EURASIP Journal on Wireless Communications and Networking

REVIEW

Open Access

An overview of generic tools for information-theoretic secrecy performance analysis over wiretap fading channels

Long Kong[1*], Yun Ai[2], Lei Lei[1,3], Georges Kaddoum[4], Symeon Chatzinotas[1] and Björn Ottersten[1]

*Correspondence: long.kong@uni.lu
[1] Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg City 1855, Luxembourg
Full list of author information is available at the end of the article

Abstract

Physical layer security (PLS) has been proposed to afford an extra layer of security on top of the conventional cryptographic techniques. Unlike the conventional complexity-based cryptographic techniques at the upper layers, physical layer security exploits the characteristics of wireless channels, e.g., fading, noise, interference, etc., to enhance wireless security. It is proved that secure transmission can benefit from fading channels. Accordingly, numerous researchers have explored what fading can offer for physical layer security, especially the investigation of physical layer security over wiretap fading channels. Therefore, this paper aims at reviewing the existing and ongoing research works on this topic. More specifically, we present a classification of research works in terms of the four categories of fading models: (i) small-scale, (ii) large-scale, (iii) composite, and (iv) cascaded. To elaborate these fading models with a generic and flexible tool, three promising candidates, including the mixture gamma (MG), mixture of Gaussian (MoG), and Fox's *H*-function distributions, are comprehensively examined and compared. Their advantages and limitations are further demonstrated via security performance metrics, which are designed as vivid indicators to measure how perfect secrecy is ensured. Two clusters of secrecy metrics, namely (i) secrecy outage probability (SOP), and the lower bound of SOP; and (ii) the probability of nonzero secrecy capacity (PNZ), the intercept probability, average secrecy capacity (ASC), and ergodic secrecy capacity, are displayed and, respectively, deployed in passive and active eavesdropping scenarios. Apart from those, revisiting the secrecy enhancement techniques based on Wyner's wiretap model, the on-off transmission scheme, jamming approach, antenna selection, and security region are discussed.

Keywords: Physical layer security (PLS), Channel state information (CSI), Mixture Gamma (MG), Mixture of Gaussian (MoG), Fox's *H*-function, Artificial noise (AN), Artificial fast fading (AFF), Wiretap fading model, Jamming, Antenna selection

1 Introduction

As stated in the latest released statistics by the International Telecommunications Union (ITU) in 2020 [1], COVID-19, to some extent, acts as an accelerator that pushes consumers and businesses to largely adopt digital services and technologies, which in return quickens the digital transformation for societies, business, and governments. Examples, including online learning, digital classrooms, contactless payment, zoom meetings, etc., are reshaping everyone's life pattern. In light of the highly confidential data streams flowing over the wireless transmission medium, the legitimate data transactions enjoy the convenience largely brought by the inherent openness of the wireless transmission medium while facing the vulnerability of being exposed to illegitimate evil parties.

Traditionally, cryptography is an appealing approach to achieve data confidentiality. It is designed to prevent data disclosure to unauthorized devices and malicious users [2]. Although secrecy is guaranteed through the key-based encoding and decoding process and requires additional computing resources, it in fact assumes there exist error-free links at the physical layer. Such an assumption would be unfeasible for the emerging decentralized networks (e.g., resource-limited sensors or radio-frequency identification (RFID) networks) due to the high computational complexity and necessary key distribution and management [3]. Besides, the impacts from the impairments of wireless transmission medium on physical layer security, i.e., the randomness of wireless channels, are totally ignorant in cryptography.

Unlike the conventional complexity-based cryptographic techniques at upper layers via encryption, physical layer security (PLS), being a promising technology complementary to cryptography and certainly not as a replacement, takes full advantage of the physical properties of the wireless propagation environment via the combination of signaling and coding mechanism to provide additional secrecy at the bottom layer [4, 5]. It is proved suitable and feasible for achieving information-theoretic security against eavesdropping attacks. More specifically, under the cover of the randomness of noise, fading, and interference, different users will receive different noisy copies of the private messages. This can enable the confidentiality of legitimate transmissions at the physical layer.

As a promising approach, physical layer security is built on the two pioneering works laid by Shannon [6] and Wyner [7], where the notion of perfect secrecy and the degraded wiretap channel model are introduced, respectively. It is noteworthy to point out that Wyner's result established the PLS from the system model level, and he considered the three-user scenario, consisting of a legitimate source (Alice), an intended legitimate user (Bob), and an eavesdropper (Eve) over the discrete memoryless wiretap channel. In [8], Wyner's wiretap model was extended to the Gaussian wiretap channel by Leung et al., and they found the fundamental basis of secrecy capacity (C_s), which is defined as the difference between the channel capacity of the main channel (Alice to Bob, i.e., C_M) and that of the wiretap channel (Alice to Eve, i.e., C_W), namely, $C_s = C_M - C_W$. The conceptual implication of secrecy capacity indicates that only when the legitimate link experiences better quality of received signals compared to the wiretap channel, positive secrecy can be surely guaranteed. Inspired by this fundamental work, considerable research efforts have been devoted to investigate the security performance metrics over wiretap fading channels, e.g., [9, 10]. The insights drawn from these works offer mathematical proofs showing that wireless channels' fading property can be reversely used to enhance secrecy.

Observing the existing books, surveys, and tutorials related to the PLS [2–5, 11–30], numerous researchers from both the wireless communication and signal processing communities summarized the state-of-the-art of PLS from the perspective of application scenarios, e.g., 5G wireless networks [25], cooperative networks [26], and ultra-reliable and low-latency communications (URLLC) [27], and secrecy enhancement, including jamming schemes [3, 19, 26], multiple-antenna techniques [24], and wiretap coding [14, Chapter 6] [25] (e.g., low-density parity-check (LDPC) codes, polar codes, and lattice codes.) . It is reported in [2] that Zou et al. have classified the PLS technique into four categories: information-theoretic security, artificial-noise aided security, security-oriented beamforming, security diversity methods, and physical layer secret key generation.

As an indispensable element of PLS techniques, information-theoretic security has been further classified into three categories according to different wiretap channels: (i) memoryless wiretap channels; (ii) Gaussian wiretap channels; and (iii) fading wiretap channels. However, the majority of information-theoretic security is centered around the fading wiretap channels, e.g., see references [9, 10, 31]. The pioneering work is laid by Bloch et al. [9], where the authors explored the impacts of fading characteristic of wireless channels on the security issue and proposed two performance metrics, i.e., the average secrecy capacity (ASC) and outage probability of secrecy capacity (equivalently, secrecy outage probability (SOP)), to measure information-theoretic security. At the same year, Gopala et al. [10] investigated the perfect secrecy capacity over wiretap fading channels for two scenarios: (i) the full channel state information (CSI) is available at the transmitter; and (ii) only the main channel CSI is perfectly known at the transmitter. The former scenario represents the active eavesdropping, to be specific, Eve is a legitimate network participant (e.g., in a time-division multiple-access (TDMA) environment). As a result, Alice is capable of accessing Eve's CSI, as well as Bob's CSI. Alice can adapt her coding scheme to every channel coefficient realization. Therefore, the ASC is chosen as the security performance metric. In contrast, the latter scenario indicates the presence of a passive eavesdropper. More specifically, Eve is a totally silent network adversary and only capable of wiretaping the Alice-Bob link. As such, Alice has no CSI knowledge of the wiretap channel, she cannot flexibly adapt her transmission rate to guarantee perfect secrecy. The SOP is correspondingly adopted as the key secrecy metric to evaluate how perfect secrecy is compromised.

Inspired by these fundamental research works, numerous research works focus on analyzing the security performance metrics over a diverse body of fading wiretap channels for the sake of better understanding the impacts of fading characteristic on secure communications, to list some, Rayleigh [9], Nakagami-m, Weibull [32], Rician (Nakagami-q) [33, 34], Hoyt (Nakagami-n) [35, 36], Lognormal [37], $\alpha-\mu$ (equivalently generalized Gamma or Stacy) [38–42], $\kappa-\mu$ [43–46], $\eta-\mu$ [47], generalized-$\mathcal{K}$ ($\mathcal{K}_G$) [48–51], extend generalized-$\mathcal{K}$ (EGK) [52], Fisher-Snedecor $\mathcal{F}$ [53, 54], Gamma-Gamma [55], shadowed $\kappa-\mu$ [56], double shadowed Rician [57], Fox's H-function [52], cascaded Rayleigh/Nakagami-m/$\alpha-\mu$ [58–60], cascaded $\kappa-\mu$ [61], $\alpha-\kappa-\mu/\alpha-\eta-\mu$ [62], Beaulieu-Xie [63], $\alpha-\kappa-\eta-\mu$ [64, 65], two-wave with diffuse power (TWDP) [31], N-wave with diffuse power (NWDP) [66], $\kappa-\mu$/Gamma [67], Fluctuating Beckmann [68], correlated Rayleigh [69], correlated composite Nakagami-m/Gamma [70], correlated $\alpha-\mu$ [71], correlated shadowed $\kappa-\mu$ [72], mixed $\eta-\mu$ and Málaga [73], Málaga [74–78], fluctuating two-ray (FTR) channels [79, 80]. The usage of these fading channels is examined practical and feasible in various wireless communications, such as, cellular networks [81], cellular device-to-device (D2D), vehicle-to-vehicle (V2V) communications [44], radio frequency-free space optical (RF-FSO) systems [55], mmWave communications [79], underwater acoustic communications (UAC), frequency diverse array (FDA) communications [82], body-centric fading channels, unmanned aerial vehicle (UAV) systems, land mobile satellite (LMS) [56, 83], etc.

