLS uses signal processing techniques designed to take advantage of specific features of the channel, including fading, noise, interference, among others. Another relevant factor to take into account in the wiretap channel (see, Fig. 1) is the availability of channel state information (CSI) in all the nodes (i.e., Alice, Bob, and Eve). CSI can vary from complete, partial to even null at the nodes. From a secrecy perspective, CSI is of paramount importance because, based on its knowledge, the transmitter can decide whether or not to transmit and at which rate. Thus, this fact will lead to achieving remarkable improvement in the SOP. However, in practice, all nodes can only obtain some kind of information about the channel between them and the other nodes. On the one hand, Alice is generally considered to know Bob's CSI but not Eve's CSI. This is because Eve is typically passive (i.e., Eve monitors the network, intercepts messages, and does not communicate with other users in the network). Several works, such as [39–41], have done performance analysis of PLS with passive eavesdropper. On the other hand, there are scenarios in which Eve is active and performs some of the following actions: intentional interference (also known as jamming), adulteration and modification, or denial of service [42]. Performance analysis of PLS, which considers Alice knows Eve's channel (i.e., active eavesdropper), can be found in [43–45]. It is worthwhile to mention that in the PLS evaluation, Eve's and Bob's channels are typically assumed to be independent of each other (i.e., both channels are separated at least half wavelength). Furthermore, the links (i.e., Alice-to-Bob and Alice-to-Eve) that do not meet the condition mentioned above (i.e., correlated channels) are investigated in [46–48].

### 3.2 Performance Metrics

In this section, we explain the most used secrecy metrics proposed in the literature. Good knowledge of these metrics will ease the understanding of the works to be addressed in the following sections.

#### *3.2.1 Secrecy Capacity*

The secrecy capacity, $C_{\mathrm{S}}$, for a wireless channel is the most used metric in PLS evaluation. $C_{\mathrm{S}}$ is defined as the capacity difference between the main and wiretap channels. Rigorously speaking, it defines the maximum secret rate at which the secret information reliably recovers at transmitter while remaining unrecoverable at Eve [54]. Therefore, the $C_{\mathrm{S}}$ in a quasi-static fading channel case is formulated as in [26] by

$$\begin{aligned} C_{\mathrm{S}} &= \max\{C_{\mathrm{B}} - C_{\mathrm{E}}, 0\} \\ &= \max\{\mathrm{W}\log_2(1+\gamma_{\mathrm{B}}) - \mathrm{W}\log_2(1+\gamma_{\mathrm{E}}), 0\} \end{aligned} \quad (1)$$

| Reference | System Model | Fading Channel | Secrecy Analysis |
|---|---|---|---|
| F. J. Lopez et al. [33] | SISOSE wiretap channels | $\kappa$-$\mu$ shadowed | SOP |
| J. D. Vega et al. [34] | MIMOME wiretap channels | $\kappa$-$\mu$ shadowed | SOP, Asymptotic SOP average secrecy capacity (ASC) Asymptotic ASC |
| A. Mathur et al. [35] | SISOSE wiretap channels | $\alpha$-$\eta$-$\kappa$-$\mu$ | SOP, Asymptotic ASC |
| W. Zheng et al. [36] | SISOSE wiretap channels | Fluctuating Two-Ray | SOP, ASC |
| J. D. Vega et al. [37] | SISOSE wiretap channels | N-Wave with Difuse Power | SOP, Asymptotic SOP |
| L. Kong et al. [38] | SISOSE wiretap channels | Fisher-Snedecor | SOP, ASC |

**Table 2** PLS performance over fading channels models.

| Reference | System Model | Testbed for PLS |
|---|---|---|
| C. Martins et al. [49] | SISOSE wiretap channels | Coding for Secrecy Schemes |
| J. Lu et al. [50] | SISOSE wiretap channels | Wiretap Lattice Codes |
| W. Guo et al. [51] | SISOSE wiretap channels with the assistance of Cooperative jamming (CJ) | A CJ Cancellation Architecture |
| J. M. Hamamreh et al. [52] | SISOSE wiretap channels | Secure Pre-coding and Post-coding |
| T. Peng et al. [53] | SISOSE wiretap channels | Secret Key Generation |

**Table 3** Testbed for PLS in real environments through software-defined radio platforms.

where $|\cdot|$ is the absolute value, $\gamma_{\rm X} = \frac{|h_{\rm AX}|^2 P_{\rm A}}{N_0}$ for X $\in \{\rm B, E\}$ is the instantaneous SNR, and $h_{\rm AB}$ and $h_{\rm AE}$ are the channel coefficients of the main and wiretap channels, respectively. $P_{\rm A}$ is the transmit power at Alice, $N_0$ is the average noise power, and $C_{\rm B}$ and $C_{\rm E}$ are the capacities of the main and wiretap channels, respectively. Without loss of generality, it is considered a normalized bandwidth of W = 1 in the capacity formulations mentioned above. Under this scenario, it is possible to attain secure transmissions only if the legitimate link has a better SNR than the eavesdropper link, i.e.,

$$C_{\rm S} = \begin{cases} \log_2\left(\frac{1+\gamma_{\rm B}}{1+\gamma_{\rm E}}\right), & \text{if } \gamma_{\rm B} > \gamma_{\rm E} \\ 0, & \text{if } \gamma_{\rm B} \leq \gamma_{\rm E}, \end{cases} \tag{2}$$

It is worth highlighting that the $C_{\rm S}$ is widely extended by researchers to compute the SOP [55].

### *3.2.2 Secrecy Outage Probability*

The SOP is defined as the probability that the secrecy capacity falls below a target secrecy rate of $R_{\rm S}$. In other words, when the current $C_{\rm S}$ is not more than a pre-established target $R_{\rm S}$, the secrecy outage happens. This fact means that the current secrecy rate cannot guarantee the security requirement. It can be formulated as in [56] by

$$\begin{aligned} \text{SOP} &= \Pr\left\{C_{\rm S}\left(\gamma_{\rm B}, \gamma_{\rm E}\right) < R_{\rm S}\right\} \\ &\overset{(a)}{=} \Pr\left\{\left(\frac{1+\gamma_{\rm B}}{1+\gamma_{\rm E}}\right) < 2^{R_{\rm S}}\right\} \\ &\overset{(b)}{\geq} \Pr\left\{\frac{\gamma_{\rm B}}{\gamma_{\rm E}} < 2^{R_{\rm S}}\right\} \end{aligned} \tag{3}$$

where $\Pr\{\cdot\}$ denotes probability. The SOP in $(a)$ indicates that whenever $R_{\rm S} < C_{\rm S}$, the wiretap channel will be worse than the legitimate channel. So, secure communications are possible [57].It is worth mentioning that state of the art on PLS's research topic over different types of fading channels focuses on the calculation of $(b)$ due to its simpler mathematical tractability concerning the formulation in $(a)$. Furthermore, the formulation in $(b)$ is well-known as the lower bound of the SOP and represents the ratio of two squared random variables (RVs), namely: $\gamma_{\rm B}$ and $\gamma_{\rm E}$, which can follow any fading distribution. In this context, to assess the PLS performance over generalized channels and their corresponding special cases, two recent works proposed in [58, 59]. These works developed closed-form fashions for the ratio of two squared RVs of the vast majority of fading channels models used to characterize the propagation environment of the 5G. Despite the important insights that the SOP provides in the characterization of secrecy performance, it has the following demerits: *i*) it cannot quantify the amount of data leaking to the eavesdroppers when the outage happens (i.e., transmission security); *ii*) it cannot offer any information about the bob's skill to decode transmitted data successfully (i.e., transmission reliability); *iii*) it cannot offer any information about the eavesdropper's skill to decrypt confidential data successfully; *iv*) it cannot be straightly connected with quality of service (QoS) requirements for network services [60]. Motivated by the limitations of the SOP, researchers in [61, 62] proposed new metrics to overcome the three demerits mentioned above of the SOP. Thus, the authors give more insights into PLS and how secrecy is measured. It is worthwhile to mention that the definition of the SOP and the $C_{\rm S}$

can also be used to the scenario with multiple antennas at different nodes. Readers are referred to [63–65] for further analysis of this field. Next, according to the classical SOP defined above, alternative secrecy outage formulations from (3) are defined to follow.

### *3.2.3 Alternative Secrecy Outage Formulation*

As previously mentioned, the conventional SOP formulation in (3) does not distinguish between reliability and security. Therefore, an outage event in (3) can imply either a fault to achieve secrecy or that the transmitted message cannot be successfully decoded by Bob. In light of the above considerations, an alternative secrecy outage formulation was proposed in [66], which measures that a transmitted data fails to attain secrecy. In a such formulation, the rate difference $R_{\mathrm{E}} \triangleq R_{\mathrm{B}} - R_{\mathrm{S}}$ denotes the cost of security when the data is transmitted. Also, $R_{\mathrm{B}}$ is the rate of the transmitted messages, and $R_{\mathrm{S}}$ is the rate of the confidential data. It is worth mentioning that Bob can decode any transmitted message successfully if and only if $C_{\mathrm{B}} > R_{\mathrm{B}}$, while secrecy fails if $C_{\mathrm{E}} > R_{\mathrm{E}}$. Therefore, the alternative SOP can be formulated as the conditional probability upon a message being transmitted.

$$\mathrm{SOP}_{\mathrm{A}} = \Pr\left\{C_{\mathrm{E}} > C_{\mathrm{B}} - R_{\mathrm{S}} | \gamma_{\mathrm{B}} > \mu\right\}, \tag{4}$$

where $\mu$ is a certain threshold, which allows Alice to decide whether (when $\gamma_{\mathrm{B}} > \mu$) or not (when $\gamma_{\mathrm{B}} \leq \mu$) to transmit the information[3]. Unlike the SOP definition in (3), the formulation in (4) takes into consideration important system design parameters, including the rate of the transmitted messages $R_{\mathrm{B}}$, and the fact whether a message was transmitted or not. Furthermore, this metric is useful when Alice knows Bob's CSI. Since in this scenario, Alice chooses whether or not to transmit, and if Alice decides to transmit, it will possibly do so with varying rates depending on Bob's CSI. In the contrast case, i.e., when the transmission is carried out at a constant rate[4], the alternative SOP formulation in (4) reduces to the unconditional probability.

