Physical Layer Security for 5G Wireless Networks: A Comprehensive Survey

José David Vega Sánchez
Dept. Electrónica,
Telecomunicaciones y Redes
Escuela Politécnica Nacional
Quito, Ecuador
jose.vega01@epn.edu.ec

Luis Urquiza-Aguiar
Dept. Electrónica,
Telecomunicaciones y Redes
Escuela Politécnica Nacional
Quito, Ecuador
luis.urquiza@epn.edu.ec

Martha Cecilia Paredes Paredes
Dept. Electrónica,
Telecomunicaciones y Redes
Escuela Politécnica Nacional
Quito, Ecuador
cecilia.paredes@epn.edu.ec

***Abstract*—Physical-layer security is emerging approach that can benefit conventional encryption methods. The main idea of physical layer security is to take advantage of the features of the wireless channel and its impairments in order to ensure secure communication in the physical layer. This paper provides a comprehensive review of information-theoretic measures of the secrecy performance in physical layer security. In addition, our work survey research about physical layer security over several enabling 5G technologies, such as massive multiple-input multiple-output, millimeter wave communications, heterogeneous networks, and full-duplex, including the key concepts of each of the aforementioned technologies. Finally, future research directions and technical challenges of physical layer security are identified.**

***Index Terms*—5G systems, Physical layer security, heterogeneous networks, massive MIMO, millimeter-Wave, full-duplex.**

I. Introduction

In wireless communications, the continuously increasing demands for wireless applications and the exponential growth of the number of connected users have saturated the capacity of current communication systems. These pivotal issues motivate to researchers and network designers to search for novel solutions that guarantee ultra-high data rate, ultra-wide radio coverage, a massive number of efficiently connected devices, ultra-low latency, and efficient energy consumption. In this context, the fifth generation of wireless networks (5G) foresees great advances in solutions that use intelligent and efficient technologies, which will allow promoting economic and social growth on a global scale in very innovative ways [1]. Accordingly, 5G must be prepared to face with major challenges with respect to the reliability, security, and efficiency of the network, in order to meet the high requirements imposed by its implementation. Specifically, the security paradigm protecting the confidentiality of wireless communication is one of the core problems to be considered in 5G [2]. Unlike from the traditional security systems that are based on higher layer cryptographic mechanisms [3], which employ mathematically complex algorithms, physical layer security (PLS) emerges as a strategy that offers secure wireless communications by smartly operating the impairments of the channel [2]. In particular, PLS provides a great advantage compared to cryptography, since it does not depend on computational complexity. Therefore, the level of security achieved will not be affected even if the eavesdropper has powerful computing capabilities. This contrasts with encryption-based approach, which is based on the idea that eavesdropper has limited computational capabilities to solve difficult mathematical problems in limited periods [4].

Cornerstone ideas of PLS are from the seminal paper of Shannon, who laid the basis of secrecy systems [5]. Later, the well-known wiretap channel was introduced by Wyner in 1975 [6]. In that work, Wyner defines that secret messages can be sent by guaranteeing that 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 this data being able to be decoded by an eavesdropper. Nevertheless, in real environments, due to the fading, random location, and broadcast nature of the wireless medium, the condition of eavesdropper's channel can be similar or even better than the legitimate channel, particularly when the eavesdropper is closer to the transmitter than the legitimate receiver. So, the Wyner's ideas become impracticable in such environments. Inspired by Wyner's work, investigations of the attainable secrecy capacity against eavesdropping were addressed in [7] for the broadcast channel, and for the Gaussian channel in [8]. These approaches have inspired an important amount of recent research activities from an information theoretic point of view for different types of channels (e.g., κ-μ shadowed, α-η-κ-μ, Fluctuating Two-Ray, and Fisher-Snedecor $\mathcal{F}$) [9]–[12], and network topologies (e.g., Full-Duplex, multiple-input multiple-output (MIMO) Transmit Antenna Selection/ Maximal Ratio Combining (TAS/MRC), and Cognitive Radio Systems) [13]–[18].

The aim of this paper is to provide a comprehensive survey

This is the authors' version of the accepted manuscript for CSNET 2019. The authors gratefully acknowledge the financial support provided by the Escuela Politécnica Nacional, for the development of the project PIJ-16-01-"Modelamiento de la Packet Error Rate (PER) incluyendo condiciones de Peak-to-Average Power Ratio (PAPR) para transmisiones Ad-Hoc". José David Vega Sánchez is the recipient of a teaching assistant fellowship from Escuela Politéecnica Nacional for doctoral studies in Electrical Engineering.

of PLS on enabling technologies for 5G. Firstly, the main PLS performance metrics are introduced, including secrecy capacity, secrecy outage probability, intercept probability, and the probability of strictly positive secrecy capacity. A brief background on these metrics are also provided. Then, 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 (HetNet), and full-duplex (FD). Subsequently, we summarize the latest PLS research advances on the aforementioned 5G technologies.

The rest of the paper is organized as follows. Section II presents some fundamentals for PLS and reviews the main secrecy performance metrics. Section III summarizes concepts of promising 5G technologies and presents the recent advances in PLS research on these key 5G technologies. Section IV presents some of the open challenges in wireless security communications, and provides some concluding remarks.

II. FUNDAMENTALS OF PHYSICAL LAYER SECURITY

This section introduces key concepts for understanding information theoretic security in wireless communications systems.

A. General System Model

The general PLS model consists of three main communication nodes as depicted in Fig. 1.