To the authors' best knowledge, no survey or tutorial paper has ever focused on analyzing the security performance metrics over wiretap fading channels. To this end, the main contributions of this work are listed as follows:

1. reviewing the state-of-the-art of information-theoretic security over four kinds of wiretap fading models: (i) small-scale, (ii) large-scale, (iii) composite, and (iv) cascaded.
2. displaying two clusters of security metrics to quantify information-theoretic security in the presence of active and passive eavesdropping.
3. summarizing three generic tools, i.e., the mixture Gamma (MG) distribution, the mixture of Gaussian (MoG) distribution, and Fox's *H*-function distribution, which are used to assist the derivation of security metrics. These three tools are especially advantageous when the main channel and the wiretap channel confront different type of wiretap fading channels, e.g., the mixture of small-scale fading and composite fading models.
4. presenting the application scenarios, advantages, and limitations of the three aforementioned statistical tools. The insights drawn from the three tools demonstrate their flexibility to largely encompass the existing four kinds of wiretap fading models via adequately configuring fading channel characteristics.
5. providing four secrecy enhancement techniques, including the on-off transmission scheme, jamming approach (artificial noise (AN) and artificial fast fading (AFF)), antenna selection, and security region for Wyner's wiretap channel model.

The remainder of this paper is organized as follows: Sect. 2 presents Wyner's wiretap channel model, followed by Sect. 3, where the security performance metrics are presented. In Sect. 4, we review physical layer security over fading wiretap channels according to the fading channel models and also present three useful and generic tools used to assist the security metrics analysis. In Sect. 5, we introduce the secrecy enhancement schemes based on classic wiretap fading channels. Finally, Sect. 6 concludes this paper.

2 Wyner's wiretap channel model

Consider the classic Alice-Bob-Eve wiretap channel model, as shown in Fig. 1, where Alice intends to send confidential messages to Bob in the presence of a malicious eavesdropper (Eve). The instantaneous signal-to-noise ratio (SNR) at Bob (B) and Eve (E) is expressed as $\gamma_i = \bar{\gamma}_i g_i, i \in \{B, E\}$, where $\bar{\gamma}_i$ is the average received SNR, and g_i is the channel gain, which can be possibly modeled by any fading channel distributions.

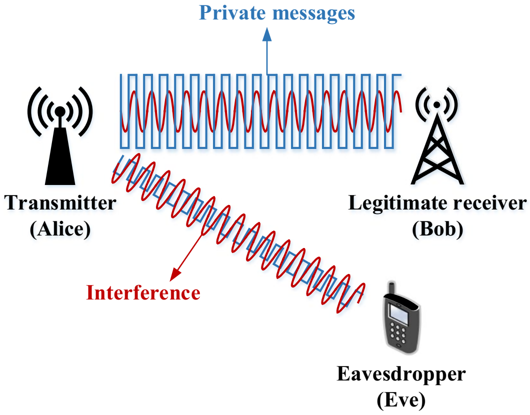


Fig. 1 A three-node wireless wiretap system model

Table 1 PLS statistical performance metrics

Scenarios	Security metrics	CSI availability
Passive eavesdropping	SOP, lower bound of SOP	Partial CSI (only main channel)
Active eavesdropping	ASC, PNZ, intercept probability, ergodic secrecy capacity	Full CSI

3 Security performance metrics

According to [9], the instantaneous secrecy capacity for one realization of the (γ_B, γ_E) pair over quasi-static wiretap fading channels is given by

$$C_s(\gamma_B, \gamma_E) = \left[\underbrace{\log_2 (1+\gamma_B)}_{C_M} - \underbrace{\log_2 (1+\gamma_E)}_{C_W} \right]^+, \qquad (1)$$

where $[x]^+ \overset{\triangle}{=} \max(x, 0)$.

Based on the definition of the instantaneous secrecy capacity, security performance metrics used to evaluate the PLS over wiretap fading channels are further developed according to the availability of full CSI or partial CSI of Wyner's wiretap model. In practice, the aforementioned two scenarios correspond to the passive eavesdropping and active eavesdropping, respectively. More specifically, it is highly questionable to have any knowledge of an evil eavesdropper's CSI. As such, security performance metrics are classified into two categories (i) the SOP and the lower bound of SOP; and (ii) the probability of nonzero secrecy capacity (PNZ) or the intercept probability, ASC, and ergodic secrecy capacity. To this end, the two clusters of security performance metrics are vivid indicators showing whether perfect secrecy can be surely achieved or not, which are shown and compared in Table 1.

3.1 Exact security performance metrics

3.1.1 Secrecy outage probability

In the presence of a passive eavesdropper, who only listens to the main channel without sending any probing messages, Alice transmits her private messages at a constant secrecy rate R_t to Bob. With this in mind, perfect secrecy can be assured only when R_t falls below the instantaneous secrecy capacity C_s. Strikingly, the SOP is commonly seen as a key secrecy indicator used for passive eavesdropping, it measures the level that how perfect secrecy is compromised. Mathematically speaking, the SOP is the probability that the instantaneous secrecy capacity is lower than a predetermined secrecy rate R_t,

$$\begin{aligned} \mathcal{P}_{out}(R_t) &= Pr(C_s < R_t) \\ &= Pr(\gamma_B < 2^{R_t}\gamma_E + 2^{R_t} - 1), \end{aligned} \tag{2}$$

3.1.2 The probability of nonzero secrecy capacity

The PNZ is regarded as another important secrecy metric that measures the existence of positive secrecy capacity with a probability,

$$\begin{aligned} \mathcal{P}_{nz} &= Pr(C_s > 0) \\ &= Pr(\gamma_B > \gamma_E) \\ &\overset{(a)}{=} 1 - \mathcal{P}_{out}(R_t = 0), \end{aligned} \tag{3}$$

where step (a) is subsequently transformed from the SOP metric by setting $R_t = 0$.

3.1.3 Intercept probability

In contrast to the PNZ metric, the intercept probability denotes the probability of the occurrence of an intercept event. In other words, it displays the probability of the occurrence of a negative instantaneous secrecy capacity event, which is mathematically interpreted as

$$\begin{aligned} \mathcal{P}_{int} &= Pr(C_s < 0) \\ &= Pr(\gamma_B < \gamma_E) \\ &= 1 - \mathcal{P}_{nz}. \end{aligned} \tag{4}$$

Compared to the PNZ metric, fewer works have investigated the intercept probability [84–87]. For instance, Zou and Wang in [85] studied the intercept probability of the industrial wireless sensor networks in the presence of an eavesdropping attacker.

3.1.4 Average secrecy capacity

When an active eavesdropper appears, the ASC serves as a critical measurement that guides Alice to adapt her transmission rate based on C_M and C_W so as to achieve perfect secrecy. In other words, the ASC is a metric that evaluates how much achievable secrecy rate can be guaranteed. It is mathematically defined as

$$\bar{C} = \mathcal{E}[C_s(\gamma_B, \gamma_E)], \tag{5}$$

where $\mathcal{E}[\cdot]$ is the expectation operator.

3.2 Security performance bounds

The usage of non-elementary functions is widely used to describe the statistical characteristics of fading models, e.g., the $\kappa - \mu$ distribution with the modified Bessel function of the first kind in its probability density function (PDF) and the generalized Marcum Q function in its cumulative distribution function (CDF), and the EGK distribution with the extended incomplete Gamma function in its PDF. Obviously, the existence of those special functions makes it highly intractable to deduce the security performance metrics embedded with both the PDF and CDF of the instantaneous SNR γ_i simultaneously. As a result, the acquisition of exact security performance metrics with closed-form expressions is a challenging issue, security performance bounds, including the lower bound of the SOP and ergodic secrecy capacity, are in turn adopted as effective alternatives in many works.

3.2.1 The lower bound of SOP

The exact SOP can be accurately approximated by its lower bound when (i) the given transmission rate tends to zero, i.e., $R_t \to 0$; and (ii) Eve is closely located to Alice, which can be physically interpreted as Eve having an extremely high average received SNR, i.e., $\bar{\gamma}_E \to \infty$. In this context, the lower bound of SOP can be computed as

$$\begin{aligned}\mathcal{P}_{out}^{L} &= Pr(\gamma_B < 2^{R_t}\gamma_E)\\ &< Pr(\gamma_B < 2^{R_t}\gamma_E + 2^{R_t} - 1).\end{aligned} \tag{6}$$

Such an alternative has been widely investigated (see references [38, 39, 48, 53, 60]), and was shown to provide a fairly tight approximation.

3.2.2 Ergodic secrecy capacity

As an appropriate secrecy measure to characterize the time-varying feature of wireless channels, the ergodic secrecy capacity is consequently utilized to quantify the ergodic features of wireless channels [42, 88–91]. The ergodic secrecy capacity is mathematically evaluated by averaging the channel capacity over all fading channel realizations, which is mathematically computed as follows,

$$\mathcal{E}(C_s) = \left[\mathcal{E}[\log_2(1+\gamma_B)] - \mathcal{E}[\log_2(1+\gamma_E)]\right]^{+}. \tag{7}$$

For instance, the authors in [92] investigated the ergodic secrecy rate of downlink multiple-input multiple-output (MIMO) systems with limited CSI feedback. Similarly, considering the zero-forcing (ZF) beamforming at Alice and ZF detectors at Bob and Eve, the upper and lower bounds of the ergodic secrecy capacity of MIMO systems were explored in [90].

4 Secrecy characterization

In wireless communication systems, the transmitted signals are reflected, diffracted, and scattered from objects that are present on their path to the receivers. The received signals experience fading (multipath) and shadowing (signal power attenuation or pathloss) phenomena, which pose destructive and harmful impacts at the receiver sides. The essence of PLS lies in reversely using the impairments of wireless channels as secrecy enhancement means.