This metric is achieving success in the latest research works related to performance in PLS. Readers can revise [67–71] for more detailed information about this research topic.

### *3.2.4 Fractional Equivocation Based Metrics*

Based on the limitation of the classic SOP in (3) in measuring both the amount of data leakage to the eavesdropper and Eve's skill to decode confidential data, three novel metrics was proposed in [72]. These metrics measure the secrecy performance of wireless systems from the partial secrecy perspective over quasi-static fading. The fractional equivocation (i.e., $\Delta$) is a random quantity due to the propagation medium's fading characteristics. Mathematically, the fractional equivocation for a given fading realization of the channel is expressed as [72]

$$\Delta = \begin{cases} 1, & \text{if } C_{\mathrm{E}} \leq C_{\mathrm{B}} - R_{\mathrm{S}} \\ \left(C_{\mathrm{B}} - C_{\mathrm{E}}\right)/R_{\mathrm{S}}, & \text{if } C_{\mathrm{B}} - R_{\mathrm{S}} < C_{\mathrm{E}} < C_{\mathrm{B}} \\ 0, & \text{if } C_{\mathrm{B}} \leq C_{\mathrm{E}}. \end{cases} \tag{5}$$

From (5), the authors in [72] proposed the following metrics:

1. **Generalized Secrecy Outage Probability (GSOP):** This metric is related to wireless systems with distinct secrecy levels measured in terms of Eve's capability to decode the confidential information and is given by

$$\mathrm{GSOP} = \Pr\left\{\Delta < \theta\right\}, \tag{6}$$

where $0 < \theta < 1$ represents the minimum reasonable value of the fractional equivocation. Here, Eve's skill to decrypt the confidential message is set by selecting different values of $\theta$. For instance, the conventional SOP is a particular case of the GSOP for $\theta = 1$.

2. **Asymptotic Lower Bound on Eve's Decoding Error Probability:** This metric is defined as the average of the fractional equivocation and is given by

$$\bar{\Delta} = \mathbb{E}\left[\Delta\right], \tag{7}$$

in which $\mathbb{E}\left[\cdot\right]$ is the expectation operation. It is worthwhile to mention that, when the entropy of data for transmission is long enough, Eve's decoding error probability for a given fading realization is lower bounded by the fractional equivocation, i.e., $P_e \geq \bar{\Delta}$[5].

3. **Average Information Leakage Rate:** This metric explains how fast the data is leaked to Eve when an unchanged rate transmission, $R_{\mathrm{S}}$, is adopted in the system. It can be expressed as

$$R_{\mathrm{L}} = \mathbb{E}\left[\left(1 - \Delta\right) R_{\mathrm{S}}\right] = \left(1 - \bar{\Delta}\right) R_{\mathrm{S}}. \tag{8}$$

In [73,74], researchers investigated the PLS performance by using different transmission topologies based on the metrics mentioned above.

[3] Note that the SNR at Bob, i.e., $\gamma_{\mathrm{B}}$ can only be estimated when Alice knows Bob's CSI.

[4] This scenario corresponds to the case when bob knows when Alice doesn't know about Bob's CSI.

[5] Interested readers can revise [72, Eq. (6)] for guidance about why the average fractional equivocation gives a lower bound of Eve's decoding error probability.

*3.2.5 Intercept Probability*

An intercept event happens when the $C_{\mathrm{S}}$ is negative or falls below 0. This means that the wiretap channel has a better SNR than the legitimate channel. The intercept probability can be formulated as in [75] by

$$P_{\mathrm{int}} = \Pr\left\{C_{\mathrm{S}}\left(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}\right) < 0\right\} \tag{9}$$

Although this metric has not been widely explored in the literature, it is currently being investigated in evaluating the secrecy performance of wireless channels. Readers are referred to [76–78] for more information on this field of research.

*3.2.6 Probability of Strictly Positive Secrecy Capacity*

The Probability of SPSC is the probability that the $C_{\mathrm{S}}$ remains higher than 0. This means that secrecy in communication has been attained[6]. Mathematically, it can be written as in [79] by

$$P_{\mathrm{SPSC}} = \Pr\left\{C_{\mathrm{S}}\left(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}\right) > 0\right\}. \tag{10}$$

In [80–82], researchers investigated the security performance of wireless systems based on the SPSC metric over different fading channels models.

*3.2.7 Secrecy Throughput*

In a secure transmission design, the secrecy throughput (ST) is a useful metric to assess the secrecy performance of the next wireless communications systems [83]. The ST can be computed based on the perfect, partial and null knowledge of the CSI of both the Bob and the Eve channels. Regarding the three scenarios[7] mentioned, the case in that Alice knows Bob's CSI but not Eve's CSI is the most practical design criterion for 5G secure networks. This scenario (i.e., passive eavesdropping) represents the worst case for communications since Alice cannot guarantee secrecy. The ST is defined as confidential data transmission, i.e, $\eta = p_{tx}(\mu)R_{\mathrm{S}}$, where $p_{tx}(\mu)$ denotes the probability of success in the transmission, and is given by [66]

$$p_{tx}(\mu) = \Pr\left\{\gamma_{\mathrm{B}} > \mu\right\}. \tag{11}$$

[6] The authors in [60] provide the theoretical meaning as well as the analytical expressions to quantify the $C_{\mathrm{S}}$ (e.g., perfect secrecy, weak secrecy, and strong secrecy) when the $C_{\mathrm{S}}$ is greater than zero.

[7] In [84], the authors carried out a complete analysis of how to pose the problem of optimizing ST based on the CSI knowledge of both Eve and Bob for the three scenarios mentioned.

In a design problem of maximizing the throughput, $\eta$, we need to consider $(i)$ the constraints based on reliability and secrecy requirements, and $(ii)$ the availability of Bob's CSI at Alice. Based on this, we review the two most widely used transmission schemes in practice, as follows:

1. **Adaptive Rate Scheme:** In this scenario, the rate of the confidential data, $R_{\mathrm{S}}$, can be adaptively chosen according to the CSI of Bob's channel. Besides, $R_{\mathrm{B}}$ is set as close to $C_{\mathrm{B}}$ to obtain the maximum possible transmission rate, ensuring that there is no decoding error at Bob. The ST for the adaptive rate scheme is given by [66]

$$\begin{aligned} \max_{\mu, R_{\mathrm{S}}} \quad & \eta \\ \text{s.t.} \quad & \mathrm{SOP}_{\mathrm{A}}(\mu, R_{\mathrm{S}}) \leq \epsilon, p_{tx}(\mu) \geq \delta, R_{\mathrm{S}} > 0, \end{aligned} \tag{12}$$

   where $\delta \in [0,1]$ and $\epsilon \in [0,1]$ denote the reliability and security requirements[8], respectively. For this transmission scheme, the $\mathrm{SOP}_{\mathrm{A}}$ and the $p_{tx}$ are given by (4) and (11), respectively. It is noteworthy that the optimal solution for this adaptive design is hard to obtain since $R_{\mathrm{S}}$ changes according to the CSI of Bob's channel. However, (12) can be treated as a two-step optimization problem, as discussed in [84].
2. **Non-Adaptive Rate Scheme:** In this scenario, both the rate of the transmitted messages, $R_{\mathrm{B}}$, and the rate of the confidential data, $R_{\mathrm{S}}$, are constant over time but need to be optimally chosen. The ST for the non-adaptive rate scheme can be formulated as [66]

$$\begin{aligned} \max_{\mu, R_{\mathrm{B}} R_{\mathrm{S}}} \quad & \eta \\ \text{s.t.} \quad & \mathrm{SOP}_{\mathrm{A}}(\mu, R_{\mathrm{B}}, R_{\mathrm{S}}) \leq \epsilon, p_{tx}(\mu) \geq \delta, R_{\mathrm{S}} > 0, \end{aligned} \tag{13}$$

   where $p_{tx}$ is given by (11). For this transmission scheme, since Alice does not know Bob' CSI, the $\mathrm{SOP}_{\mathrm{A}}$ in (4) reduces to the unconditional probability as

$$\mathrm{SOP}_{\mathrm{A}} = \Pr\left\{C_{\mathrm{E}} > R_{\mathrm{B}} - R_{\mathrm{S}}\right\}. \tag{14}$$

It is worth mentioning that in [85], the authors introduced a different framework for determining the ST. A summary of the latest ST performance contributions in 5G enabling technologies is given in Table 4.