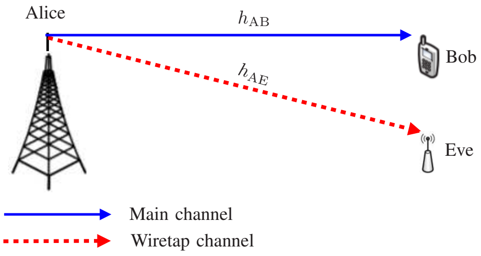


Fig. 1. The system model of a wiretap channel consisting of two legitimate correspondents and an eavesdropper.

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 main channel, while the link between Alice and Eve is called the wiretap channel (also known as Eavesdropper channel). In this setup, the transmitter (Alice) sends a confidential message to the legitimate receiver (Bob), while the eavesdropper (Eve) receives the signal and intends to decode it. Therefore, Alice's goal is to use a transmission approach that can deliver the uncharted secret information to Bob, while making sure that Eve can not decode the transmitted secret information. 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, diversity, among others. Another important aspect to take into account in the system model (see, Fig. 1) is the availability of channel state information (CSI) at the nodes varies from complete to partial to even zero knowledge. This fact is important because if the CSI of the main channel is available, Alice can decide whether or not transmit and at which rate, thus attaining a considerable reduce on the secrecy outage probability. However, in real communication systems, all nodes can only obtain some kind of information about the channel between them and the other nodes. Furthermore, Alice is typically assumed to know Bob's channel but not to know Eve's channel. This is because Eve is usually passive (i.e., Eve monitors the network, intercepts messages and does not communicate with other nodes in the system). Several works such as [23]–[25] 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 [19]. Performance analysis of PLS, which consider Alice knows Eve's channel (i.e., active eavesdropper) can be found in [20]–[22]. It is worthwhile to mention that in the performance evaluations of PLS, 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). On the other hand, the links (i.e., Alice-to-Bob and Alice-to-Eve) do not meet the aforementioned condition (i.e., correlated channels) are investigated in [26]–[28].

B. Performance Metrics

Some of the main secrecy performance metrics most used in the literature are explained in this section. A good knowledge of these metrics will ease the understanding of the works to be addressed in the following sections,

1) Secrecy Capacity: The secrecy capacity C_S for a wireless channel is the most used metric in PLS evaluation. C_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 message reliably recovers at Bob while remaining unrecoverable at Eve [29]. Mathematically, the secrecy capacity for a channel in a quasi-static fading scenario is given as in [6] by

$$\begin{aligned}C_S =& \max\{C_B - C_E, 0\}\\ =& \max\left\{W\log_2\left(1+\frac{|h_{\mathrm{AB}}|^2 P_{\mathrm{A}}}{N_0}\right) - W\log_2\left(1+\frac{|h_{\mathrm{AE}}|^2 P_{\mathrm{A}}}{N_0}\right), 0\right\}\\ =& \max\{W\log_2(1+\gamma_B) - W\log_2(1+\gamma_E), 0\} \qquad (1)\end{aligned}$$

where $|\cdot|$ is the absolute value, $\gamma_X = \frac{|h_{\mathrm{AX}}|^2 P_{\mathrm{A}}}{N_0}$ for $X \in \{B, E\}$ is signal-to-noise ratio (SNR), h_{AB} and h_{AE} are the channel coefficients of the main and wiretap channels, respectively. P_{A} is the transmit power at Alice, N_0 is the average noise power, and C_B and C_E are the capacities of the main and wiretap channels, respectively. Without loss of generality, it is assumed a normalized bandwidth $W = 1$ in the previous capacity definitions. In this scenario, it is possible to attain secure communications only if the main link has a better SNR than the wiretap link, i.e.,

$$C_S = \begin{cases} \log_2\left(\frac{1+\gamma_B}{1+\gamma_E}\right), & \text{if } \gamma_B > \gamma_E \\ 0, & \text{if } \gamma_B \leq \gamma_E, \end{cases} \tag{2}$$

It is worth mentioning that secrecy capacity is widely extended by researchers to secrecy outage probability (SOP) in order to measure the resulting secrecy in different network typologies [30].

2) Secrecy Outage Probability: The SOP is defined as the probability that the secrecy capacity falls below a target secrecy rate threshold R_{th}. In other words, when the current secrecy capacity C_S is not more than a pre-established threshold R_{th}, the secrecy outage happens, which means the current secrecy rate cannot guarantee the security requirement. It can be formulated as in [31] by

$$\begin{aligned} \text{SOP} &= \Pr\left\{C_S\left(\gamma_B, \gamma_E\right) < R_{th}\right\} \\ &= \Pr\left\{\left(\frac{1+\gamma_B}{1+\gamma_E}\right) < 2^{R_{th}}\right\} \end{aligned} \tag{3}$$

where $\Pr\{\cdot\}$ indicates probability. The SOP in (3) indicates that whenever $C_S < R_{th}$, the wiretap channel will be worse than the main channel, so a secure communication is possible [32]. Despite of the important insights that the SOP provides in the characterization of the security performance of wireless communications, it has the following drawbacks: $i)$ it lacks the ability to quantify the amount of information leaking to the eavesdroppers when the outage occurs; $ii)$ it cannot offer any information about the eavesdropper's ability to decode confidential messages successfully; $iii)$ it cannot be directly linked to the Quality of Service (QoS) requirements for different services [33]. Motivated by the limitations of the secrecy outage probability, the authors in [34], [35] proposed new metrics to overcome the three aforementioned demerits of the SOP. Thus, the authors give more insights into physical layer security and how secrecy is measured. It is worthwhile to mention that the concept of secrecy outage probability and secrecy outage capacity can also be extended to the case with multiple antennas at different nodes. Readers are referred to [36]–[38] for further studies on this topic. Next, according to the classical SOP defined above, alternative secrecy outage formulations from (3) are defined to follow.