Under the assumption that the main and wiretap channels undergo independent fading conditions, this section mainly presents the security performance analysis over wiretap fading channels according to the following four categories.

4.1 Exact secrecy analysis

4.1.1 Small-scale fading channels

The random changes in signal amplitude and phase from the spatial positioning between a receiver and a transmitter is referred to small-scale fading. The well-known small-scale fading models are Rayleigh, Nakagami-m, Rician, $\alpha - \mu$, etc. The simple and tractable form of these models makes small-scale fading appealing and popular in the security and reliability performance analysis. Examples can be found in [9, 33, 38–41], where the SOP, PNZ, and ASC metrics are analyzed with either closed-form or highly tight approximated expressions. It is noteworthy of mentioning that the $\alpha - \mu$ distribution can be reduced to Rayleigh ($\alpha = 2, \mu = 1$), Nakagami-m ($\alpha = 2, \mu = m$), Weibull (α is the fading parameter, $\mu = 1$), and Gamma ($\alpha = 1$, μ is the fading parameter) distributions by properly attributing the values of α and μ. To this end, the applicability and flexibility of the $\alpha - \mu$ distribution have been well explored in the literature. Besides, the TWDP fading model is also of high flexibility as it includes Rayleigh, Rician, and hyper-Rayleigh as special cases. The TWDP model characterizes propagating scenarios where the received signal contains two strong, specular multipath waves, moreover, it can also model a link worse than Rayleigh fading. More importantly, it provides a good fit to the the real-world frequency-selective fading data from wireless sensor networks [93]. The PLS investigation over TWDP wiretap fading channels was studied in [31]. Apart from the aforementioned works, in [94], the authors studied the effect of eavesdroppers' location uncertainty on the SOP metric, where Eve is located in a ring-shaped area around Alice and undergoes Rayleigh fading.

Another interesting direction of PLS over small-scale fading channels lies in the secrecy investigation over correlated fading channels. The correlation is caused due to the distances between Bob and Eve, or the scattering environments. The physical correlation essentially makes the fading statistics, i.e., the mathematical representation of the joint PDF of γ_B and γ_E, fairly complex and eventually makes it intractable and highly difficult to obtain exact closed-form security performance metrics, instead, secrecy performance bounds are derived (see references [69, 71]).

4.1.2 Large-scale fading channels

The so-called large-scale fading results from signal attenuation due to signal propagation over large distance and diffraction around large objects, e.g., hills, mountains, forests, billboards, buildings, etc., in the propagation path. One widely studied example of large-scale fading channels is the Lognormal distribution. However, its complex mathematical form hinders the derivation of exact reliability and security performance expressions. For instance, Pan et al. [37] investigated the PLS over non-small scale fading channels, wherein independent/correlated Lognormal fading channels and composite fading channels were considered and approximated security performance representations were derived.

4.1.3 Composite fading channels

Different from the small-scale (fading) and large-scale (shadowing) fading models, composite fading models are proposed to account for the effects of both small-scale and large-scale fading simultaneously. For instance, Kumar et al. in [44] presented the SOP, PNZ, and ASC over $\kappa-\mu$ fading channels and explored the obtained results in several wireless communication scenarios, including cellular D2D, body area networks (BAN), and V2V. Moualeu and Hamouda in [46] subsequently extended the results in [44] to the single-input multiple-output (SIMO) scenario and derived the ASC and lower bound of SOP. More recently, to elaborate the shadowing effect of wireless channels, the authors in [57, 72] investigated the security performance over the shadowed Rician and $\kappa-\mu$ wiretap fading channels.

Other widely used fading models, e.g., generalized-$\mathcal{K}$, Rayleigh/Lognormal (RL), Nakagami-m/Lognormal (NL), Gamma-Gamma, and Fisher-Snedecor $\mathcal{F}$, are examined in practice to model the channel-induced physical layer dynamics. For example, the Fisher-Snedecor $\mathcal{F}$ fading model was proposed in [95] to characterize D2D communications, where its simplicity and feasibility are compared with the generalized-$\mathcal{K}$ fading model. Similarly, the Gamma-Gamma, mixed $\eta-\mu$ and Málaga, and Málaga distributions were shown feasible to accurately model the RF-FSO links, and the security performance analysis of RF-FSO systems over these fading models are explored in [73–76, 96]. To encompass more special models in one distribution, one can find that [62, 64, 65], respectively, analyzed the security performance metrics over $\alpha-\eta-\mu$, $\alpha-\kappa-\mu$, and $\alpha-\eta-\kappa-\mu$ fading models. For instance, the $\alpha-\eta-\kappa-\mu$ model can be reduced to the Rayleigh, Nakagami-m, Rician, $\kappa-\mu$, $\eta-\mu$, $\alpha-\mu$, etc. Those models are highly valuable and flexible. However, its complex mathematical representation of characteristics makes it difficult to derive the exact closed-form security metrics.

4.1.4 Cascaded fading channels

Cascaded fading models were found feasible to characterize the multi-hop non-regenerative amplify-and-forward (AF) relaying with fixed gain, the propagation in the presence of keyholes, the keyhole/pinhole phenomena in MIMO systems, and the reconfigurable intelligent surface (RIS)-aided wireless systems [97–99]. Yang et al. [97] modeled the RIS-aided main link as a multiplication of two Rayleigh distributed random variables. For vehicular networks, Ai et al. [58] considered the double Rayleigh fading channels and analyzed the ASC metric. Regarding other works over cascaded Nakagami-m, cascaded Fisher-Snedecor $\mathcal{F}$, and cascaded $\alpha-\mu$ wiretap fading channels, readers can refer to [58–61, 87, 100]. As discussed earlier, the cascaded

Table 2 Major information-theoretic secrecy analysis works over the classic wiretap fading channels

Year	References	Contributions
2008	Bloch et al. [9]	Derived simple and exact SOP, PNZ, and ASC closed-form expressions over **Rayleigh** fading channels
2013	Liu [32, 33]	Derived the PNZ over **Rician** and **Weibull** fading channels
2014	Wang et al. [31]	Derived the ASC and SOP over **TWDP** fading channels
2015–2018	Lei et al. [38, 40], Kong et al. [39, 41]	Analyzed the SOP, lower bound of SOP, PNZ, and ASC over $\alpha-\mu$ fading channels
2016	Pan et al. [37]	Proposed an highly accurate approximated secrecy solution over **lognormal** fading channels
	Bhargav et al. [44]	Derived the lower bound of SOP and PNZ over $\kappa-\mu$ fading channels
	Lei et al. [48–50]	Analyzed the security metrics over **generalized**-$\mathcal{K}$ fading channels
2017	Saber and Sadough [74]	Derived the SOP, PNZ, and ASC over the **Málaga** fading channels
2018	Kong and Kaddoum [53]	Derived the SOP, lower bound of SOP, PNZ and ASC over **Fisher-Snedecor** $\mathcal{F}$ fading channels
	Kong et al. [60]	Derived closed-form expressions for the SOP, PNZ, and ASC over **cascaded** $\alpha-\mu$ fading channels
	Mathur et al. [65]	Derived the ASC and SOP over $\alpha-\eta-\kappa-\mu$ fading channels
2019	Kong & Kaddoum [36]	Analyzed the security metrics with the assistance of the **MG** distribution
	Kong et al. [52]	Analyzed the security metrics over a general and flexible **Fox's** *H*-**function** fading channels
	Moualeu et al. [62]	Derived closed-form expressions of lower bound of SOP and their asymptotic behavior over the $\alpha-\eta-\mu$ & $\alpha-\kappa-\mu$ fading channels
	Zeng et al. [79], Zhao et al. [80]	Analyzed the security metrics over the **FTR** fading channels
2020	Kong et al. [101]	Proposed a unified secrecy analysis framework with the help of **MoG** distribution
	Sánchez et al. [56]	Derived the closed-form expressions of SOP and ASC metrics over **shadowed** $\kappa-\mu$ fading channels
	Sánchez et al. [66]	Derived the exact and asymptotic SOP behavior over **NWDP** fading channels
	Tashman et al. [61]	Derived the SOP and PNZ over cascaded $\kappa-\mu$ fading channels
	Badarneh et al. [54]	Derived the ASC, PNZ, and SOP over **Nakagami**-*m*/**Fisher Snedecor** $\mathcal{F}$, **Fisher Snedecor** $\mathcal{F}$/**Nakagami**-*m*, and **Nakagami**-*m*/**Nakagami**-*m* fading channels
2021	Ai et al. [78]	Derived the SOP and PNZ over correlated **Málaga** fading channels

The bold items are used to highlight the contributions of the cited works

$\alpha-\mu$ fading channel similarly includes the cascaded Rayleigh, cascaded Nakagami-m, cascaded Weibull, and cascaded Gamma distributions. The authors of [60] studied the SOP, PNZ, and ASC performances with closed-form expressions, which are given in terms of Fox's H-function. The obtained results therein are identical to the exact analytical representations given in [87, 100]. In [61], Tashman et al. considered multiple eavesdroppers and investigated the SOP and PNZ metrics with closed-form expressions over cascaded $\kappa-\mu$ wiretap fading channels.

As shown in Table 2, the existing research works focusing on analyzing security performance metrics over wiretap fading channels are summarized and their contributions are highlighted.

4.2 Generic secrecy analysis tools

With the above in mind and under the assumption that the main and wiretap channels undergo independent fading conditions, this subsection will present three useful and flexible distributions, which can largely encompass the aforementioned fading channel models by properly attributing their parameters. It is proved in literature that they are general and advantageous to assist the theoretical analysis of security metrics.