[8] It is worth to mention that a good transmission scheme achieves a tradeoff between reliability and secrecy.

| Reference | System Model | CSI | ST Analysis |
|---|---|---|---|
| G. Gomez et al. [86] | NOMA in MISOSE wiretap channels | No CSI of the eavesdropper Both the perfect CSI and the no CSI of the desired user | Both adaptive and non-adaptive design schemes |
| Z. Wang et al. [87] | Simultaneous wireless information and power transfer in SISOSE wiretap channels | No CSI of the eavesdropper Perfect CSI of the desired user | Adaptive design scheme |
| T. Zheng et al. [88] | SISOSE and MISOSE wiretap channels | Statistical CSI of the eavesdropper Both the perfect CSI and the no CSI of the desired user | Both adaptive and non-adaptive design schemes |
| K. Jiang et al. [89] | NOMA with cooperative jamming in MISOSE wiretap channels | Statistical CSI of the eavesdropper Perfect CSI of the desired users | Adaptive design scheme |

**Table 4** ST analysis in different topologies.

## 4 Physical Layer Security Techniques

This section introduces the background of PLS techniques commonly used in the research community.

### 4.1 Artificial Noise Generation

The main idea of this technique is to artificially degrade Eve's channel by injecting artificial noise (AN). The process consists in that an authorized node in the network (e.g., Alice, Bob, or another) adds well designed artificially jamming signals to the transmitted signal that can only harm Eve's channel [90]. The basic system model of AN network for PLS is depicted in Fig. 2.

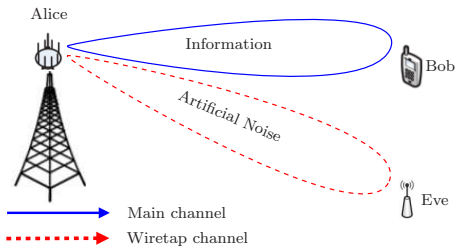


**Fig. 2** The model of AN network for a wiretap channel consisting of two main nodes and an eavesdropper.

In what follows, we review the fundamental works that use AN or jamming to improve PLS performance. In [91], the authors proposed the design of AN-aided precoding to enhance PLS in a multi-user single eavesdropper wiretap visible light communication (VLC) networks. A fairness comparison of three AN-aided secure transmission approaches in wiretap channels was studied in [92]. In such work, it is was demonstrated that regarding the secrecy performance, the partially adaptive scheme (only the rate $R_{\mathrm{B}}$ changes) outperforms the on-off scheme (both $R_{\mathrm{B}}$ and confidential rate $R_{\mathrm{S}}$ vary). In [93], the researches proposed a $C_{\mathrm{S}}$ optimization (SCO)-AN to improve the $C_{\mathrm{S}}$ in wireless networks. The results in such an approach demonstrated that SCO-AN achieved greater improvement in the $C_{\mathrm{S}}$ than traditional AN.

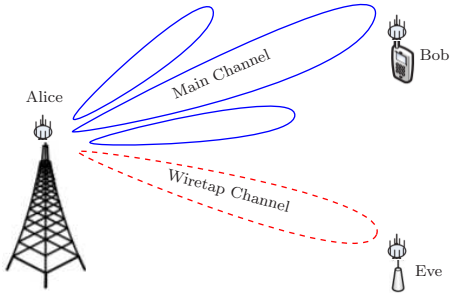


**Fig. 3** A MIMO wireless system by using secure beamforming with nulls directed towards Eve.

### 4.2 Multi-Antenna Diversity

By leveraging the available spatial dimensions of wireless channels, MIMO techniques can diminish the impacts of fading while increasing the $C_{\mathrm{S}}$ [94]. To achieve the full benefits of MIMO, the system must be protected against eavesdroppers attacks. In Multi-Antenna Diversity, the basic idea of beamforming is to send the desired signal in the null space of the eavesdropper channel, as shown in Fig. 3. A seminal work in [95] was the first to investigate beamforming schemes for enhancing the PLS performance in MIMO wiretap channels. This paper encourages other researches to investigate beamforming challenges regarding PLS. Thus, in [96], the authors were the first to study PLS in a two-tier downlink HetNets. A novel layered PLS model was proposed in [97]. Here, the zero-forcing beamforming was applied to layered PLS to tradeoff the achievable secrecy performance and the computational complexity. Moreover, an optimal technique commonly used on the

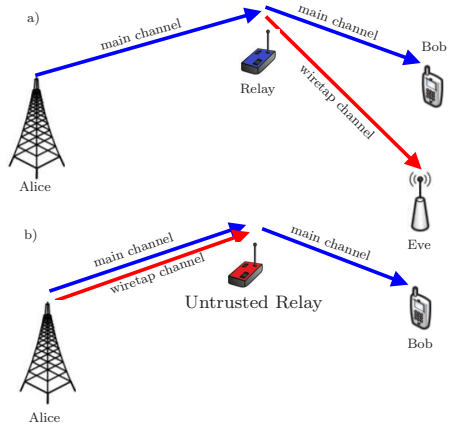


**Fig. 4** a) Traditional relay network in wiretap channel. b) Untrusted relay network in wiretap channel.

receiver side in MIMO systems for improving PLS was presented in [98].

### 4.3 Cooperative Diversity

In this section, we introduce cooperative communications, which, besides providing reliability and extended coverage, are used for improving the PLS performance. Relaying techniques allow the transmitter sends its information to the destination through a relay located between the two nodes. The most famous re-transmission protocols are: *i*) amplify and forward (AF), and *ii*) decode and forward (DF) [60]. Relays can be configured in different ways to counteract eavesdropping. Specifically, they can behave like a conventional relay to attend the legitimate communication (vide Fig. 4a), or they can also act as jammers by sending AN to degrade Eve's channel. Moreover, they can take the role of potential eavesdroppers when they are untrusted. So, the confidential signals are vulnerable (vide Fig. 4b) [94]. Next, we present interesting works on cooperative relaying methods to provide PLS in wireless systems. In [99], the authors were the first to use cooperative relays to provide secure transmissions. In such work, three cooperative schemes were considered: DF, AF, and cooperative jamming (CJ)[9] to maximize the attainable secrecy rate subject to a transmit power constraint. The work in [100] studied the reachable secrecy diversity gain of cooperative networks with untrusted relays. In that approach, it was shown that the secrecy rate decreases as the number of untrusted relays increases. To enhance the PLS of the untrusted relay networks, a new FD destination jamming (FDJ) topology was introduced in [101]. The results showed that FDJ strategies provided superior secrecy performance to that of the non-jamming schemes.

[9] In CJ, while the transmitter sends the data, the relay transmits an interference signal to harm the eavesdropper's channel.

## 5 Next Generation Physical Layer Technologies

Next-generation cellular networks are planned to attain high capacity rates to face the rapid growth of data traffic. The combination of 5G key technologies is considered as a cost-effective solution to cover the high QoS requirements in 5G. However, the dramatic increase in the amount of data and complex communication scenarios put forward higher requirements on the security of 5G. Here, we review the notions of each of the promising enabling technologies for 5G, including their advantages and disadvantages. Next, we summarize the latest research results of PLS for 5G technologies.

### 5.1 Massive MIMO

Massive MIMO is a multi-user topology in which the base station (BS) has a large number of antennas, as depicted in Fig. 5. These arrangements provide several degrees of freedom for networks, better performance in channel capacities, and improve communication qualities in 5G networks [102]. For security purposes, massive MIMO gives a very oriented beam guide to the legitimate user's location. So, the information leakage is reduced to undesired locations (i.e., Eve) significantly [103].

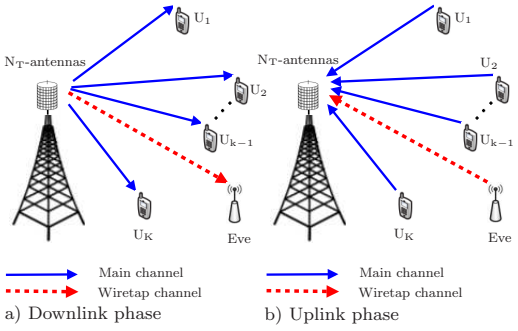


**Fig. 5** Massive MIMO downlink with K legitimate user nodes, $U_k$ for $k = 1, \cdots, K$, and an eavesdropper.

The authors in [104] were the first to investigate the drawbacks of PLS performance by assuming that the number of antennas goes to infinity (i.e., massive MIMO). Unlike the traditional MIMO, massive MIMO presents the following big challenges: 1) CSI estimation process is a difficult task; 2) the channels models are not independent as the distances of antennas are

shorter than a half of the wavelength. Therefore, massive MIMO is still an open research field [105]. Then, we survey the current security attacks of massive MIMO relying on passive and active eavesdropper cases, respectively.

### *5.1.1 Passive Eavesdropper Scenarios*

The key concept here is that the existence of a passive eavesdropper does not affect at all the beam of transmission at the BS. So, it has a negligible effect on the $C_S$. Recently, in [106] an algorithm was developed to optimize power allocation of beam transmission for single-cell massive MIMO consisting of a passive eavesdropper with multiple antennas. The findings showed that beam transmission can attain optimal performance in terms of $C_S$. Authors in [107] investigated secure transmissions of multi-pair massive MIMO AF relaying systems by considering Ricean fading. In that work, the attainable sum secrecy rate is maximized by using a power control topology. Also, the use of AN-aiding schemes to degrade the eavesdropping channel to improve the security in massive MIMO was analyzed in [108].