3) Intercept Probability: An intercept event occurs when the C_S is negative or falls below 0, which means that the wiretap channel has a better SNR than the main channel, it can be expressed as in [39] by

$$P_{int} = \Pr\left\{C_S\left(\gamma_B, \gamma_E\right) < 0\right\} \tag{4}$$

Although this metric has not been widely explored in the literature, it is currently being investigated in evaluating and characterizing the security performance of wireless channels. Readers are referred to [40]–[42] for more detailed information of this field of research.

4) Probability of Strictly Positive Secrecy Capacity: The Probability of strictly positive secrecy capacity (SPSC) is the probability that the secrecy capacity C_S remains higher than 0, which means that security in communication has been attained[1]. Mathematically, it can be written as in [43] by

$$P_{SPSC} = \Pr\left\{C_S\left(\gamma_B, \gamma_E\right) > 0\right\} \tag{5}$$

In [44]–[46], researchers investigated the security performance of wireless systems based on the SPSC metric over different fading channels models.

III. Next Generation Physical Layer Technologies

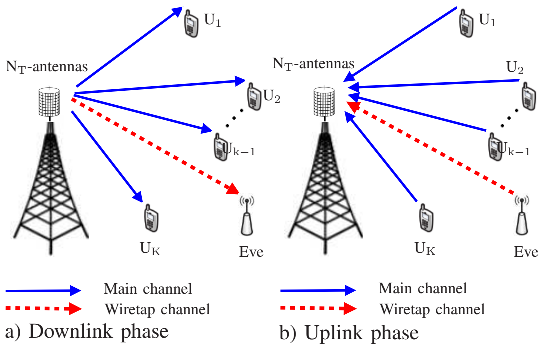
Future mobile networks are expected to achieve high capacity rates and reduced latency to support the rapid growth of data traffic. The combination of 5G key technologies is considered as a cost-effective solution to fulfill these stringent requirements in the 5G wireless networks. However, the dramatically increasing in the data amount and complex communication environment put forward higher requirements on the security of mobile communications. In this section, we review the concepts of each of the promising enabling technologies for 5G, including their advantages and disadvantages. Next, we summarize the latest research results of PLS from the point of view of 5G technologies.

A. Massive MIMO

Massive MIMO is a multi-user scheme in which the base station (BS) is equipped with an big number of antennas as depicted in Fig. 2. These arrangement provide several degrees of freedom for wireless systems, better performance in channel capacities and improve communication qualities in the 5G networks [48]. For security purposes, massive MIMO gives very directed beam patterns to the location of the legitimate user so that the information leakage is reduced to undesired locations (i.e., Eve) significantly [49].

The authors in [47] were the first to investigate the drawbacks of PLS performance when the number of antennas approaches infinity in massive MIMO scenarios. Compared to tradicional MIMO, the massive MIMO introduces the following challenges: 1) the CSI estimation process is highly complex; 2) the channels models are correlated as the distances of antennas are very shorter than a half of the wavelength. Therefore, massive MIMO is still an open research field [50]. Next, we survey the current security attacks of massive MIMO technology based on passive and active eavesdropper scenarios, respectively.

[1] The authors in [33] provide the theoretical meaning as well as the mathematical expressions to quantify the secrecy capacity (e.g., perfect secrecy, ideal secrecy, weak secrecy, strong secrecy), when the C_S is greater than zero.



a) Downlink phase

b) Uplink phase

Fig. 2. Massive MIMO downlink with K legitimate user nodes, $\mathrm{U_k}$ for $\mathrm{k} = 1, \cdots, \mathrm{K}$, and an eavesdropper.

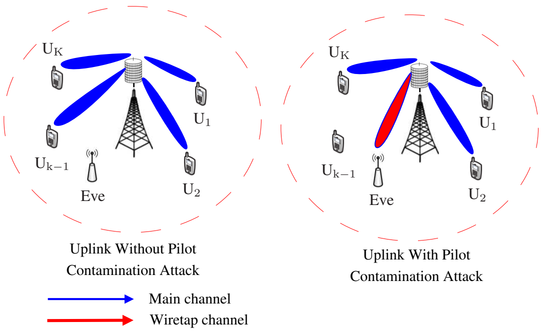
1) Passive Eavesdropper Scenarios: The key concept here is that the existence of a passive eavesdropper does not affect at all the beam of transmission at the BS, so it has a negligible effect on the secret capacity. Recently, in [51] was developed an algorithm to optimize power allocation of beam transmission for single-cell massive MIMO in presence of passive eavesdropper with multiple antennas. The results showed that beam domain transmission can achieve optimal performance in terms of secrecy capacity. Authors in [52] investigated secure transmissions of multi-pair massive MIMO AF relaying system over Ricean fading channels, where using a simple power control scheme the achievable sum secrecy rate is maximized. The use of artificial noise (AN)-aiding schemes to degrade the eavesdropping channel to improve the security in massive MIMO was analyzed in [53].

Other massive MIMO approaches with passive eavesdroppers include: impact of hardware deficiencies on the secret performance of massive downlink MIMO systems in the existence of eavesdropper with multiple antennas [54], performance analysis of wireless communications in a multi-user massive MIMO by considering imperfect CSI [55], secrecy outage probability analysis performance for massive MIMO scenarios [56], etc.