4.2.1 Mixture Gamma (MG) distribution

According to [102, 103], the instantaneous received SNR γ over wireless Rayleigh, Nakagami-m, NL, $\kappa-\mu$, Hoyt, $\eta-\mu$, Rician, $\mathcal{K}$, $\mathcal{K}_G$, $\kappa-\mu$/Gamma, $\eta-\mu$/Gamma, and $\alpha-\mu$/Gamma fading channels can be reformulated using the MG distribution, whereas the PDF and CDF of the instantaneous received SNR γ are denoted as $f(\gamma)$ and $F(\gamma)$ and given by

$$f(\gamma)=\sum_{l=1}^{L}\alpha_l\gamma^{\beta_l-1}\exp(-\zeta_l\gamma), \tag{8}$$

$$F(\gamma)=\sum_{l=1}^{L}\alpha_l\zeta_l^{-\beta_l}\Upsilon(\beta_l,\zeta_l\gamma), \tag{9}$$

where L is the number of terms in the mixture, while α_l, β_l, and ζ_l are the parameters of the lth Gamma component. $\Upsilon(\cdot,\cdot)$ is the lower incomplete Gamma function.

Lei et al. [49] used the MG distribution to assist the information-theoretic security performance analysis over wiretap generalized-$\mathcal{K}$ fading channels. Motivated by [36], the security metrics over the FTR and Málaga turbulence fading channels [74, 79] can be similarly derived using the MG distribution.

4.2.2 Mixture of Gaussian (MoG) distribution

Based on the unsupervised expectation-maximization (EM) learning algorithm, the MoG distribution is essentially beneficial when the characteristics of fading channels are unavailable. In [104], the authors modeled the RL, NL, $\eta-\mu$, $\kappa-\mu$, and shadowed $\kappa-\mu$ fading channels using the MoG distribution. The findings of [104] showcase that the MoG distribution is, especially advantageous to approximate any arbitrarily shaped non-Gaussian density and can accurately model both composite and non-composite channels in a simple expression.

Assuming the instantaneous SNR γ follows the MoG distribution, its PDF and CDF are given by

$$f(\gamma)=\sum_{l=1}^{C}\frac{w_l}{\sqrt{8\pi\bar{\gamma}}\eta_l\sqrt{\gamma}}\exp\left(-\frac{(\sqrt{\gamma/\bar{\gamma}}-\mu_l)^2}{2\eta_l^2}\right), \tag{10}$$

$$F(\gamma)=\sum_{l=1}^{C}w_l\Phi\left(\frac{\sqrt{\gamma/\bar{\gamma}}-\mu_l}{\eta_l}\right), \tag{11}$$

Table 3 Fox's H-equivalents of typical and generalized statistical models for instantaneous received SNR $\gamma_i, i \in \{B, E\}$, and $\bar{\gamma}_i$ is the average SNR

Model	$\boldsymbol{\mathcal{K}}$	$\boldsymbol{\lambda}$	$\boldsymbol{m\ n}$ $\boldsymbol{p\ q}$	$\mathfrak{a}$ $\mathscr{A}$	$\mathfrak{b}$ $\mathscr{B}$
Rayleigh	$\frac{1}{\bar{\gamma}_i}$	$\frac{1}{\bar{\gamma}_i}$	1 0	–	0
			0 1	–	1
Nakagami	$\frac{m}{\Gamma(m)\bar{\gamma}_i}$	$\frac{m}{\bar{\gamma}_i}$	1 0	–	$m-1$
			0 1	–	1
Weibull	$\frac{\Gamma(1+\frac{2}{\alpha})}{\bar{\gamma}_i}$	$\frac{\Gamma(1+\frac{2}{\alpha})}{\bar{\gamma}_i}$	1 0	–	$1-\frac{2}{\alpha}$
			0 1	–	$\frac{2}{\alpha}$
α-μ	$\frac{\Gamma(\mu+\frac{2}{\alpha})}{\Gamma(\mu)^2\bar{\gamma}_i}$	$\frac{\Gamma(\mu+\frac{2}{\alpha})}{\Gamma(\mu)\bar{\gamma}_i}$	1 0	–	$\mu-\frac{2}{\alpha}$
			0 1	–	$\frac{2}{\alpha}$
Maxswell	$\frac{3}{\sqrt{\pi}\bar{\gamma}_i}$	$\frac{3}{2\bar{\gamma}_i}$	1 0	–	$\frac{1}{2}$
			0 1	–	1
$N*(\alpha$-$\mu)$	$\prod_{i=1}^{N}\frac{\Gamma(\mu_i+\frac{2}{\alpha_i})}{\Gamma(\mu_i)^2\bar{\gamma}_i}$	$\prod_{i=1}^{N}\frac{\Gamma(\mu_i+\frac{2}{\alpha_i})}{\Gamma(\mu_i)\bar{\gamma}_i}$	N 0	–	$(\mu_1-\frac{2}{\alpha_1},\cdots,\mu_N-\frac{2}{\alpha_N})$
			0 N	–	$(\frac{2}{\alpha_1},\cdots,\frac{2}{\alpha_N})$
Fisher-Snedecor $\mathcal{F}$	$\frac{m}{m_s\bar{\gamma}_i\Gamma(m)\Gamma(m_s)}$	$\frac{m}{m_s\bar{\gamma}_i}$	1 1	$-m_s$	1
			1 1	$m-1$	1
Generalized-$\mathcal{K}$	$\frac{m_l m_{sl}}{\Gamma(m_l)\Gamma(m_{sl})\bar{\gamma}_i}$	$\frac{m_1 m_2}{\bar{\gamma}_i}$	2 0	–	$(m_l-1, m_{s1}-1)$
			0 2	–	$(1, 1)$
EGK	$\frac{\Gamma(m+\frac{1}{\xi})\Gamma(m_s+\frac{1}{\xi_s})}{\bar{\gamma}_i\Gamma(m)^2\Gamma(m_s)^2}$	$\frac{\Gamma(m+\frac{1}{\xi})\Gamma(m_s+\frac{1}{\xi_s})}{\bar{\gamma}_i\Gamma(m)\Gamma(m_s)}$	2 0	–	$(m-\frac{1}{\xi}, m_s-\frac{1}{\xi_s})$
			0 2	–	$(\frac{1}{\xi}, \frac{1}{\xi_s})$

where C represents the number of Gaussian components. $w_l > 0$, μ_l, and η_l are the lth mixture component's weight, mean, and variance with $\sum_l^C w_l = 1$, $\Phi(x)$ is the CDF of the standard normal distribution.

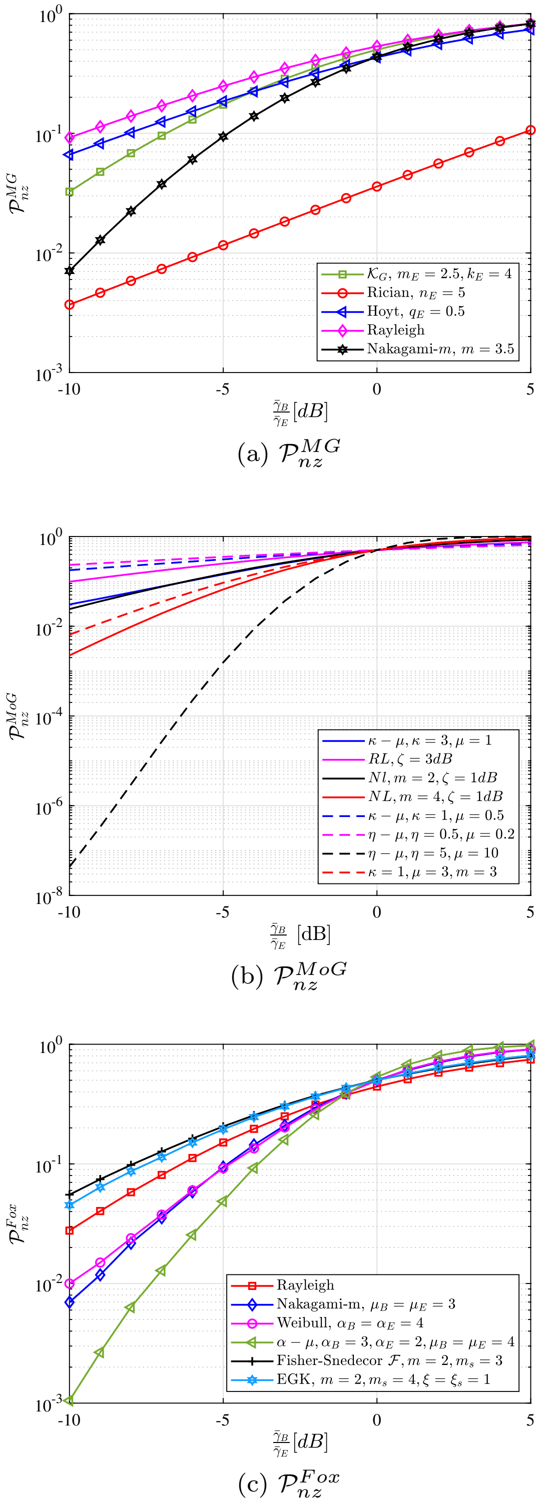
4.2.3 Fox's H-function distribution

For known fading characteristics, the Fox's H-function distribution is a general and flexible tool. It is reported in [52, 105–107] that many well-known distributions in the literature, e.g., Rayleigh, Exponential, Nakagami-m, Weibull, $\alpha-\mu$, Gamma, Fisher-Snedecor $\mathcal{F}$, Chi-square, cascaded Rayleigh/Nakagami-$m/\alpha-\mu$, Gamma-Gamma, Málaga, $\mathcal{K}_G$, EGK, etc., can be represented using Fox's H-function distribution. Interested readers are suggested to refer to Table 3.