Other massive MIMO approaches with passive eavesdroppers include the effect of hardware deficiencies on the PLS performance of massive downlink MIMO in the existence of eavesdropper with multiple antennas [109], performance analysis of wireless communications in a multi-user massive MIMO by using imperfect CSI [110], and SOP analysis for massive MIMO scenarios [111].

### *5.1.2 Active Eavesdropper Scenarios*

A large number of PLS research works consider that Bob's CSI is known at Alice and does not take into account the process for obtaining this CSI. In time duplex division (TDD) massive MIMO, legitimate nodes transmit pilot signals to the BS to estimate the CSI for the later transmission of the downlink during the uplink phase. At the same time, an active eavesdropper can interfere in the training stage to produce pilot contamination at the BS (see Fig. 6). This forces in the transmission phase (i.e., downlink) of the BS to inherently beamform towards the eavesdropper, increasing its received signal power [112]. This fact compromises that a secrecy rate may not be attainable. The result of this attack is that the advantages of PLS for massive MIMO are lost [113]. To circumvent the referred limitation, the following works investigated techniques to avoid the pilot contamination attack (PCA). In [114], the authors proposed a reliable communication that does not need statistical information about the links for a TDD massive MIMO with an active eavesdropper. In the proposed transmission, an asynchronous protocol is used instead of the conventional synchronous protocol. A transmit power control policy was presented in [115], to allocate the transmit power at the BS/relay for maximizing the attainable secrecy rate in Massive MIMO Downlink. For PLS in massive MIMO, in [116] was designed robust scheme together with AN beamforming to deliver the legitimate nodes and eavesdroppers different signal-to-interference-and-noise ratio (SINR).

Other secure massive transmissions against active eavesdropper include cooperative scheme strategy [117], a product channel attack [118], data-aided secure downlink transmission scheme [119], and the secure communications design based on game theory [120].

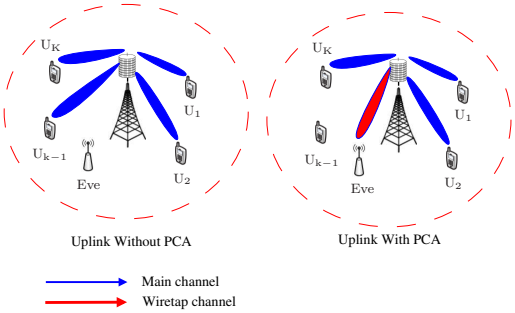


**Fig. 6** PCA on massive MIMO systems.

## 5.2 mm-Wave

Nowadays, most wireless systems are allocated in the band spectrum of 300 MHz to 3 GHz, which is full. In this context, mm-Wave[10] is a very innovative key solution for the next wireless networks (5G and beyond) to overcome this limitation. The idea behind mm-Wave communications is to take advantage of the unexploited high-frequency mm-wave spectrum, ranging from 3-300 GHz to face with future multi-gigabit-per-second mobile applications. Unlike microwave networks, mm-Wave networks have several novel features, such as a large number of antennas[11], short-range, and different propagation laws [123]. The adoption of PLS mm-Wave networks systems is a remarkably emerging topic of research. Several approaches have been developed in this domain[12].The general PLS model for mm-Wave, mas-

[10] To have a more detailed framework about millimeter wireless systems, we refer the reader to [121].

[11] The small wavelength of high-frequency signals in mm-Wave enables a large number of antennas, which can be exploited to cover the requirements of massive MIMO. Therefore, the combination of massive MIMO, small cell geometries (which will be described later), and mm-Wave has vast potential to improve the security of the next networks [122].

[12] For a good summary of works about the beginnings of PLS in mm-Wave, we refer the reader to the survey in [124]

sive MIMO, FD, and Small Cells for 5G is presented in Fig. 7. Then, we review some of the current works to highlight the potential of this emerging field. The major research papers focus on 28, 38, and 60 GHz band [125].

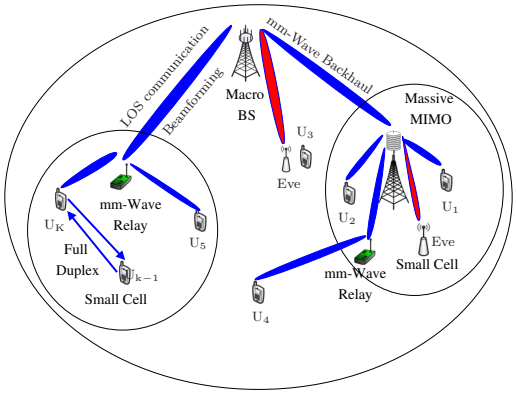


**Fig. 7** Illustration of promising technologies such as mm-Wave, massive MIMO, Full Duplex, and Small Cells.

In [126], to maximize the SNR (i.e., to improve the $C_S$), the authors proposed AN aided two stages secure hybrid beamforming method in MIMO mm-Wave relay eavesdropping scenario. Here, the combination of the two-stage hybrid beamforming algorithm with AN allows guaranteeing both high throughput and communication security. The authors in [127] investigated secure communications techniques, namely, maximum ratio transmitting (MRT) beamforming, and AN beamforming. Specifically, it was developed the optimal power allocation between AN and the signal of interest that maximizes the $C_S$ for AN beamforming. Concerning vehicular environments, in [128], the researchers proposed a location-based PLS technique for secure mm-Wave vehicular communication. Such a proposed method takes advantage of a large number of antennas at the mm-Wave frequencies to jam eavesdroppers with sensitive receivers. The technique proved to offer excellent performance in terms of SOP.

Other approaches include PLS Analysis of Hybrid mm-Wave Networks [129], and $C_S$ of 5G mm-Wave Small Cells [130].

### 5.3 HetNets – Small Cells

Traditionally, macro-cellular networks are efficient in offering area coverage for voice applications and services that support low data traffic but limited in providing high data rates. So, one of the promising solutions for users is to reduce the cell size in future wireless networks [131]. In this context, HetNets will perform a pivotal role in meeting the demands of 5G. The goal of HetNetsis to make efficient use of the spectrum to satisfy the spectacular growth of the data demands of the upcoming mobile services. In the HetNets topologies, users with different capabilities (i.e., transmission powers, coverage areas, etc.) are implemented as part of a multi-tier hierarchical structure, as depicted in Fig. 8. The high-power nodes (HPNs) with broad radio coverage fields are located in the macro cell, while low-power nodes (LPNs) with limited coverage are located in small cells [17]. The small cells (typically with coverage of a few meters) can have different configurations. For instance, the femtocells that are usually used in homes and development companies, and the picocells that are used for ample outdoor coverage [131]. Besides, HetNets include a device level that incorporates device-to-device (D2D) communications. This technology favors nearby devices to connect directly and collaborate without using HPNs/LPNs, making them a robust tool for low-latency, and high-performance data services [132].

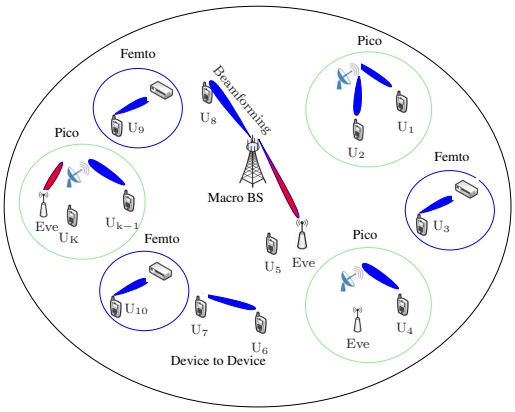


**Fig. 8** HetNets with legitimate users and eavesdroppers.

The multi-tier topology in HetNets entails technical challenges (e.g., self-organization, backhauling, handover, and interference) to the investigation of PLS compared to the traditional single-tier architecture [133]. Then, we review the most current works that address the challenges mentioned above of the HetNets on PLS. In two novel approaches [134,135], PLS performance in multi-cell networks has been studied. The researchers have taken advantage of cooperative multi-antenna transmissions to improve the $C_S$ by assuming: *i*) a single eavesdropper [134], and *ii*) a multiple untrusted relays [135]. In [136], the authors presented an interference-canceled opportunistic antenna selection (IC-OAS) topology to improve PLS in HetNets. Here, a passive eavesdropper is considered to intercept the communications of both the macro and small cells.

Other secure communications works in HetNets systems include: Stochastic Geometry strategies [137], se-

crecy outage analysis undergo Nakagami-$m$ fading channels [138], and secure communications design based on game theory [139].

### 5.4 Full-Duplex

Among the promising technologies for 5G, FD technology carries major challenges for PLS communications. On the one hand, FD enables the destination node to create AN to interfere with the eavesdropper and receive the data at the same time. On the other hand, if the eavesdropper has the FD technology, it can actively attack the receiver in the transmission while eavesdropping. Also, FD systems can double the spectral efficiency concerning the common half-duplex schemes. However, the main drawback that affects the transmission of FD is the management of the self-interference signal imposed by the transmission antenna on the receiving antenna within the same transceiver [140]. The research on FD PLS communication can be classified into four categorizations of FD PLS schemes. Specifically, the FD receiver, the FD transmitter and receiver, the FD BS, and the FD eavesdropper [124]. Next, we review the most current works concerning the different configurations of the aforementioned FD technology. In [141], the authors proposed a novel channel training (CT) method for an FD receiver to improve PLS. In this setup, the receiver (i.e., Bob) is equipped with $N_{\mathrm{B}}$ antennas. So, it can simultaneously receive the data and transmits AN to the eavesdropper. Here, to diminish the non-cancelable self-interference due to the transmitted AN, the destination node has to estimate the self-interference channel before the communication stage. In [142] was considered a problem of a passive and smart eavesdropping attack on the MIMO wiretap scheme, where the receiver operates with FD mode. In such a system model, the clever eavesdropper cancels the interference (caused by the receiver) by stealing the CSI between legitimate nodes. To counteract this, the authors presented a cooperative jamming approach between transceivers to attain the optimal PLS performance. About FD active eavesdropper (FDAE), in [143], was analyzed the anti-eavesdropping and anti-jamming performance of D2D scenarios. In this case, the FDAE can passively intercept secret data in D2D topologies and actively jam all legitimate channels. In this respect, the authors proposed a hierarchical and power control method with multiple D2D node equipment and one cellular node to confront the smart FDAE.