2) Active Eavesdropper Scenarios: A large number of PLS research works assume that the perfect CSI of the legitimate node channel is available in the transmitter and do not take into account the process for obtaining this channel information. In time duplex division (TDD) massive MIMO systems, during the uplink phase, legitimate nodes transmit pilot signals to the BS to estimate the channel for the later transmission of the downlink. At the same time, an active eavesdropper can interfere in the training phase to cause pilot contamination at the transmitter BS (see, for instance, Fig. 3). This forces in the transmission phase (i.e., downlink) of the BS to inherently beamform towards the eavesdropper, so increasing its received signal power [57]. This fact compromises that a positive secrecy rate may not be achievable. The result of this attack is that the advantages of PLS for massive MIMO are lost [58]. To circumvent the referred limitation, the following works investigated techniques to avoid the pilot contamination attack (PCA). In [59], the authors proposed a reliable communication that does not require statistical information about the links for a TDD massive MIMO with an active eavesdropper. In the proposed transmission scheme, an asynchronous protocol is used instead of the conventional synchronous protocol. A transmit power control policy was designed in [60] to efficiently allocate transmit power at the BS/relay for payload data and AN sequences for maximizing the achievable secrecy rate in Massive MIMO Downlink. For PLS in massive MIMO, in [61] was designed robust scheme together with AN beamforming to offer legitimate nodes and eavesdroppers with different signal-to-interference-and-noise ratio (SINR), while minimizing the transmit power of BS.

In [7] was designed simultaneous robust information and AN beamforming to offer the legiteme nodes and Eavesdropper with different signal-to-interference-and-noise ratio (SINR), meanwhile minimizing the transmit power of BS.

Other secure massive transmissions against active eavesdropper include: cooperative scheme strategy [62], data-aided secure downlink transmission scheme [63], and the secure communications design based on game theory [64], etc.



Uplink Without Pilot Contamination Attack

Uplink With Pilot Contamination Attack

Fig. 3. Pilot Contamination Attack on massive MIMO systems.

B. *mm-Wave*

Nowadays, most wireless systems are allocated in the band spectrum of 300 MHz to 3 GHz, which is extremely full. In this context, millimeter-Wave (mm-Wave)[2] is a very innovative key solution for 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 band, ranging from 3-300 GHz to cope with future multi-gigabit-per-second mobile, imaging, and multimedia applications. Compared to microwave networks, mm-Wave networks have several novel features, such as large number of antennas[3], short range, different propagation laws, highly dense mm-Wave small cells, and beamforming as the main technique, which denotes that mm-Wave networks are implicitly directional [67].The adoption of PLS mm-Wave

[2] In order to have more detailed framework about millimeter wireless communication systems, we refer the reader to [65].

[3] 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 physical layer with massive MIMO, small cell geometries (which will be described later), and mm-Wave has the potential to further enhance the security of wireless networks, wireless access, and throughput [66].

networks systems is a remarkably emerging topic of research. The general model of PLS for mm-Wave, massive MIMO, Full-Duplex, and Small Cells for 5G is presented in Fig. 4. Several approaches have been developed in this domain[4], here we review some of the current works to highlight the potential of this emerging field. Most of the current research is focused on the 28, 38, and 60 GHz band [69].

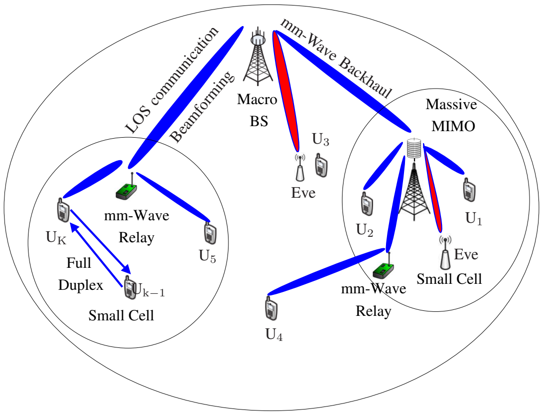


Fig. 4. Illustration of promising technologies (e.g., mm-Wave, massive MIMO, Full Duplex, and Small Cells) in 5G networks.

In [70], in order to maximize the signal power of interest and neglect interference among different data flows (i.e., to improve the secrecy capacity), the authors proposed an AN aided two stages secure hybrid beamforming algorithm in MIMO mm-Wave relay eavesdropping scenario. Here, the combination of two stage hybrid beamforming algorithm with AN allows guaranteeing both high throughput and communication security. Next, based on multi-input single-output (MISO) mm-Wave system, where multiple single-antenna eavesdroppers are randomly located, the authors in [71] investigated secure communications techniques: maximum ratio transmitting (MRT) beamforming and AN beamforming. Particularly, it was developed the optimal power allocation between AN and the signal of interest that maximizes the secrecy throughput for AN beamforming. With regard to vehicular environments, in [72], the researchers proposed a location-based PLS technique for secure mm-Wave vehicular communication. Such a proposed technique takes advantage of the large antenna at the mm-Wave frequencies to jam eavesdroppers with sensitive receivers. The technique proved to offer good performance in terms of safety when an eavesdropper can have access to the direct path either by directly intercepting it or via a reflected path.

Other approaches include: PLS Analysis of Hybrid Millimeter Wave Networks [73], secrecy capacity of 5G mm-Wave Small Cells [74].

C. Heterogeneous Networks - Small Cells

Traditionally, macro cellular network is efficient in providing 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 size of the cell in future wireless networks [75]. In this context, the Heterogeneous Networks (HetNet) will perform a pivotal role to meet the demands of 5G. The goal of HetNet is to offer a spectrum efficient solution that satisfies the spectacular growth of the data demands of the upcoming wireless services. In the HetNet topology, users with different capabilities (i.e., transmission powers, coverage areas, etc.) are implemented to be part of a multi-tier hierarchical architecture, as depicted in Fig. 5. The high-power nodes (HPNs) with broad radio coverage fields are located in macro cell, meanwhile low-power nodes (LPNs) with limited radio coverage fields are located in small cells [4]. The small cells (typically with coverage of a few meters) can have different configurations, the femto cells that are usually used in homes and development companies, and the pico cells that are used for ample outdoor coverage or to fill the empty spaces of macro cell coverage [75]. In addition, HetNet includes a device level that supports device-to-device (D2D) communications. D2D communication favors nearby devices to connect directly and collaborate with each other without using HPNs/LPNs, making them a powerful tool of low-latency, and high-performance data services [76].