Assuming γ follows Fox's H-function distribution, its PDF and CDF are given by

$$f(\gamma) = \mathcal{K} H_{p,q}^{m,n}\left[\mathcal{C}\gamma \middle| \begin{matrix} (a_\tau + A_\tau, A_\tau)_{\tau=1:p} \\ (b_\varsigma + B_\varsigma, B_\varsigma)_{\varsigma=1:q} \end{matrix}\right], \tag{12}$$

$$F(\gamma) = \frac{\mathcal{K}}{\mathcal{C}} H_{p+1,q+1}^{m,n+1}\left[\mathcal{C}\gamma \middle| \begin{matrix} (1,1), (a_\tau + A_\tau, A_\tau)_{\tau=1:p} \\ (b_\varsigma + B_\varsigma, B_\varsigma)_{\varsigma=1:q}, (0,1) \end{matrix}\right], \tag{13}$$



(a) $\mathcal{P}_{nz}^{MG}$

(b) $\mathcal{P}_{nz}^{MoG}$

(c) $\mathcal{P}_{nz}^{Fox}$

Fig. 2 Illustration of $\mathcal{P}_{nz}$ versus $\frac{\bar{\gamma}_B}{\bar{\gamma}_E}$ using the MG, MoG, and Fox's *H*-function distributions when $\bar{\gamma}_E = 0$ dB, **a** the main channel undergoes $\mathcal{K}_G$ ($m_B = 2.5, k_B = 4$) fading while the wiretap channel experiences $\mathcal{K}_G$, Rician, Hoyt, Rayleigh, and Nakagami-*m* ($m = 3.5$) fading; **b** the main and wiretap channels undergo same fading while using the MoG distribution; and **c** the main and wiretap channels undergo same fading while using the Fox's *H*-function distribution

where $H_{p,q}^{m,n}[.]$ is the univariate Fox's H-function [108, Eq. (8.4.3.1)], $\mathcal{K} > 0$ and $\mathcal{C}$ are constants such that $\int_0^\infty f(\gamma)d\gamma = 1$. $A_i > 0$ for $i = 1, \cdots, p$, $B_l > 0$ for $l = 1, \cdots, q$, $0 \leq m \leq q$, and $0 \leq n \leq p$. For notational convenience, let $\mathfrak{a} = (a_1, \cdots, a_p)$, $\mathscr{A} = (A_1, \cdots, A_p)$, $\mathfrak{b} = (b_1, \cdots, b_q)$, and $\mathscr{B} = (B_1, \cdots, B_q)$. Thus, hereafter the Fox's H-function is denoted as $\mathcal{H}_{p,q}^{m,n}(\mathcal{K}, \mathcal{C}, \mathfrak{a}, \mathscr{A}, \mathfrak{b}, \mathscr{B})$.

To compare the security performance analysis using the three aforementioned approaches, the PNZ metric is taken as an example. Provided that the main and wiretap links undergo the same fading conditions, the PNZ expressions are derived in terms of the Gauss Hypergeometric function [36, Eq. (7)], error function [101, Eq. (9)], and Fox's H-function [52, Eq. (16)]. In Fig. 2, we plotted the PNZ performance versus $\bar{\gamma}_B$ for different fading channel models. Their tightness and accuracy have already been individually presented and confirmed in [36, 52, 101].

Remark Conclusively speaking, the MG, MoG, and Fox's H-function distributions have demonstrated their feasibility and applicability when analyzing security performance metrics. They all are valid when the main channel and wiretap channel are subjected to different wireless fading channels. Their advantages and limitations are listed in Table 4.

Note that the three aforesaid solutions are unfeasible when the main and wiretap channels are correlated.

4.3 Outdated and imperfect and correlated CSI

The aforementioned works mainly focus on the scenario that perfect CSI is available at all parties. Such an assumption is unrealistic in practice, since outdated CSI and imperfect CSI are the general cases due to the time varying nature of wireless channels and channel estimation errors.

In [109], the effects of outdated CSI on security performance were investigated over multiple-input single-output (MISO) systems when the transmit antenna selection (TAS) scheme is applied at Alice. The obtained analytical results show that the diversity gain of using multiple antenna techniques cannot be achieved when the CSI is outdated during the TAS process. Later on in [110], Hu et al. adopted the on-off-based transmission scheme at Alice to efficiently take advantage of the useful information in the outdated CSI. Alice does transmission only when she has a better link to Bob compared with that to Eve. Perfect knowledge of the main and wiretap channel CSI are always favorable, but the existence of noise in the channel estimation process makes it

Table 4 Comparisons among the MG, MoG, and Fox's *H*-function distributions

	Applicable scenarios	Advantages	Limitations
MG	Exactly known fading models	Highly accurate solutions with simple expressions	Accuracy depends on *L*
MoG	Unavailability of fading model	Highly accurate approximated solution	Accuracy relies on *C*
Fox	Exactly known and transformable models	Exact and general solution	Inflexibility to some composite fading channels

an unrealistic assumption. The impacts of imperfect CSI have been widely explored in diverse research topics, e.g., imperfect CSI in the AN-assisted training and communications [111], imperfect CSI with an active full-duplex eavesdropper [112], imperfect CSI in a mixed RF/FSO system [55], etc.

Apart from the above two scenarios, the correlation between the main channel and wiretap channel also attracts a growing body of research interests. Channel correlation at the physical layer is often observed, which is mainly caused by the antenna deployments (e.g., insufficient antenna spacing in small mobile units equipped with space and polarization antenna diversity), proximity of the legitimate and illegitimate receivers, and random scatters around them [69]. The correlation is mathematically modeled with the correlated wiretap fading channel models. For example, Jeon et al. in [69] used the correlated Rayleigh fading wiretap channel and explored the secrecy capacity bounds. The results quantitatively showcased how much of secrecy capacity is lost due to channel correlation. In continuation of this work, the security performance analysis over correlated Nakagami-m, correlated $\alpha - \mu$, correlated shadowed $\kappa - \mu$, and correlated Málaga fading channels are explored in [71, 72, 78, 113].

5 Secrecy enhancement approaches

The essence of PLS is to utilize the impairments (e.g., fading, noise, interference, and path diversity) of wireless channels to enhance security. In this section, we mainly focus on comparing the existing secrecy enhancement techniques suitable for wiretap channels.

5.1 On-off transmission scheme

Consider the imperfect channel estimation, He and Zhou in [89] first proposed the on-off transmission scheme to improve the reliability and security performance. The principle of on-off transmission lies in the comparison between the estimated instantaneous SNRs at Bob and Eve, i.e., $\hat{\gamma}_B$ and $\hat{\gamma}_E$, and two given corresponding thresholds i.e., μ_B and μ_E. More specifically, only when the condition $\hat{\gamma}_B \geq \mu_B$ and $\hat{\gamma}_E \leq \mu_E$ meet, the 'on' mode at Alice is then activated, otherwise, Alice is in 'off' mode. The on-off transmission scheme is an appealing enabler to allow the SOP metric to be arbitrarily small. Building on He's work, the on-off transmission is thereafter widely investigated in the following works [110, 114–116], where the imperfect CSI, outdated CSI, and correlated CSI are considered.

5.2 Jamming approach

Assuming the transmitter has more antennas than the eavesdropper, Goel and Negi proposed the concept of artificial noise (AN) [117]. The principle of AN lies in that the transmitter allocates some of its available power to generate AN to confuse passive eavesdroppers. Similarly, Wang et al. in [118] proposed the artificial fast fading (AFF) secrecy enhancement scheme, where the randomized beamforming is employed at the transmitter to 'upgrade' the main channel to an AWGN one and degrade the wiretap channel to a fast fading channel.

Unlike the aforesaid transmitting beamforming-based techniques, i.e., AN and AFF, the quality of the wiretap link is further degraded by allocating part of the transmitting resources (i.e., power or antennas) at the transmitter, specifically to Eve. Based on the survey papers [3, 19], one can conclude that jamming is a useful means to enhance the PLS. Considering the three-node wiretap fading channel, jamming can be alternatively realized by a full-duplex Bob, where Bob would receive signals from Alice and send jamming signals (e.g., noise) to Eve in order to reduce Eve's received SNR's quality [119]. Bob and Eve usually only act purely as a legitimate receiver or an illegitimate evil eavesdropper. However, in practice, they might behave with multiple roles. For instance, in [112], an active eavesdropper operates in full-duplex mode so that it can send jamming signals to degrade the legitimate receiver's SNR, while in [120, 121], an untrustworthy relay works as a relay and eavesdropper simultaneously in a bidirectional cooperative network.

5.3 Antenna selection technique

In multiple-antenna systems, TAS is seen as an effective way for reducing hardware complexity while boosting diversity benefits. In [113, 116, 122–127], TAS is deployed as a secrecy enhancement solution in MIMO systems. There exist three kinds of TAS schemes, i.e., (i) the antenna that maximizes the instantaneous output SNR at Bob is selected (see [122, 123]); (ii) more than one single antenna are selected (see [124]); and (iii) a general order of antenna is selected (see [126]).

Unlike the works [122–125] assuming that the multi-antenna channels are independent, quite recently, Si et al. consider antenna correlation in [116], where the exact and asymptotic SOP are derived with consideration of three diversity combining schemes, namely maximal ratio combining (MRC), selection combining (SC), and equal gain combining (EGC) at Bob. This work is extended in [113], where the authors continuously consider the joint antenna and channel correlation, while the relationship between the correlation and the SOP is analytically established.