Other works include FD strategies in HetNets [144, 145], secrecy rate maximization in Wireless Multi-Hop FD Networks [146], and secure communication based on joint design of information and AN beamforming for FD Networks [147].

### 5.5 Non-Orthogonal Multiple Access

Due to the limited spectral efficiency of orthogonal multiple access (OMA) systems in wireless networks, the OMA schemes are not appropriate to face the explosive growth in data traffic of the 5G. As a result, NOMA emerges as a promising candidate for 5G multiple access to provide massive connectivity and large system throughput [148]. Furthermore, it is well-known that NOMA will use advanced reception techniques such as successive interference cancellation (SIC) for robust multiple access. This fact may be a drawback in terms of processing delays. Fortunately, transmission/reception schemes in low-latency for NOMA systems are being investigated in the literature. The basic NOMA model for PLS is shown in Fig. 9. There are two kinds of eavesdroppers scenarios: $i$) the passive eavesdropper, whose channel cannot be known at Alice; $ii$) the active eavesdropper (i.e., common user), whose channel can be known at Alice. Therefore, providing security levels against the two types of eavesdroppers in NOMA technology is a challenging research topic in the design of the 5G networks [60]. The main idea behind PLS for NOMA is to mitigate the security problems by finding the optimal power allocation policy that maximizes the secrecy sum-rate (SSR) while satisfying the QoS requirements of users.

Then, we survey the key contributions regarding PLS in 5G NOMA systems. In [149], the authors investigated the PLS performance in a single-input single-output (SISO) NOMA scheme by maximizing the SSR of the NOMA subject to the users' QoS requirements. Here, NOMA has proven a remarkable SSR improvement concerning the classical OMA.

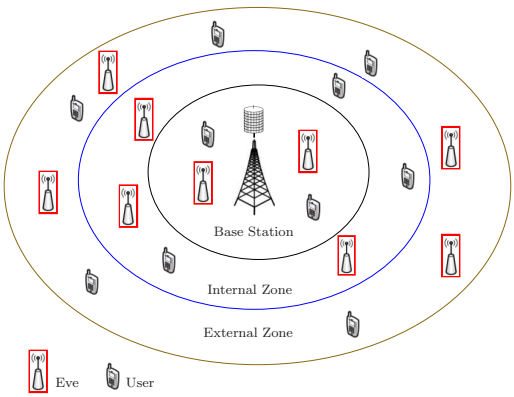


**Fig. 9** PLS model for NOMA

In [150], the researchers proposed a secure transmission for downlink multiple-input single-output (MISO) NOMA and energy-efficient design. This approach showed that the cooperative jamming NOMA scheme achieves much better secrecy performance than the direct transmission NOMA scheme. The secrecy in simultaneous wireless information and power transferring (SWIPT) in downlink NOMA systems was investigated in [151]. Later, the security challenges of vehicular users in an ultra-dense network were studied in [152]. Here, it was demonstrated that NOMA-based multiple access is successful in attaining a high SSR for vehicular users by efficiently designing the allocation resources.

Other interesting works include PLS performance of uplink NOMA in both non-colluding- and colluding-eavesdropper scenarios to analyze the effective secrecy throughput [153], the impact of random mobility on SSR maximization of NOMA systems subject to power limits and users' QoS requirements [154], the achievable secrecy rate by using the optimal security beamforming design in NOMA VLC networks [155], and the SSR optimization for both primary users and randomly deployed secondary users in the NOMA underlay cognitive radio network [156].

## 6 Conclusions and Future Research Directions

This work has tackled the fundamentals concepts and techniques regarding PLS over the enabling 5G technologies. The following research topics emerge from the reviewed technologies in this survey:

- Accurate fading channel models play a remarkable role in an optimal secure transmission design over 5G. Thus, some efforts have been oriented to propose more accurate channel models that provide a better fit to field measurements in a variety of new mm-Wave propagation scenarios. In this context, as claimed by the authors in [31], both Fluctuating Multiple-Ray and the $N$-Wave with Diffuse Power fading models constitute promising alternative models to characterize the propagation environment on mm-Wave communications. Therefore, the performance of PLS techniques over these generalized channels is an important topic for further investigations.
- Providing PLS usually entails compromising other system QoS requirements. For instance, high-security levels often sacrifice throughput, while AN schemes compromise power efficiency. Based on these factors, the characterizing of the secrecy metrics in novel adversary models wireless through nontraditional (e.g., fractional equivocation, average information leakage rate, and GSOP) metrics are essential tracks in future research.
- In the security paradigms, a promising direction of research is the integration of PLS and the classic wireless cryptography. Specifically, the physical layer features of the wireless medium can be exploited for designing new security algorithms to improve the current authentication and key management in higher layers. However, the integration of both approaches has not been studied adequately at present. Thus, this topic needs further investigation.
- An interesting future research direction could be to provide a detailed survey on the main drawbacks and merits of physical layer authentication (PLA) and Secret-Key Generation in 5G. In this sense, a research field that is not yet investigated extensively in the literature is the machine learning for intelligent PLA in 5G wireless networks.
- In order to support massive connectivity in 5G wireless networks, the multiple access technique called FHSS Based Sparse Code Multiple Access (SCMA) was proposed in [157]. Consequently, it is promising to investigate the anti-jamming schemes that achieve a reasonable tradeoff between spectrum efficiency and security in the FHSS-SCMA networks.
- Due to the combination of innovative technologies to cover the growing demands of data traffic and emerging services, it is essential to investigate PLS techniques regarding these new network scenarios. Within these networks, the following stand out: Unmanned Aerial Vehicles (UAV), enhanced Mobile Broadband (eMBB), URLLC, massive Machine-Type Communications (mMTC), and Vehicle-to-Everything (V2X) networks.
- Based on the PLS theoretical framework discussed throughout the survey, we notice that the PLS research has brought a lot of literature with topics ranging from security-theoretical studies to practical criteria designs. All the proposed scenarios have been investigated in specific topologies. However, since 5G is a multi-level system with different security levels, resorting to PLS techniques in this complicated environment is a challenging task. In this sense, the PLS approach should interact with other protocol stack techniques to reach a fair tradeoff between security and QoS.
- In PLS papers, it is often assumed that Eve has the same or worse channel conditions as the legitimate link. However, this may not always be true in practice, as the simple fact that Eve has more antennas than Bob and Alice leads to worrying security failures. This hurdle needs to be addressed when moving to PLS implementation.