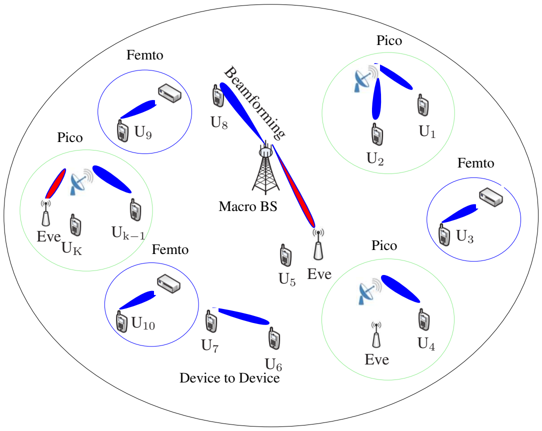


Fig. 5. A 4-tier macro/pico/femto/D2D heterogeneous network with users and eavesdroppers.

On the other hand, the multi-tier topology in HetNet entails technical challenges (e.g., self-organization, backhauling, handover, and interference) to the investigation of PLS compared to the traditional single-tier architecture [77]. Then, we review the most current works that address the aforementioned challenges in HetNet in the field of PLS. In two novel approaches [78], [79], PLS in a multi-cell wireless caching network has been studied. The researchers have taken advantage of cooperative multi-antenna transmissions to improve the secrecy capacity against a single eavesdropper in [78] and multiple non-reliable cache helpers in [79]. In [80], the authors proposed an interference-canceled opportunistic antenna selection (IC-OAS) scheme to enhance PLS for the HetNet, where a passive eavesdropper is assumed to tap the transmissions of both the macro cell and small cell. Here, it was shown

[4] For a good summary of works about the beginnings of PLS in mm-Wave, we refer the reader to the survey in [68].

that the IC-OAS method outperforms the conventional IC-OAS scheme not only brings security-reliability tradeoff benefits to the macro cell, but also has the potential of improving the security-reliability tradeoff of small cell.

Other secure communications works in HetNet systems include: Stochastic Geometry strategies [81], secrecy outage analysis over Nakagami-m fading channels [82], and secure communications design based on game theory [83], etc.

D. Full-Duplex

Among the promising technologies for 5G, the Full Duplex (FD) technology carries both opportunities and challenges for PLS communications. On one hand, FD allows the destination node to create AN to interfere with the eavesdropper and receive the information at the same time. On the other hand, if the eavesdropper has the FD technology, it can actively attack the receiver in the transmission process while eavesdropping. In addition, FD communications can double the spectral efficiency with regard to the traditional half-duplex communications. However, the main drawback that affects the transmission of FD is the management of the strong self-interference signal imposed by the transmission antenna on the receiving antenna within the same transceiver [84]. The research on FD PLS communication can be classified in four categorizations of FD PLS communications, including the FD receiver, the FD transmitter and receiver, the FD BS, and the FD eavesdropper [68]. Next, we review the most current works with regard to the different configurations aforementioned FD technology. In [85], the authors proposed a novel channel training (CT) scheme for a full-duplex receiver to improve PLS. In this setup, the receiver (i.e., Bob) is equipped with N_B antennas, so it can simultaneously receive the information signal and transmits AN to the eavesdropper. Here, in order to diminish the non-cancelable self-interference due to the transmitted AN, the the destination node has to estimate the self-interference channel prior to the data communication phase. In [86] was considered a problem of a passive and smart eavesdropping attack on MIMO wiretap scenario, where the receiver operates with FD mode. In such a system model, the smart eavesdropper can cancel jamming (caused by the receiver) by stealing the CSI between legitimate nodes. To counteract this, the authors proposed a cooperative jamming solution between transceivers to achieve the optimal secrecy performance. With regard to FD active eavesdropper (FDAE), in [87], was analyzed the anti-eavesdropping and anti-jamming performance of D2D communications. In this scenario, the FDAE can passively intercept confidential messages in D2D communications and actively jam all legitimate channels. In this respect, the authors proposed a hierarchical and heterogeneous power control mechanism with multiple D2D node equipment and one cellular node equipment to combat the smart FDAE.

Other works include: FD strategies in HetNet [88], [89], secrecy rate maximization in Wireless Multi-Hop FD Networks [90], secure communication based on joint design of information and AN beamforming for the FD simultaneous wireless information and power transferring (FD-SWIPT) systems with loopback self-interference cancellation [91].

IV. Conclusions and Future research directions

In this paper, we have presented a comprehensive overview of PLS for 5G wireless networks. The following research topics emerge from the reviewed technologies in this survey:

- Traditionally in most of the PLS works (as illustrated along of paper), the performance of secure communication is only measured using the metrics of secrecy capacity or outage probability, which as seen in section II, these metrics have their drawbacks. In this context, the optimal design of secrecy, reliability, throughput and the trade-off among them is still a challenge research field, and should be the target of future research work.
- Providing PLS usually entails compromising other system requirements. For instance, moderate levels of security sacrifice throughput, while AN schemes compromise power efficiency, where the AN power is transmitted to the eavesdropper. Based on these factors, the characterizing the security performance in novel adversary models wireless scenarios through new metrics that take into account the main demerits of the conventional metrics are essential tracks in future research. Some of these metrics include: average fractional equivocation, average information leakage rate, and generalized secrecy outage probability [33].
- In the security paradigms, a promising direction of research is the integration of PLS and the classic wireless cryptography. In particular, 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.
- In the scenarios with passive eavesdroppers, a realistic assumption is that the transmitter does not know their locations either their CSI. In this context, an interesting future research direction could be to combine techniques such as channel coding and injection of AN (i.e., noise/interfering signals). The challenge would be to find a trade-off between the merits and demerits of the aforementioned techniques while seeking to maximize the secrecy capacity.