5.4 Protected zones

Protected zones (equivalently, secrecy region) mean a geometrical region (see [91, 128]), defined as the legitimate receiver's locations having a certain guaranteed level of secrecy, or an area where the set of ordered nodes can safely communicate with typical destination, for a given secrecy outage constraint [42, 129].

6 Concluding remarks

In this paper, we have comprehensively reviewed the development of PLS over various wiretap fading channels. Based on the characteristics of wireless channels, research works focusing on investigating security performance metrics are thereafter classified into four categories: (i) small-scale fading; (ii) large-scale fading; (iii) cascaded fading; and (iv) composite fading models. After comparing some significant existing and ongoing research works, we introduced three valuable and practical approaches, i.e., the MG, MoG, and Fox's H-function distributions, to simplify the analysis of security performance metrics. The three approaches are highly beneficial and advantageous since they can broadly encompass the existing fading models. Besides, we discussed four secrecy enhancement techniques deployed on Wyner's wiretap channel model, including on-off transmission, jamming approach, TAS technique, and protected zones. Hopefully, this paper can serve as a valuable reference for interested readers on better understanding the physical layer security over wiretap fading channels.

Abbreviations

AN: Artificial noise; AF: Amplify-and-forward; AFF: Artificial fast fading; ASC: Average secrecy capacity; D2D: Device-to-device; EGK: Extended generalized $\mathcal{K}$; MG: Mixture of Gamma; MoG: Mixture of Gaussian; SNR: Signal-to-noise ratio; MIMO: Multiple-input multiple-output; MISO: Multiple-input single-output; CDF: Cumulative distribution function; PDF: Probability density function; TAS: Transmit antenna selection; SC: Selection combining; MRC: Maximal ratio combining; EGC: Equal gain combining; SOP: Secrecy outage probability; PNZ: Probability of nonzero secrecy capacity; AWGN: Additive white Gaussian noise; ITU: International Telecommunications Union; CSI: Channel state information; RF-FSO: Radio frequency-free space optical; OSI: Open systems interconnection; RFID: Radio-frequency identification; IRS: Intelligent reconfigurable surfaces; TDMA: Time-division multiple-access; TWDP: Two-wave with diffuse power; NWDP: *N*-wave with diffuse power; V2V: Vehicle-to-vehicle; FTR: Fluctuating two-ray; UAC: Underwater acoustic communications; UAV: Unmanned aerial vehicle; LMS: Land mobile satellite; PLS: Physical layer security.

Acknowledgements

The authors appreciate the University of Luxembourg for sponsoring the publication of this article.

Authors' contributions

All authors read and approved the final manuscript.

Funding

This work was supported in part by the Luxembourg National Research Fund (FNR) projects, titled Exploiting Interference for Physical Layer Security in 5G Networks (CIPHY) and Resource Optimization for integrated Satellite-5G nETworks with non-orThogonal multiple Access (ROSETTA).

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg City 1855, Luxembourg. [2]Faculty of Engineering, Norwegian University of Science and Technology, Gjøvik 2815, Norway. [3]School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China. [4]LaCIME Laboratory, Department of Electrical Engineering, École de Technologie Supérieure (ÉTS), Université du Québec, Montréal, QC H3C 1K3, Canada.

Received: 12 November 2020 Accepted: 5 November 2021
Published online: 04 December 2021

References

1. ITU, Digital trends in Europe 2021ICT trends and developments in Europe, 2017–2020. Technical report. https://www.itu.int/en/myitu/Publications/2021/02/05/14/28/Digital-trends-in-Europe-2021
2. Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: technical challenges, recent advances, and future trends. Proc. IEEE **104**(9), 1727–1765 (2016)
3. Y. Huo, Y. Tian, L. Ma, X. Cheng, T. Jing, Jamming strategies for physical layer security. IEEE Wirel. Commun. **25**(1), 148–153 (2018)
4. R. Liu, W. Trappe, *Securing Wireless Communications at the Physical Layer*, vol. 7 (Springer, Boston, 2010)
5. X. Zhou, L. Song, Y. Zhang, *Physical Layer Security in Wireless Communications* (CRC Press, Boca Raton, 2013)
6. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
7. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
8. S. Leung-Yan-Cheong, M.E. Hellman, The Gaussian wire-tap channel. IEEE Trans. Inf. Theory **24**(4), 451–456 (1978)
9. M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory **54**(6), 2515–2534 (2008)
10. P.K. Gopala, L. Lai, H. El Gamal, On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory **54**(10), 4687–4698 (2008)
11. R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M.R. Bloch, S. Ulukus, A. Yener, Cooperative security at the physical layer: a summary of recent advances. IEEE Signal Process. Mag. **30**(5), 16–28 (2013)
12. P. Mukherjee, R. Tandon, S. Ulukus, in *Physical-Layer Security with Delayed, Hybrid, and Alternating Channel State Knowledge*. ed. by R.F. Schaefer, H. Boche, A. Khisti, H.V. Poor (Cambridge University Press, Cambridge, 2017), pp. 200–230
13. H.V. Poor, R.F. Schaefer, Wireless physical layer security. Proc. Natl. Acad. Sci. **114**(1), 19–26 (2017)
14. M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge University Press, Cambridge, 2011)

15. B. He, X. Zhou, T.D. Abhayapala, Wireless physical layer security with imperfect channel state information: a survey. ZTE Commun. **11**(3), 11–19 (2013)
16. Y. Shiu, S.Y. Chang, H. Wu, S.C. Huang, H. Chen, Physical layer security in wireless networks: a tutorial. IEEE Wirel. Commun. **18**(2), 66–74 (2011)
17. D.P.M. Osorio, J.D.V. Sánchez, H. Alves, Physical-layer security for 5G and beyond, in *Wiley 5G Ref*, pp. 1–19 (2019)
18. A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014)
19. M. Atallah, G. Kaddoum, L. Kong, A survey on cooperative jamming applied to physical layer security, in *IEEE ICUWB, Montreal, Quebec, Canada*, pp. 1–5 (2015)
20. X. Chen, C. Zhong, C. Yuen, H. Chen, Multi-antenna relay aided wireless physical layer security. IEEE Commun. Mag. **53**(12), 40–46 (2015)
21. Y. Liu, H. Chen, L. Wang, Physical layer security for next generation wireless networks: theories, technologies, and challenges. IEEE Commun. Surv. Tutor. **19**(1), 347–376 (2017)
22. R.F. Schaefer, H. Boche, H.V. Poor, Secure communication under channel uncertainty and adversarial attacks. Proc. IEEE **103**(10), 1796–1813 (2015)
23. A. Hyadi, Z. Rezki, M. Alouini, An overview of physical layer security in wireless communication systems with CSIT uncertainty. IEEE Access **4**, 6121–6132 (2016)
24. X. Chen, D.W.K. Ng, W.H. Gerstacker, H. Chen, A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutor. **19**(2), 1027–1053 (2017)
25. Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J. Sel. Areas Commun. **36**(4), 679–695 (2018)
26. B.V. Nguyen, H. Jung, K. Kim, Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond. IEEE Commun. Mag. **56**(11), 131–137 (2018)
27. R. Chen, C. Li, S. Yan, R. Malaney, J. Yuan, Physical layer security for ultra-reliable and low-latency communications. IEEE Wirel. Commun. **26**(5), 6–11 (2019)
28. B. Dai, C. Li, Y. Liang, H.V. Poor, S. Shamai, Enhancing physical layer security via channel feedback: a survey. EURASIP J. Wirel. Commun. Netw. **58**, 201–225 (2020)
29. B. Li, Z. Fei, C. Zhou, Y. Zhang, Physical-layer security in space information networks: a survey. IEEE Internet Things J. **7**(1), 33–52 (2020)
30. M. Bloch, O. Günlü, A. Yener, F. Oggier, H.V. Poor, L. Sankar, R.F. Schaefer, An overview of information-theoretic security and privacy: metrics, limits and applications. IEEE J. Sel. Areas Inf. Theory **2**(1), 5–22 (2021)
31. L. Wang, N. Yang, M. Elkashlan, P.L. Yeoh, J. Yuan, Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels. IEEE Trans. Inf. Forensics Secur. **9**(2), 247–258 (2014)
32. X. Liu, Probability of strictly positive secrecy capacity of the Weibull fading channel, in *IEEE GLOBECOM, Atlanta, GA, USA*, pp. 659–664 (2013)
33. X. Liu, Probability of strictly positive secrecy capacity of the Rician-Rician fading channel. IEEE Wirel. Commun. Lett. **2**(1), 50–53 (2013)
34. S. Iwata, T. Ohtsuki, P. Kam, Performance analysis of physical layer security over Rician/Nakagami-*m* fading channels, in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia*, pp. 1–6 (2017)
35. F. Jameel, Faisal, M.A.A. Haider, A.A. Butt, Physical layer security under Rayleigh/Weibull and Hoyt/Weibull fading, in *IEEE ICET, Islamabad, Pakistan*, pp. 1–5 (2017)
36. L. Kong, G. Kaddoum, Secrecy characteristics with assistance of mixture Gamma distribution. IEEE Wirel. Commun. Lett. **8**(4), 1086–1089 (2019)
37. G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, Y. Chen, Physical-layer security over non-small-scale fading channels. IEEE Trans. Veh. Technol. **65**(3), 1326–1339 (2016)
38. H. Lei, C. Gao, Y. Guo, G. Pan, On physical layer security over generalized Gamma fading channels. IEEE Commun. Lett. **19**(7), 1257–1260 (2015)
39. L. Kong, H. Tran, G. Kaddoum, Performance analysis of physical layer security over α-μ fading channel. Electron. Lett. **52**(1), 45–47 (2016)
40. H. Lei, I.S. Ansari, G. Pan, B. Alomair, M.S. Alouini, Secrecy capacity analysis over α-μ fading channels. IEEE Commun. Lett. **21**(6), 1445–1448 (2017)
41. L. Kong, G. Kaddoum, Z. Rezki, Highly accurate and asymptotic analysis on the SOP over SIMO α-μ fading channels. IEEE Commun. Lett. **22**(10), 2088–2091 (2018)
42. L. Kong, S. Vuppala, G. Kaddoum, Secrecy analysis of random MIMO wireless networks over α-μ fading channels. IEEE Trans. Veh. Technol. **67**(12), 11654–11666 (2018)
43. S. Kumar, G. Chandrasekaran, S. Kalyani, Analysis of outage probability and capacity for κ-μ/η-μ faded channel. IEEE Commun. Lett. **19**(2), 211–214 (2015)
44. N. Bhargav, S.L. Cotton, D.E. Simmons, Secrecy capacity analysis over κ-μ fading channels: Theory and applications. IEEE Trans. Commun. **64**(7), 3011–3024 (2016)
45. S. Iwata, T. Ohtsuki, P.Y. Kam, Secure outage probability over κ-μ fading channels, in *IEEE ICC, Paris, France*, pp. 1–6 (2017)
46. J.M. Moualeu, W. Hamouda, On the secrecy performance analysis of SIMO systems over κ-μ fading channels. IEEE Commun. Lett. **21**(11), 2544–2547 (2017)
47. L. Yang, M.O. Hasna, 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. **67**(12), 12421–12426 (2018)
48. H. Lei, C. Gao, I.S. Ansari, Y. Guo, G. Pan, K.A. Qaraqe, On physical-layer security over SIMO generalized-K fading channels. IEEE Trans. Veh. Technol. **65**(9), 7780–7785 (2016)
49. H. Lei, H. Zhang, I.S. Ansari, C. Gao, Y. Guo, G. Pan, K.A. Qaraqe, Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution. IEEE Commun. Lett. **20**(2), 408–411 (2016)
50. H. Lei, I.S. Ansari, C. Gao, Y. Guo, G. Pan, K.A. Qaraqe, Physical-layer security over generalised-K fading channels. IET Commun. **10**(16), 2233–2237 (2016)