## References


1. D. Liu, W. Hong, T. S. Rappaport, C. Luxey, and W. Hong. What will 5g antennas and propagation be? *IEEE Transactions on Antennas and Propagation*, 65(12):6205–6212, Dec 2017.
2. Y. Gao, S. Hu, W. Tang, Y. Li, Y. Sun, D. Huang, S. Cheng, and X. Li. Physical layer security in 5g based large scale social networks: Opportunities and challenges. *IEEE Access*, 6:26350–26357, 2018.
3. D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1):74–81, 2008.
4. J. D. Vega Sánchez, L. Urquiza-Aguiar, and M. C. Paredes Paredes. Physical layer security for 5g wireless networks: A comprehensive survey. In *2019 3rd Cyber Security in Networking Conference (CSNet)*, pages 122–129, 2019.
5. Dimitriya Mihaylova. An overview of methods of reducing the effect of jamming attacks at the physical layer of wireless networks. In Vladimir Poulkov, editor, *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, pages 271–284, Cham, 2019. Springer International Publishing.
6. Kanika Grover, Alvin Lim, and Qing Yang. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc Ubiquitous Comput.*, 17(4):197–215, December 2014.
7. Satish Vadlamani, Burak Eksioglu, Hugh Medal, and Apurba Nandi. Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*, 172:76 – 94, 2016.
8. L. Jia, Y. Xu, Y. Sun, S. Feng, and A. Anpalagan. Stackelberg game approaches for anti-jamming defence in wireless networks. *IEEE Wireless Communications*, 25(6):120–128, 2018.
9. F. Wang, C. Zhong, M. C. Gursoy, and S. Velipasalar. Defense strategies against adversarial jamming attacks via deep reinforcement learning. In *2020 54th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6, 2020.
10. A. Alagil and Y. Liu. Randomized positioning dsss with message shuffling for anti-jamming wireless communications. In *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8, 2019.
11. N. Van Huynh, D. N. Nguyen, D. Thai Hoang, E. Dutkiewicz, and M. Mueck. Ambient backscatter: A novel method to defend jamming attacks for wireless networks. *IEEE Wireless Communications Letters*, 9(2):175–178, 2020.
12. Wen Li, Yuhua Xu, Qiuju Guo, Yuli Zhang, Dianxiong Liu, Yangyang Li, and Wei Bai. A q-learning-based channel selection and data scheduling approach for high-frequency communications in jamming environment. In Xiangping Bryce Zhai, Bing Chen, and Kun Zhu, editors, *Machine Learning and Intelligent Communications*, pages 145–160, Cham, 2019. Springer International Publishing.
13. Zlatka Valkova-Jarvis, Dimitriya Mihaylova, Albena Mihovska, and Georgi Iliev. Adaptive complex filtering for narrowband jamming mitigation in resource-constrained wireless networks. *Int. J. Interdiscip. Telecommun. Netw.*, 12:46–58, 2020.
14. J. Zhang, T. Q. Duong, A. Marshall, and R. Woods. Key generation from wireless channels: A review. *IEEE Access*, 4:614–626, 2016.
15. S. Chandra, S. Paira, S. S. Alam, and G. Sanyal. A comparative survey of symmetric and asymmetric key cryptography. In *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, pages 83–93, 2014.
16. W. Stallings. *'Cryptography and Network Security: Principles and Practice*. Prentice Hall, New York, NY, USA, 2008.
17. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo. Safeguarding 5g wireless communication networks using physical layer security. *IEEE Communications Magazine*, 53(4):20–27, April 2015.
18. L. Mucchi, F. Nizzi, T. Pecorella, R. Fantacci, and F. Esposito. Benefits of physical layer security to cryptography: Tradeoff and applications. In *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pages 1–3, 2019.
19. L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication. In *2007 IEEE International Conference on Communications*, pages 4646–4651, 2007.
20. A. Abdelaziz, R. Burton, and C. E. Koksal. Poster: Message authentication and secret key agreement in vanets via angle of arrival. In *2016 IEEE Vehicular Networking Conference (VNC)*, pages 1–2, 2016.
21. A. Weinand, R. Sattiraju, M. Karrenbauer, and H. D. Schotten. Supervised learning for physical layer based message authentication in urllc scenarios. In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pages 1–7, 2019.
22. Ning Gao, Qiang Ni, Daquan Feng, Xiaojun Jing, and Yue Cao. Physical layer authentication under intelligent spoofing in wireless sensor networks. *Signal Processing*, 166:107272, 2020.
23. L. Senigagliesi, M. Baldi, and E. Gambi. Performance of statistical and machine learning techniques for physical layer authentication. Jan. 2020, arXiv:2001.06238. [Online].
24. J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo. Physical layer security for the internet of things: Authentication and key generation. *IEEE Wireless Communications*, 26(5):92–98, 2019.
25. C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28(4):656–715, October 1949.
26. A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, October 1975.
27. I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.
28. S. Leung-Yan-Cheong and M. Hellman. The gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 24(4):451–456, July 1978.
29. J. F. Paris. Statistical characterization of $\kappa-\mu$ shadowed fading. *IEEE Transactions on Vehicular Technology*, 63(2):518–526, 2014.
30. M. D. Yacoub. The $\alpha$-$\eta$-$\kappa$-$\mu$ fading model. *IEEE Transactions on Antennas and Propagation*, 64(8):3597–3610, 2016.
31. J. M. Romero-Jerez, F. J. Lopez-Martinez, J. F. Paris, and A. J. Goldsmith. The fluctuating two-ray fading model: Statistical characterization and performance analysis. *IEEE Transactions on Wireless Communications*, 16(7):4420–4432, July 2017.
32. S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, and G. K. Karagiannidis. The fisher–snedecor $\mathcal{F}$ distribution: A simple and accurate

composite fading model. *IEEE Communications Letters*, 21(7):1661–1664, 2017.
33. F. J. Lopez-Martinez, J. M. Romero-Jerez, and J. F. Paris. On the calculation of the incomplete mgf with applications to wireless communications. *IEEE Transactions on Communications*, 65(1):458–469, 2017.
34. J. D. Vega Sanchez, D. P. Moya Osorio, F. Javier Lopez-Martinez, M. C. Paredes Paredes, and L. Urquiza-Aguiar. Information-theoretic security of mimo networks under $\kappa$-$\mu$ shadowed fading channels. May 2020, arXiv:2002.05206. [Online].
35. A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki. On physical layer security of $\alpha$-$\eta$-$\kappa$-$\mu$ fading channels. *IEEE Communications Letters*, 22(10):2168–2171, Oct 2018.
36. W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai. Physical layer security over fluctuating two-ray fading channels. *IEEE Transactions on Vehicular Technology*, 67(9):8949–8953, Sep. 2018.
37. J. D. Vega Sanchez, D. P. Moya Osorio, F. Javier Lopez-Martinez, M. C. Paredes Paredes, and L. Urquiza-Aguiar. On the secrecy performance over N-wave with diffuse power fading channel. Mar. 2020, arXiv:2002.05206. [Online].
38. L. Kong and G. Kaddoum. On physical layer security over the fisher-snedecor $\mathcal{F}$ wiretap fading channels. *IEEE Access*, 6:39466–39472, 2018.
39. F. Ud Din and F. Labeau. Multiple antenna physical layer security against passive eavesdroppers: A tutorial. In *2018 IEEE Canadian Conference on Electrical Computer Engineering (CCECE)*, pages 1–6, May 2018.
40. L. Qing, H. Guangyao, and F. Xiaomei. Physical layer security in multi-hop af relay network based on compressed sensing. *IEEE Communications Letters*, 22(9):1882–1885, Sep. 2018.
41. H. Boche and C. Deppe. Secure identification under passive eavesdroppers and active jamming attacks. *IEEE Transactions on Information Forensics and Security*, 14(2):472–485, Feb 2019.
42. B. Bhushan and G. Sahoo. Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Pers. Commun.*, 98(2):2037–2077, January 2018.
43. Z. Liu, N. Li, X. Tao, S. Li, J. Xu, and B. Zhang. Artificial-noise-aided secure communication with full-duplex active eavesdropper. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–7, Oct 2017.
44. S. Timilsina, G. A. Aruma Baduge, and R. F. Schaefer. Secure communication in spectrum-sharing massive mimo systems with active eavesdropping. *IEEE Transactions on Cognitive Communications and Networking*, 4(2):390–405, June 2018.
45. L. Li, A. P. Petropulu, and Z. Chen. Mimo secret communications against an active eavesdropper. *IEEE Transactions on Information Forensics and Security*, 12(10):2387–2401, Oct 2017.
46. K. N. Le. Performance analysis of secure communications over dual correlated rician fading channels. *IEEE Transactions on Communications*, 66(12):6659–6673, Dec 2018.
47. G. C. Alexandropoulos and K. P. Peppas. Secrecy outage analysis over correlated composite nakagami- $m$ /gamma fading channels. *IEEE Communications Letters*, 22(1):77–80, Jan 2018.
48. K. N. Le and T. A. Tsiftsis. Wireless security employing opportunistic relays and an adaptive encoder under outdated csi and dual-correlated nakagami- $m$ fading. *IEEE Transactions on Communications*, 67(3):2405–2419, March 2019.
49. C. Martins, T. Fernandes, M. Gomes, and J. Vilela. Testbed implementation and evaluation of interleaved and scrambled coding for physical-layer security. In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pages 1–6, 2018.
50. J. Lu, J. Harshan, and F. Oggier. A usrp implementation of wiretap lattice codes. In *2014 IEEE Information Theory Workshop (ITW 2014)*, pages 316–320, 2014.
51. W. Guo, H. Zhao, and Y. Tang. Testbed for cooperative jamming cancellation in physical layer security. *IEEE Wireless Communications Letters*, 9(2):240–243, 2020.
52. J. M. Hamamreh, H. M. Furqan, and H. Arslan. Secure pre-coding and post-coding for ofdm systems along with hardware implementation. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1338–1343, 2017.
53. T. Peng, W. Dai, and M. Z. Win. Efficient and robust physical layer key generation. In *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, pages 1–6, 2019.
54. P. K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory*, 54(10):4687–4698, Oct 2008.
55. M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, June 2008.
56. V. U. Prabhu and M. R. D. Rodrigues. On wireless channels with $M$-antenna eavesdroppers: Characterization of the outage probability and $\varepsilon$-outage secrecy capacity. *IEEE Transactions on Information Forensics and Security*, 6(3):853–860, Sep. 2011.
57. L. Wang. *Physical Layer Security in Wireless Cooperative Networks*. Springer, Cham, Switzerland, 2018.
58. C. R. N. Da Silva, N. Simmons, E. J. Leonardo, S. L. Cotton, and M. D. Yacoub. Ratio of two envelopes taken from $\alpha$ - $\mu$ , $\eta$ - $\mu$ , and $\kappa$ - $\mu$ variates and some practical applications. *IEEE Access*, 7:54449–54463, 2019.
59. J. D. Vega Sanchez, D. P. Moya Osorio, E. E. Benitez Olivo, H. Alves, M. C. Paredes Paredes, and L. Urquiza-Aguiar. On the statistics of the ratio of nonconstrained arbitrary $\alpha$ - $\mu$ random variables: A general framework and applications. *Transactions on Emerging Telecommunications Technologies*, Dec 2019.
60. J. M. Hamamreh, H. M. Furqan, and H. Arslan. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 21(2):1773–1828, Secondquarter 2019.
61. B. He, X. Zhou, and A. L. Swindlehurst. On secrecy metrics for physical layer security over quasi-static fading channels. *IEEE Transactions on Wireless Communications*, 15(10):6913–6924, Oct 2016.
62. L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang. A new metric for measuring the security of an environment: The secrecy pressure. *IEEE Transactions on Wireless Communications*, 16(5):3416–3430, May 2017.
63. R. Zhao, H. Lin, Y. He, D. Chen, Y. Huang, and L. Yang. Secrecy performance of transmit antenna selection for mimo relay systems with outdated csi. *IEEE*