References

[1] D. Liu, W. Hong, “What will 5G Be,” *IEEE Trans. Antennas Propag.,* vol. 65, no. 12, pp. 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,* vol. 6, pp. 26350-26357, May 2018.

[3] W. Stallings,“Cryptography and Network Security: Principles and Practice,” *Int. Ann. Criminol.,* vol. 46, no. 4, pp. 121-136, 2008.

[4] N. Yang, L. Wang, M. Elkashlan, J. Yuan, and M. D. Renzo,“Safeguarding 5G Wireless Communication Networks using Physical Layer Security,” *IEEE Commun. Mag.,* pp. 20-27, Apr. 2015.

[5] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Syst. Tech. J.,* vol. 28, no. 4, pp. 656-715, Oct. 1949.

[6] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.* vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory,* vol. 24, no. 3, pp. 339-348, May 1978.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory,* vol. 24, no. 4, pp. 451-456, Jul. 1978.

[9] M. Srinivasan, and S. Kalyani, "Secrecy Capacity of κ-μ Shadowed Fading Channels," *IEEE Commun. Lett.,* vol. 22, no. 8, pp. 1728–1731, Aug. 2018.

[10] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On Physical Layer Security of α-η-κ-μ Fading Channels," *IEEE Commun. Lett.,* vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[11] W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai, "Physical Layer Security Over Fluctuating Two-Ray Fading Channels," *IEEE Trans. Veh. Technol.,* vol. 67, no. 9, pp. 8949–8953, Sep. 2018.

[12] L. Kong, and G. Kaddoum, "On Physical Layer Security Over the Fisher-Snedecor $\mathcal{F}$ Wiretap Fading Channels," *IEEE Access,* vol. 6, pp. 39466–39472, Jul. 2018.

[13] 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 Trans. Inf. Forensics Security,* vol. 13, no. 11, pp. 2788–2700, Nov. 2018.

[14] L. Yang, M. O. Hasna, and I. S. Ansari, "Physical Layer Security for TAS/MRC Systems With and Without Co-Channel Interference Over η–μ Fading Channels," *IEEE Trans. Veh. Technol.,* vol. 67, no. 12, pp. 12421–12426, Dec. 2018.

[15] Y. Ju, H. Wang, T. Zheng, Q. Yin, and M. H. Lee, "Safeguarding Millimeter Wave Communications Against Randomly Located Eavesdroppers," *IEEE Trans. Wireless Commun.,* vol. 17, no. 4, pp. 2675–2689, Apr. 2018.

[16] 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,* vol. X, pp. XX–XX, Feb. 2019.

[17] H. A. Shah, and I. Koo, "A Novel Physical Layer Security Scheme in OFDM-Based Cognitive Radio Networks," *IEEE Access,* vol. 6, pp. 29486–29498, Jun. 2018.

[18] P. Yan, Y. Zou, and J. Zhu, "Energy-Aware Multiuser Scheduling for Physical-Layer Security in Energy-Harvesting Underlay Cognitive Radio Systems," *IEEE Trans. Veh. Technol.,* vol. 67, no. 3, pp. 2084–2096, Mar. 2018.

[19] B. Bhushan and G. Sahoo, "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and their Countermeasures in Wireless Sensor Networks," *Wireless Pers. Commun.,* vol. 98, no. 2, pp. 2037–2077, Jan. 2018.

[20] Z. Liu, N. Li, X. Tao, S. Li, J. Xu, and B. Zhang, "Artificial-Noise-Aided Secure Communication with Full-Duplex Active Eavesdropper," in *Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC),* Bologna, Italy, Sep. 2018.

[21] S. Timilsina, G. A. A. Baduge, and R. F. Schaefer, "Secure Communication in Spectrum-Sharing Massive MIMO Systems with Active Eavesdropping," *IEEE Trans. Cogn. Commun. Netw.,* vol. 4, no. 2, pp. 390–405, Jun. 2018.

[22] L. Li, A. P. Petropulu, and Z. Chen, "MIMO Secret Communications Against an Active Eavesdropper," *IEEE Trans. Inf. Forensics Security,* vol. 12, no. 10, pp. 2387–2401, Oct. 2017.

[23] 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),* Quebec, Canada, May. 2018.

[24] L. Qing, H. Guangyao, and F. Xiaomei, "Physical Layer Security in Multi-Hop AF Relay Network Based on Compressed Sensing," *IEEE Commun. Lett.,* vol. 22, no. 9, pp. 1882–1885, Sep. 2018.

[25] H. Boche and C. Deppe, "Secure Identification Under Passive Eavesdroppers and Active Jamming Attacks," *IEEE Trans. Inf. Forensics & Security,* vol. 14, no. 2, pp. 472–485, Feb. 2019.

[26] K. N. Le, " Performance Analysis of Secure Communications Over Dual Correlated Rician Fading Channels," *IEEE Trans. Commun.,* vol. 66, no. 12, pp. 6659–6673, Dec. 2018.

[27] G. C. Alexandropoulos, and K. P. Peppas, "Secrecy Outage Analysis Over Correlated Composite Nakagami- m /Gamma Fading Channels," *IEEE Commun. Lett.,* vol. 22, no. 1, pp. 77–80, Jan. 2018.