51. L. Wu, L. Yang, J. Chen, M. Alouini, Physical layer security for cooperative relaying over generalized-K fading channels. IEEE Wirel. Commun. Lett. **7**(4), 606–609 (2018)
52. L. Kong, G. Kaddoum, H. Chergui, On physical layer security over Fox's H-function wiretap fading channels. IEEE Trans. Veh. Technol. **68**(7), 6608–6621 (2019)
53. L. Kong, G. Kaddoum, On physical layer security over the Fisher-Snedecor F wiretap fading channels. IEEE Access **6**(1), 39466–39472 (2018)
54. O.S. Badarneh, P.C. Sofotasios, S. Muhaidat, S.L. Cotton, K.M. Rabie, N. Aldhahir, Achievable physical-layer security over composite fading channels. IEEE Access **8**, 195772–195787 (2020)
55. H. Lei, H. Luo, K.H. Park, Z. Ren, G. Pan, M.S. Alouini, Secrecy outage analysis of mixed RF-FSO systems with channel imperfection. IEEE Photon. J. **10**(3), 1–13 (2018)
56. J.D.V. Sánchez, D.P.M. Osorio, F.J. López-Martínez, M.C.P. Paredes, L. Urquiza-Aguiar, Physical Layer Security of TAS/MRC Over κ-μ Shadowed Fading Channel (2020). arXiv:2005.02441
57. Y. Ai, L. Kong, M. Cheffena, Secrecy outage analysis of double shadowed Rician channels. Electron. Lett. **55**(13), 765–767 (2019)
58. Y. Ai, M. Cheffena, A. Mathur, H. Lei, On physical layer security of double Rayleigh fading channels for vehicular communications. IEEE Wirel. Commun. Lett. **7**(6), 1038–1041 (2018)
59. S.O. Ata, Secrecy performance analysis over double Nakagami-m fading channels, in *IEEE TSP*, pp. 1–4 (2018)
60. L. Kong, G. Kaddoum, D.B. da Costa, Cascaded α-μ fading channels: Reliability and security analysis. IEEE Access **6**, 41978–41992 (2018)
61. D.H. Tashman, W. Hamouda, I. Dayoub, Secrecy analysis over cascaded κ-μ fading channels with multiple eavesdroppers. IEEE Trans. Veh. Technol. **69**(8), 8433–8442 (2020)
62. J.M. Moualeu, D.B. da Costa, W. Hamouda, U.S. Dias, R.A.A. de Souza, Physical layer security over α-κ-μ and α-η-μ fading channels. IEEE Trans. Veh. Technol. **68**(1), 1025–1029 (2019)
63. P.S. Chauhan, S. Kumar, S.K. Soni, On the physical layer security over Beaulieu-Xie fading channel. AEU-Int. J. Electron. C **113**, 152940 (2020)
64. S. Jia, J. Zhang, H. Zhao, Y. Xu, Performance analysis of physical layer security over α-η-κ-μ fading channels. China Commun. **15**(11), 138–148 (2018)
65. A. Mathur, Y. Ai, M.R. Bhatnagar, M. Cheffena, T. Ohtsuki, On physical layer security of α-η-κ-μ fading channels. IEEE Commun. Lett. **22**(10), 2168–2171 (2018)
66. J.D.V. Sánchez, D.P.M. Osorio, F.J. López-Martínez, M.C.P. Paredes, L.F. Urquiza-Aguiar, On the secrecy performance over N-wave with diffuse power fading channel. IEEE Trans. Veh. Technol. **69**(12), 15137–15148 (2020)
67. R. Singh, M. Rawat, Secrecy capacity of physical layer over κ-μ/Gamma composite fading channel, in *IEEE TENCON*, pp. 1472–1477 (2019)
68. H. Al-Hmood, H. Al-Raweshidy, Performance analysis of physical-layer security over fluctuating Beckmann fading channels. IEEE Access **7**, 119541–119556 (2019)
69. H. Jeon, N. Kim, J. Choi, H. Lee, J. Ha, Bounds on secrecy capacity over correlated ergodic fading channels at high SNR. IEEE Trans. Inf. Theory **57**(4), 1975–1983 (2011)
70. G.C. Alexandropoulos, K.P. Peppas, Secrecy outage analysis over correlated composite Nakagami-*m*/Gamma fading channels. IEEE Commun. Lett. **22**(1), 77–80 (2018)
71. A. Mathur, Y. Ai, M. Cheffena, G. Kaddoum, Secrecy performance of correlated α-μ fading channels. IEEE Commun. Lett. **23**(8), 1323–1327 (2019)
72. J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, K.M. Rabie, Secrecy performance analysis of SIMO systems over correlated κ-μ shadowed fading channels. IEEE Access **7**, 86090–86101 (2019)
73. L. Yang, T. Liu, J. Chen, M. Alouini, Physical-layer security for mixed η-μ and M-distribution dual-hop RF/FSO systems. IEEE Trans. Veh. Technol. **67**(12), 12427–12431 (2018)
74. M.J. Saber, S.M.S. Sadough, On secure free-space optical communications over Málaga turbulence channels. IEEE Wirel. Commun. Lett. **6**(2), 274–277 (2017)
75. J. Wang, C. Liu, J. Wang, J. Dai, M. Lin, M. Chen, Secrecy outage probability analysis over Malaga-Malaga fading channels, in *IEEE ICC, Kansas City, MO, USA*, pp. 1–6 (2018)
76. H. Lei, H. Luo, K. Park, I.S. Ansari, W. Lei, G. Pan, M. Alouini, On secure mixed RF-FSO systems with TAS and imperfect CSI. IEEE Trans. Commun. **68**(7), 4461–4475 (2020)
77. Y. Ai, A. Mathur, G.D. Verma, L. Kong, M. Cheffena, Comprehensive physical layer security analysis of FSO communications over Málaga channels. IEEE Photon. J. **12**(6), 1–17 (2020)
78. Y. Ai, A. Mathur, L. Kong, M. Cheffena, Secure outage analysis of fso communications over arbitrarily correlated Málaga turbulence channels. IEEE Trans. Veh. Technol. **70**(4), 3961–3965 (2021)
79. W. Zeng, J. Zhang, S. Chen, K.P. Peppas, B. Ai, Physical layer security over fluctuating two-ray fading channels. IEEE Trans. Veh. Technol. **67**(9), 8949–8953 (2018)
80. H. Zhao, L. Yang, G. Pan, M. Alouini, Secrecy outage analysis over fluctuating two-ray fading channels. Electron. Lett. **55**(15), 866–868 (2019)
81. S. Wang, Y. Gao, N. Sha, G. Zhang, G. Zang, Physical layer security in *K*-tier heterogeneous cellular networks over Nakagami-*m* channel during uplink and downlink phases. IEEE Access **7**, 14581–14592 (2019)
82. S. Ji, W. Wang, H. Chen, S. Zhang, On physical-layer security of FDA communications over Rayleigh fading channels. IEEE Trans. Cogn. Commun. Netw. **5**(3), 476–490 (2019)
83. Y.J. Chun, S.L. Cotton, H.S. Dhillon, F.J. Lopez-Martinez, J.F. Paris, S.K. Yoo, A comprehensive analysis of 5G heterogeneous cellular systems operating over κ-μ shadowed fading channels. IEEE Trans. Wirel. Commun. **16**(11), 6995–7010 (2017)
84. Y. Zou, X. Wang, W. Shen, Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack, in *IEEE ICC, Budapest, Hungary*, pp. 2183–2187 (2013)
85. Y. Zou, G. Wang, Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. IEEE Trans. Ind. Inf. **12**(2), 780–787 (2016)
86. L. Kong, G. Kaddoum, S. Vuppala, On secrecy analysis for D2D networks over α-μ fading channels with randomly distributed eavesdroppers, in *2018 IEEE ICC Workshop 5G-Security, Kansas City, MO, USA* (2018)