*Transactions on Communications*, 66(2):546–559, Feb 2018.
64. L. Kong, S. Vuppala, and G. Kaddoum. Secrecy analysis of random mimo wireless networks over $\alpha$-$\mu$ fading channels. *IEEE Transactions on Vehicular Technology*, 67(12):11654–11666, Dec 2018.
65. M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante. Maximum secrecy throughput of mimome fso communications with outage constraints. *IEEE Transactions on Wireless Communications*, 17(5):3487–3497, May 2018.
66. X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes. Rethinking the secrecy outage formulation: A secure transmission design perspective. *IEEE Communications Letters*, 15(3):302–304, March 2011.
67. H. Alves, M. De Castro Tomé, P. H. J. Nardelli, C. H. M. De Lima, and M. Latva-Aho. Enhanced transmit antenna selection scheme for secure throughput maximization without csi at the transmitter. *IEEE Access*, 4:4861–4873, 2016.
68. H. Zhao, L. Yang, G. Pan, and M. Alouini. Secrecy outage analysis over fluctuating two-ray fading channels. *Electronics Letters*, 55(15):866–868, 2019.
69. S. Yan, B. He, Y. Cong, and X. Zhou. Covert communication with finite block length in awgn channels. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2017.
70. Z. Li, P. Mu, Z. Li, H. Wang, W. Zhang, and T. Zheng. Nonadaptive transmission for slow fading misose wiretap channel with adjustable power allocation. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–6, Dec 2017.
71. B. He, A. Liu, N. Yang, and V. K. N. Lau. 1on the design of secure non-orthogonal multiple access systems. *IEEE Journal on Selected Areas in Communications*, 135(10):2196–2206, Oct 2017.
72. B. He, X. Zhou, and A. L. Swindlehurst. On secrecy metrics for physical layer security over quasi-static fading channels. *IEEE Transactions on Wireless Communications*, 15(10):6913–6924, Oct 2016.
73. K. T. Phan, Y. Hong, and E. Viterbo. Adaptive resource allocation for secure two-hop relaying communication. *IEEE Transactions on Wireless Communications*, 17(12):8457–8472, Dec 2018.
74. D. P. Moya Osorio, H. Alves, and E. E. Benitez Olivo. On the secrecy performance and power allocation in relaying networks with untrusted relay in the partial secrecy regime. *IEEE Transactions on Information Forensics and Security*, 15:2268–2281, 2020.
75. A. Naeem, M. H. Rehmani, Y. Saleem, I. Rashid, and N. Crespi. Network coding in cognitive radio networks: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 19(3):1945–1973, thirdquarter 2017.
76. J. M. Moualeu, W. Hamouda, and F. Takawira. Intercept probability analysis of wireless networks in the presence of eavesdropping attack with co-channel interference. *IEEE Access*, 6:41490–41503, 2018.
77. Y. Choi and D. Kim. Optimal power and rate allocation in superposition transmission with successive noise signal sharing toward zero intercept probability. *IEEE Wireless Communications Letters*, 7(5):824–827, Oct 2018.
78. F. Jameel, Z. Chang, and T. Ristaniemi. Intercept probability analysis of wireless powered relay system in kappa-mu fading. In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pages 1–6, June 2018.
79. F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Communications Surveys Tutorials*, 21(3):2734–2771, thirdquarter 2019.
80. H. Lei, C. Gao, Y. Guo, and G. Pan. On physical layer security over generalized gamma fading channels. *IEEE Communications Letters*, 19(7):1257–1260, July 2015.
81. H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe. Performance analysis of physical layer security over generalized-$k$ fading channels using a mixture gamma distribution. *IEEE Communications Letters*, 20(2):408–411, Feb 2016.
82. X. Liu. Probability of strictly positive secrecy capacity of the rician-rician fading channel. *IEEE Wireless Communications Letters*, 2(1):50–53, February 2013.
83. Pengcheng Mu, Peizhi Yang, Bo Wang, Hui-Ming Wang, and Qinye Yin. A new scheme to improve the secrecy throughput under the constraints of secrecy outage probability and average transmit power. In *2014 IEEE International Conference on Communications Workshops (ICC)*, pages 777–782, 2014.
84. B. He and X. Zhou. Secure on-off transmission design with channel estimation errors. *IEEE Transactions on Information Forensics and Security*, 8(12):1923–1936, 2013.
85. S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan. Optimization of code rates in sisome wiretap channels. *IEEE Transactions on Wireless Communications*, 14(11):6377–6388, 2015.
86. G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan. Physical layer security in uplink noma multi-antenna systems with randomly distributed eavesdroppers. *IEEE Access*, 7:70422–70435, 2019.
87. Z. Wang, H. Zhao, S. Wang, J. Zhang, and M. Alouini. Secrecy analysis in swipt systems over generalized-$k$ fading channels. *IEEE Communications Letters*, 23(5):834–837, 2019.
88. T. Zheng, H. Wang, D. W. K. Ng, and J. Yuan. Physical-layer security in the finite blocklength regime over fading channels. *IEEE Transactions on Wireless Communications*, 19(5):3405–3420, 2020.
89. K. Jiang, W. Zhou, and L. Sun. Jamming-aided secrecy performance in secure uplink noma system. *IEEE Access*, 8:15072–15084, 2020.
90. K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis. Physical layer security jamming: Theoretical limits and practical designs in wireless networks. *IEEE Access*, 5:3603–3611, December 2017.
91. T. V. Pham, T. Hayashi, and A. T. Pham. Artificial-noise-aided precoding design for multi-user visible light communication channels. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, May 2018.
92. S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan. Three artificial-noise-aided secure transmission schemes in wiretap channels. *IEEE Transactions on Vehicular Technology*, 67(4):3669–3673, April 2018.
93. Y. Gu, Z. Wu, Z. Yin, and X. Zhang. The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in mimo system. *IEEE Access*, 7:58353–58360, March 2019.
94. D. P. Moya Osorio, J. D. Vega, and H. Alves. *Physical-Layer Security for 5G and Beyond in 5G REF: The*