[28] 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 Trans. Commun.,* vol. 67, no. 3, pp. 2405–2419, Mar. 2019.

[29] P. K. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inf. Theory,* vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[30] M. Bloch, J. Barros, M. R. D. Rodrigues, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[31] V. U. Prabhu and M. R. D.Rodrigues, "On Wireless Channels with Antenna Eavesdroppers: Characterization of the Outage Probability and ϵ-Outage Secrecy Capacity," *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 853–860, Sep. 2011.

[32] L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, 1$^{\text{st}}$ ed., Cham, Switzerland: Springer, 2018.

[33] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Commun. Surveys Tuts.,* pp. 1–1, Oct. 2018.

[34] B. He, X. Zhou, and A. L. Swindlehurst, "On Secrecy Metrics for Physical Layer Security Over Quasi-Static Fading Channels," *IEEE Trans. Wireless Commun.,* vol. 15, no. 10, pp. 6913–6924, Oct. 2016.

[35] 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 Trans. Wireless Commun.,* vol. 16, no. 5, pp. 3416–3430, May. 2017.

[36] 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 Trans. Commun.,* vol. 66, no. 2, pp. 546–559, Feb. 2018.

[37] L. Kong, S. Vuppala, and G. Kaddoum, "Secrecy Analysis of Random MIMO Wireless Networks Over α-μ Fading Channels," *IEEE Trans. Veh. Technol.,* vol. 67, no. 12, pp. 11654–11666, Dec. 2018.

[38] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum Secrecy Throughput of MIMOME FSO Communications With Outage Constraints," *IEEE Trans. Wireless Commun.,* vol. 17, no. 5, pp. 3487–3497, May. 2018.

[39] A. Naeem, M. H. Rehmani, Y. Saleem, I. Rashid, and N. Crespi, "Network Coding in Cognitive Radio Networks: A Comprehensive Survey," *IEEE Commun. Surveys Tuts.,* pp. 1–1, Aug. 2018.

[40] 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,* vol. 6, pp. 41490–41503, Jul. 2018.

[41] Y. Choi, and D. Kim, "Optimal Power and Rate Allocation in Superposition Transmission With Successive Noise Signal Sharing Toward Zero Intercept Probability," *IEEE Wireless Commun. Lett.,* vol. 7, no. 5, pp. 824–827, Oct. 2018.

[42] 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),* Porto, Portugal, Jun. 2018, pp. 1-6.

[43] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Commun. Surveys Tuts.,* pp. 1–1, Aug. 2018.

[44] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical Layer Security Over Generalized Gamma Fading Channels," *IEEE Commun. Lett.,* vol. 19, no. 7, pp. 1257–1260, Jul. 2015.

[45] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. Qaraqe, "Performance Analysis of Physical Layer Security Over Generalized-K Fading Channels Using a Mixture Gamma Distribution," *IEEE Commun. Lett.,* vol. 20, no. 2, pp. 408–411, Feb. 2016.

[46] X. Liu, "Probability of Strictly Positive Secrecy Capacity of the Rician—Rician Fading Channel," *IEEE Wireless Commun. Lett.,* vol. 2, no. 1, pp. 50–53, Feb. 2013.

[47] J. Zhu, R. Schober, and V. K. Bhargava, "Secure Transmission in Multi-Cell Massive MIMO Systems," *IEEE Trans. Wireless Commun.,* vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[48] R. F. Schaefer, G. Amarasuriya, and H. V. Poor, "Physical Layer Security in Massive MIMO Systems," in *Proc. 51st Asilomar Conference on Signals, Systems, and Computers,* CA, USA, Oct. 2017, pp. 3–8.

[49] A. Al-Dulaimi, X. Wang, and C. Lin l, *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*, 1$^{\text{st}}$ ed., New Jersey, NJ, USA: John Wiley & Sons Inc, 2018.

[50] Y. Liu, H.-H. Chen, and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Chal-

lenges," *IEEE Commun. Surveys Tut.,* vol. 19, no. 1, pp. 347–376, Mar. 2017.

[51] W. Wu, X. Gao, Y. Wu, and C. Xiao, 'Beam Domain Secure Transmission for Massive MIMO Communications," *IEEE Trans. Veh. Technol.,* vol. 67, no. 8, pp. 7113–7127, Aug. 2018.

[52] X. Zhang, D. Guo, and K. Guo, "Secure Performance Analysis for Multipair AF Relaying Massive MIMO Systems in Ricean Channels," *IEEE Access,* vol. 6, pp. 57708–57720, Oct. 2018.

[53] 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 J. Sel. Areas Commun.,* vol. 36, no. 4, pp. 802–816, Apr. 2018.

[54] 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 Trans. Wireless Commun.,* vol. 16, no. 3, pp. 2001–2016, Mar. 2017.

[55] 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),* Kansas, USA, May. 2018, pp. 1-6.

[56] H. Wei, D. Wang, X. Hou, Y. Zhu, and J. Zhu, "Security Analysis for Massive MIMO System Internal Eavesdroppers," in *Proc. IEEE Veh. Tech. Conf. (VTC'2015),* Boston, USA, Sep. 2015, pp. 1-5.

[57] B. Akgun, M. Krunz, and O. Ozan Koyluoglu, "Vulnerabilities of Massive MIMO Systems to Pilot Contamination Attacks," *IEEE Trans. Inf. Forensics Security,* vol. 14, no. 5, pp. 1251–1263, Oct. 2018.

[58] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot Contamination for Active Eavesdropping," *IEEE Trans. Wireless Commun.,* vol. 11, no. 3, pp. 903–907, Mar. 2012.