87. L. Kong, Y. Ai, J. He, N. Rajatheva, G. Kaddoum, Intercept probability analysis over the cascaded Fisher-Snedecor F fading wiretap channels, in *IEEE ISWCS, Oulu, Finland*, pp. 672–676 (2019)
88. J. Li, A.P. Petropulu, On ergodic secrecy rate for Gaussian MISO wiretap channels. IEEE Trans. Wirel. Commun. **10**(4), 1176–1187 (2011)
89. B. He, X. Zhou, Secure On-Off transmission design with channel estimation errors. IEEE Trans. Inf. Forensics Secur. **8**(12), 1923–1936 (2013)
90. L. Kong, G. Kaddoum, D.B. da Costa, E. Bou-Harb, On secrecy bounds of MIMO wiretap channels with ZF detectors, in *IEEE IWCMC, Limassol, Cyprus*, pp. 724–729 (2018)
91. W. Liu, Z. Ding, T. Ratnarajah, J. Xue, On ergodic secrecy capacity of random wireless networks with protected zones. IEEE Trans. Veh. Technol. **65**(8), 6146–6158 (2016)
92. N. Li, X. Tao, J. Xu, Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback. IEEE Commun. Lett. **18**(6), 969–972 (2014)
93. J. Frolik, A case for considering hyper-Rayleigh fading channels. IEEE Trans. Wirel. Commun. **6**(4), 1235–1239 (2007)
94. D.S. Karas, A.A. Boulogeorgos, G.K. Karagiannidis, Physical layer security with uncertainty on the location of the eavesdropper. IEEE Wirel. Commun. Lett. **5**(5), 540–543 (2016)
95. S.K. Yoo, S.L. Cotton, P.C. Sofotasios, M. Matthaiou, M. Valkama, G.K. Karagiannidis, The Fisher-Snedecor F distribution: a simple and accurate composite fading model. IEEE Commun. Lett. **21**(7), 1661–1664 (2017)
96. H. Lei, Z. Dai, I.S. Ansari, K.H. Park, G. Pan, M.S. Alouini, On secrecy performance of mixed RF-FSO systems. IEEE Photon. J. **9**(4), 1–14 (2017)
97. L. Yang, Y. Jinxia, W. Xie, M. Hasna, T. Tsiftsis, M. Di Renzo, Secrecy performance analysis of RIS-aided wireless communication systems. IEEE Trans. Veh. Technol. **69**(10), 12296–12300 (2020)
98. L. Kong, Y. Ai, S. Chatzinotas, B. Ottersten, Effective rate evaluation of RIS-assisted communications using the sums of cascaded α-μ random variates. IEEE Access **9**, 5832–5844 (2021)
99. Y. Ai, F.A. Pereira, R. de Figueiredo, L. Kong, M. Cheffena, S. Chatzinotas, B. Ottersten, Secure vehicular communications through reconfigurable intelligent surfaces. IEEE Trans. Veh. Technol. (2021). https://doi.org/10.1109/TVT.2021.3088441
100. S.O. Ata, Secrecy performance analysis over cascaded fading channels. IET Commun. **13**(2), 259–264 (2019)
101. L. Kong, S. Chatzinotas, B. Ottersten, Unified framework for secrecy characteristics with mixture of Gaussian (MoG) distribution. IEEE Wirel. Commun. Lett. **9**(10), 1625–1628 (2020)
102. S. Atapattu, C. Tellambura, H. Jiang, A mixture Gamma distribution to model the SNR of wireless channels. IEEE Trans. Wirel. Commun. **10**(12), 4193–4203 (2011)
103. H. Al-Hmood, H.S. Al-Raweshidy, Unified modeling of composite κ-μ/Gamma, η-μ/Gamma, and α-μ/Gamma fading channels using a mixture Gamma distribution with applications to energy detection. IEEE Antennas Wirel. Propag. Lett. **16**, 104–108 (2017)
104. B. Selim, O. Alhussein, S. Muhaidat, G.K. Karagiannidis, J. Liang, Modeling and analysis of wireless channels via the mixture of gaussian distribution. IEEE Trans. Veh. Technol. **65**(10), 8309–8321 (2016)
105. F. Yilmaz, M.S. Alouini, A novel unified expression for the capacity and bit error probability of wireless communication systems over generalized fading channels. IEEE Trans. Commun. **60**(7), 1862–1876 (2012)
106. H.R. Alhennawi, M.M.H.E. Ayadi, M.H. Ismail, H.A.M. Mourad, Closed-form exact and asymptotic expressions for the symbol error rate and capacity of the H-function fading channel. IEEE Trans. Veh. Technol. **65**(4), 1957–1974 (2016)
107. Y. Jeong, J.W. Chong, H. Shin, M.Z. Win, Intervehicle communication: Cox-Fox modeling. IEEE J. Sel. Areas Commun. **31**(9), 418–433 (2013)
108. A.P. Prudnikov, Y.A. Brychkov, O.I. Marichev, *Integrals and Series: More Special Functions*, vol. 3 (Gordon and Breach Science Publishers, New York, 1990)
109. N.S. Ferdinand, D.B. da Costa, M. Latva-aho, Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection. IEEE Commun. Lett. **17**(5), 864–867 (2013)
110. J. Hu, W. Yang, N. Yang, X. Zhou, Y. Cai, On-off-based secure transmission design with outdated channel state information. IEEE Trans. Veh. Technol. **65**(8), 6075–6088 (2016)
111. T. Liu, S. Lin, Y.-P. Hong, On the role of artificial noise in training and data transmission for secret communications. IEEE Trans. Inf. Forensics Secur. **12**(3), 516–531 (2017)
112. L. Kong, J. He, G. Kaddoum, S. Vuppala, L. Wang, Secrecy analysis of a MIMO full-duplex active eavesdropper with channel estimation errors, in *IEEE VTC-Fall, Montreal, Quebec, Canada*, pp. 1–5 (2016)
113. J. Si, Z. Li, J. Cheng, C. Zhong, Asymptotic secrecy outage performance for TAS/MRC over correlated Nakagami-*m* fading channels. IEEE Trans. Commun. **67**(11), 7700–7714 (2019)
114. P. Mu, Z. Li, B. Wang, Secure on-off transmission in slow fading wiretap channel with imperfect CSI. IEEE Trans. Veh. Technol. **66**(10), 9582–9586 (2017)
115. J. Yao, X. Zhou, Y. Liu, S. Feng, Secure transmission in linear multihop relaying networks. IEEE Trans. Wirel. Commun. **17**(2), 822–834 (2018)
116. J. Si, Z. Li, J. Cheng, C. Zhong, Secrecy performance of multi-antenna wiretap channels with diversity combining over correlated Rayleigh fading channels. IEEE Trans. Wirel. Commun. **18**(1), 444–458 (2019)
117. S. Goel, R. Negi, Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**(6), 2180–2189 (2008)
118. H. Wang, T. Zheng, X. Xia, Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading. IEEE Trans. Wirel. Commun. **14**(1), 94–106 (2015)
119. S. Yan, X. Zhou, N. Yang, T.D. Abhayapala, A.L. Swindlehurst, Secret channel training to enhance physical layer security with a full-duplex receiver. IEEE Trans. Inf. Forensics Secur. **13**(11), 2788–2800 (2018)
120. C. Jeong, I. Kim, D.I. Kim, Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system. IEEE Trans. Sig. Process. **60**(1), 310–325 (2012)
121. L. Wang, M. Elkashlan, J. Huang, N.H. Tran, T.Q. Duong, Secure transmission with optimal power allocation in untrusted relay networks. IEEE Wirel. Commun. Lett. **3**(3), 289–292 (2014)
122. N. Yang, P.L. Yeoh, M. Elkashlan, R. Schober, J. Yuan, MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining. IEEE Commun. Lett. **17**(9), 1754–1757 (2013)

123. L. Wang, M. Elkashlan, J. Huang, R. Schober, R.K. Mallik, Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels. IEEE Trans. Wirel. Commun. **13**(11), 6054–6067 (2014)
124. N. Yang, P.L. Yeoh, M. Elkashlan, R. Schober, I.B. Collings, Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans. Commun. **61**(1), 144–154 (2013)
125. J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, G.K. Karagiannidis, On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping. IEEE Trans. Veh. Technol. **65**(1), 214–225 (2016)
126. Y. Huang, F.S. Al-Qahtani, T.Q. Duong, J. Wang, Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. IEEE Trans. Commun. **63**(8), 2959–2971 (2015)
127. J.M. Moualeu, D.B. da Costa, F.J. Lopez-Martinez, W. Hamouda, T.M.N. Nkouatchah, U.S. Dias, Transmit antenna selection in secure MIMO systems over α-μ fading channels. IEEE Trans. Commun. **67**(9), 6483–6498 (2019)
128. T.X. Zheng, H.M. Wang, Q. Yin, On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers. IEEE Commun. Lett. **18**(8), 1299–1302 (2014)
129. S. Vuppala, S. Biswas, T. Ratnarajah, Secrecy outage analysis of *k*th best link in random wireless networks. IEEE Trans. Commun. **65**(10), 4478–4491 (2017)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.