*Essential 5G Reference Online*. John Wiley & Sons, 2019.
95. A. Mukherjee and A. L. Swindlehurst. Robust beamforming for security in mimo wiretap channels with imperfect csi. *IEEE Transactions on Signal Processing*, 59(1):351–361, Jan 2011.
96. T. Lv, H. Gao, and S. Yang. Secrecy transmit beamforming for heterogeneous networks. *IEEE Journal on Selected Areas in Communications*, 33(6):1154–1170, June 2015.
97. W. Zhang, J. Chen, Y. Kuo, and Y. Zhou. Transmit beamforming for layered physical layer security. *IEEE Transactions on Vehicular Technology*, 68(10):9747–9760, Oct 2019.
98. F. He, H. Man, and W. Wang. Maximal ratio diversity combining enhanced security. *IEEE Communications Letters*, 15(5):509–511, May 2011.
99. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, 58(3):1875–1888, March 2010.
100. M. Chraiti, A. Ghrayeb, C. Assi, and M. O. Hasna. On the achievable secrecy diversity of cooperative networks with untrusted relays. *IEEE Transactions on Communications*, 66(1):39–53, Jan 2018.
101. R. Zhao, X. Tan, D. Chen, Y. He, and Z. Ding. Secrecy performance of untrusted relay systems with a full-duplex jamming destination. *IEEE Transactions on Vehicular Technology*, 67(12):11511–11524, Dec 2018.
102. R. F. Schaefer, G. Amarasuriya, and H. V. Poor. Physical layer security in massive mimo systems. In *2017 51st Asilomar Conference on Signals, Systems, and Computers*, pages 3–8, Oct 2017.
103. A. Al-Dulaimi, X. Wang, and C. Lin. *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*. John Wiley & Sons Inc, New Jersey, NJ, USA, 2018.
104. J. Zhu, R. Schober, and V. K. Bhargava. Secure transmission in multicell massive mimo systems. *IEEE Transactions on Wireless Communications*, 13(9):4766–4781, Sep. 2014.
105. Y. Liu, H. Chen, and L. Wang. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys Tutorials*, 19(1):347–376, Firstquarter 2017.
106. W. Wu, X. Gao, Y. Wu, and C. Xiao. Beam domain secure transmission for massive mimo communications. *IEEE Transactions on Vehicular Technology*, 67(8):7113–7127, Aug 2018.
107. X. Zhang, D. Guo, and K. Guo. Secure performance analysis for multi-pair af relaying massive mimo systems in ricean channels. *IEEE Access*, 6:57708–57720, 2018.
108. N. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and K. Tourki. Secure massive mimo with the artificial noise-aided downlink training. *IEEE Journal on Selected Areas in Communications*, 36(4):802–816, April 2018.
109. J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava. Analysis and design of secure massive mimo systems in the presence of hardware impairments. *IEEE Transactions on Wireless Communications*, 16(3):2001–2016, March 2017.
110. T. Yang, R. Zhang, X. Cheng, and L. Yang. Performance analysis of secure communication in massive mimo with imperfect channel state information. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2018.
111. H. Wei, D. Wang, X. Hou, Y. Zhu, and J. Zhu. Secrecy analysis for massive mimo systems with internal eavesdroppers. In *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, pages 1–5, Sep. 2015.
112. B. Akgun, M. Krunz, and O. Ozan Koyluoglu. Vulnerabilities of massive mimo systems to pilot contamination attacks. *IEEE Transactions on Information Forensics and Security*, 14(5):1251–1263, May 2019.
113. X. Zhou, B. Maham, and A. Hjorungnes. Pilot contamination for active eavesdropping. *IEEE Transactions on Wireless Communications*, 11(3):903–907, March 2012.
114. D. Hu, W. Zhang, L. He, and J. Wu. Secure transmission in multi-cell multi-user massive mimo systems with an active eavesdropper. *IEEE Wireless Communications Letters*, 8(1):85–88, Feb 2019.
115. D. Kudathanthirige, S. Timilsina, and G. A. Aruma Baduge. Secure communication in relay-assisted massive mimo downlink with active pilot attacks. *IEEE Transactions on Information Forensics and Security*, 14(11):2819–2833, Nov 2019.
116. F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian. Robust beamforming for physical layer security in bdma massive mimo. *IEEE Journal on Selected Areas in Communications*, 36(4):775–787, April 2018.
117. R. Wu, S. Yuan, and C. Yuan. Secure transmission against pilot contamination: A cooperative scheme with multiple antennas. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 00052–00057, June 2018.
118. G. J. Anaya-Lopez, G. Gomez, and F. Javier Lopez-Martinez. A product channel attack to wireless physical layer security. Jul 2020, arXiv:2007.08162 [Online].
119. Y. Wu, C. Wen, W. Chen, S. Jin, R. Schober, and G. Caire. Data-aided secure massive mimo transmission with active eavesdropping. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2018.
120. L. D. H. Sampaio, T. Abrao, and F. R. Durand. Game theory based resource allocation in multi-cell massive mimo ofdma networks. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, March 2017.
121. T. Rappaport, R. Heath, R. Daniels, and J. Murdock. Mimo for millimeter-wave wireless communications: Beamforming, spatial multiplexing, or both? *IEEE Communications Magazine*, 52(12):110–121, Dec 2014.
122. H.-M. Wang and T.-X. Zheng. *Physical Layer Security in Random Cellular Networks*. Springer, Singapore, 2016.
123. Z. Lin, X. Du, H. Chen, B. Ai, Z. Chen, and D. Wu. Millimeter-wave propagation modeling and measurements for 5g mobile networks. *IEEE Wireless Communications*, 26(1):72–77, February 2019.
124. Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao. A survey of physical layer security techniques for 5g wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, 36(4):679–695, April 2018.
125. T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez. Millimeter wave mobile communications for 5g cellular: It will work! *IEEE Access*, 1:335–349, 2013.
126. S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, and L. Jin. Artificial noise aided hybrid analog-digital beamforming

for secure transmission in mimo millimeter wave relay systems. *IEEE Access*, 7:28597–28606, 2019.
127. Y. Ju, H. Wang, T. Zheng, Q. Yin, and M. H. Lee. Safeguarding millimeter wave communications against randomly located eavesdroppers. *IEEE Transactions on Wireless Communications*, 17(4):2675–2689, April 2018.
128. M. E. Eltayeb and R. W. Heath. Securing mmwave vehicular communication links with multiple transmit antennas. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, May 2018.
129. S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu. On the physical layer security analysis of hybrid millimeter wave networks. *IEEE Transactions on Communications*, 66(3):1139–1152, March 2018.
130. K. Xiao, W. Li, M. Kadoch, and C. Li. On the secrecy capacity of 5g mmwave small cell networks. *IEEE Wireless Communications*, 25(4):47–51, AUGUST 2018.
131. M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder. 5g: A tutorial overview of standards, trials, challenges, deployment, and practice. *IEEE Journal on Selected Areas in Communications*, 35(6):1201–1221, June 2017.
132. R. I. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, and J. J. P. C. Rodrigues. 5g d2d networks: Techniques, challenges, and future prospects. *IEEE Systems Journal*, 12(4):3970–3984, Dec 2018.
133. D. Lopez-Perez, I. Guvenc, G. de la Roche, M. Kountouris, T. Q. S. Quek, and J. Zhang. Enhanced intercell interference coordination challenges in heterogeneous networks. *IEEE Wireless Communications*, 18(3):22–30, June 2011.
134. L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong. Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks. *IEEE Transactions on Wireless Communications*, 17(2):736–751, Feb 2018.
135. L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong. Secure video streaming in heterogeneous small cell networks with untrusted cache helpers. *IEEE Transactions on Wireless Communications*, 17(4):2645–2661, April 2018.
136. Y. Zou, M. Sun, J. Zhu, and H. Guo. Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks. *IEEE Transactions on Wireless Communications*, 17(12):8444–8456, Dec 2018.
137. W. Wang, K. C. Teh, S. Luo, and K. H. Li. Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach. *IEEE Transactions on Communications*, 66(12):6437–6449, Dec 2018.
138. S. Wang, Y. Gao, N. Sha, G. Zhang, H. Luo, and Y. Chen. Physical layer security in two-tier heterogeneous cellular networks over nakagami channel during uplink phase. In *2018 10th International Conference on Communication Software and Networks (ICCSN)*, pages 1–5, July 2018.
139. N. Wu, X. Zhou, and M. Sun. Secure transmission with guaranteed user satisfaction in heterogeneous networks: A two-level stackelberg game approach. *IEEE Transactions on Communications*, 66(6):2738–2750, June 2018.
140. A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. Wong. Full-duplex small-cell networks: A physical-layer security perspective. *IEEE Transactions on Communications*, 66(7):3006–3021, July 2018.
141. S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst. Secret channel training to enhance physical layer security with a full-duplex receiver. *IEEE Transactions on Information Forensics and Security*, 13(11):2788–2800, Nov 2018.
142. J. Kim, J. Kim, J. Lee, and J. P. Choi. Physical-layer security against smart eavesdroppers: Exploiting full-duplex receivers. *IEEE Access*, 6:32945–32957, 2018.
143. Y. Luo, Z. Feng, H. Jiang, Y. Yang, Y. Huang, and J. Yao. Game-theoretic learning approaches for secure d2d communications against full-duplex active eavesdropper. *IEEE Access*, 7:41324–41335, 2019.
144. A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. Wong. Full-duplex small-cell networks: A physical-layer security perspective. *IEEE Transactions on Communications*, 66(7):3006–3021, July 2018.
145. P. Anokye, R. K. Ahiadormey, C. Song, and K. Lee. Achievable sum-rate analysis of massive mimo full-duplex wireless backhaul links in heterogeneous cellular networks. *IEEE Access*, 6:23456–23469, 2018.
146. F. Tian, X. Chen, S. Liu, X. Yuan, D. Li, X. Zhang, and Z. Yang. Secrecy rate optimization in wireless multi-hop full duplex networks. *IEEE Access*, 6:5695–5704, 2018.
147. Y. Dong, A. E. Shafie, M. J. Hossain, J. Cheng, N. Al-Dhahir, and V. C. M. Leung. Secure beamforming in full-duplex swipt systems with loopback self-interference cancellation. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2018.
148. W. Liang, Z. Ding, and H. V. Poor. *, Non-Orthogonal Multiple Access (NOMA) for 5G Systems*. Cambridge University Press, 2017.
149. Y. Zhang, H. Wang, Q. Yang, and Z. Ding. Secrecy sum rate maximization in non-orthogonal multiple access. *IEEE Communications Letters*, 20(5):930–933, May 2016.
150. B. Su, Q. Ni, and B. He. Robust transmit designs for secrecy rate constrained miso noma system. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 1–5, Sep. 2018.
151. J. Tang, T. Dai, M. Cui, X. Y. Zhang, A. Shojaeifard, K. Wong, and Z. Li. Optimization for maximizing sum secrecy rate in swipt-enabled noma systems. *IEEE Access*, 6:43440–43449, July 2018.
152. G. Chopra, R. K. Jha, and S. Jain. Rank-based secrecy rate improvement using noma for ultra dense network. *IEEE Transactions on Vehicular Technology*, 68(11):10687–10702, Nov 2019.
153. K. Jiang, T. Jing, Y. Huo, F. Zhang, and Z. Li. Sic-based secrecy performance in uplink noma multi-eavesdropper wiretap channels. *IEEE Access*, 6:19664–19680, 2018.
154. J. Tang, L. Jiao, N. Wang, P. Wang, K. Zeng, and H. Wen. Mobility improves noma physical layer security. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, Dec 2018.
155. C. Du, F. Zhang, S. Ma, Y. Tang, H. Li, H. Wang, and S. Li. Secure transmission for downlink noma visible light communication networks. *IEEE Access*, 7:65332–65341, May 2019.
156. L. Wei, T. Jing, X. Fan, Y. Wen, and Y. Huo. The secrecy analysis over physical layer in noma-enabled cognitive radio networks. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2018.
157. Z. Bai, B. Li, M. Yang, Z. Yan, X. Zuo, and Y. Zhang. Fh-scma: Frequency-hopping based sparse code multiple access for next generation internet of things. In *2017*

*IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2017.