[59] 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 Commun. Lett.,* vol. 8, no. 1, pp. 85–88, Feb. 2019.

[60] D. Kudathanthirige, S. Timilsina, and G. A. A. Baduge, "Secure Communication in Relay-Assisted Massive MIMO Downlink With Active Pilot Attacks," *IEEE Trans. Inf. Forensics Security,* pp. 1–1, Feb. 2019.

[61] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, "Robust Beamforming for Physical Layer Security in BDMA Massive MIMO," *IEEE J. Sel. Areas Commun.,*, vol. 34, no. 4, pp. 775–787, Apr. 2018.

[62] 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),* Natal, Brazil, Jun. 2018, pp. 1-6.

[63] 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),* Kansas, USA, May 2018, pp. 1-6.

[64] L. D. H. Sampaio, T. Abrao, and F. R. Durand, "Game Theory Based Resource Allocation in Multi-Cell Massive MIMO OFDMA Networks," in *Comunications and Networking Conference (WCNC),* San Francisco, USA, May 2017, pp. 1-6.

[65] T. Rappaport, R. Heath, R. Daniels, and J. Murdock, *Millimeter Wave Wireless Communications,* Prentice Hall, 2015.

[66] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*, Singopere: Springer, 2016.

[67] 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 Commun.,* vol. 26, no. 1, pp. 72–77, Feb. 2019.

[68] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE J. Sel. Areas Commun.,* vol. 36, no. 4, pp. 679–695, Apr. 2018.

[69] 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,* vol. 1, pp. 335–349, Aug. 2013.

[70] 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,* vol. 7, pp. 28597–28606, Feb. 2019.

[71] Y. Ju, H. Wang, T. Zheng, Q. Yin, and M. H. Lee, "Safeguarding Millimeter Wave Communications Against Randomly Located Eavesdroppers," *IEEE Trans. Wireless Commun.,* vol. 17, no. 4, pp. 2675–2689, Feb. 2018.

[72] 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),* Kansas, USA, May 2018, pp. 1-6.

[73] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, " On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks," *IEEE Trans. Commun.,* vol. 66, no. 3, pp. 1139–1152, Mar. 2018.

[74] K. Xiao, W. Li, M. Kadoch, and C. Li, "On the Secrecy Capacity of 5G MmWave Small Cell Networks," *IEEE Wireless Commun.,* vol. 25, no. 4, pp. 1236–1284, Aug. 2018.

[75] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, and P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice," *IEEE J. Sel. Areas Commun.,* vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[76] 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,* vol. 12, no. 4, pp. 3970–3984, Dec. 2018.

[77] D. Lopez-Perez, I. Guvenc, G. De La Roche, M. Kountouris, T. Q. Quek, and J. Zhang, "Enhanced Intercell Interference Coordination Challenges in Heterogeneous Networks," *IEEE Wireless Commun.,* vol. 18, no. 3, pp. 22–30, Jun. 2011.

[78] 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 Trans. Wireless Commun.,* vol. 17, no. 2, pp. 736–751, Feb. 2018.

[79] 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 Trans. Wireless Commun.,* vol. 17, no. 4, pp. 2645–2661, Apr. 2018.

[80] Y. Zou, M. Sun, J. Zhu, H. Guo, "Security-Reliability Tradeoff for Distributed Antenna Systems in Heterogeneous Cellular Networks," *IEEE Trans. Wireless Commun.,* vol. 17, no. 12, pp. 8444–8456, Dec. 2018.

[81] 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 Trans. Commun.,* vol. 66, no. 12, pp. 6437–6449, Dec. 2018.

[82] S. Wang, Y. Gao, N. Sha, G. Zhang, H. Luo, and Y. Chen, "Physical Layer Security in Two-tier Heterogeneous Cellular Networks over Nakagami-m Channel during Uplink Phase," in *2018 10th International Conference on Communication Software and Networks (ICCSN),* Chengdu, China, Jul. 2018, pp. 1-5.

[83] N. Wu, X. Zhou, and M. Sun, "Secure Transmission With Guaranteed User Satisfaction in Heterogeneous Networks: A Two-Level Stackelberg Game Approach," *IEEE Trans. Commun.,* vol. 66, no. 6, pp. 2738–2750, Jun. 2018.

[84] A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. Wong, "Full-Duplex Small-Cell Networks: A Physical-Layer Security Perspective," *IEEE Trans. Commun.,* vol. 66, no. 7, pp. 3006–3021, Jul. 2018.

[85] 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 Trans. Inf. Forensics Security,* vol. 13, no. 11, pp. 2788–2800, Nov. 2018.

[86] J. Kim, J. Kim, J. Lee, and J. P. Choi, "Physical-Layer Security Against Smart Eavesdroppers: Exploiting Full-Duplex Receivers," *IEEE Access,* vol. 6, pp. 32945–32957, Jun. 2018.

[87] 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,* vol. X, pp. XX–XX, Mar. 2019.

[88] A. Babaei, A. H. Aghvami, A. Shojaeifard, and K. Wong, "Full-Duplex Small-Cell Networks: A Physical-Layer Security Perspective," *IEEE Trans. Commun.,* vol. 66, no. 7, pp. 3006–3021, Jul. 2018.

[89] P. Anokye, R. Ahiadormey, C. Song and K. Lee, "Achievable Sum-Rate Analysis of Massive MIMO Full-Duplex Wireless Backhaul Links in Heterogeneous Cellular Networks," *IEEE Access,* vol. 6, pp. 23456–23469, Apr. 2018.

[90] 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,* vol. 6, pp. 5695–5704, Jan. 2018.

[91] 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),* Kansas, USA, May 2017, pp. 1-6.