Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2020.DOI

An Overview of Information-Theoretic Secrecy Analysis over Classical Wiretap Fading Channels

LONG KONG[1], YUN AI[2], (Member, IEEE), LEI LEI[1], (Member, IEEE), GEORGES KADDOUM[3], (Member, IEEE), SYMEON CHATZINOTAS[1], (SENIOR MEMBER, IEEE), and BJÖRN OTTERSTEN[1], (FELLOW, IEEE)

[1]The Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg City 1855, Luxembourg (e-mail: {long.kong, lei.lei, symeon.chatzinotas, björn.ottersten}@uni.lu.)

[2]Faculty of Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway (e-mail: yun.ai@ntnu.no)

[3]LaCIME Laboratory, Department of Electrical Engineering, École de Technologie Supérieure (ÉTS), Université du Québec, Montréal (Québec), Canada, H3C 1K3, e-mail: (georges.kaddoum@etsmtl.ca.)

Corresponding author: Long Kong (e-mail: long.kong@uni.lu).

This work was supported by Luxembourg National Research Fund (FNR) projects, titled Exploiting Interference for Physical Layer Security in 5G Networks (CIPHY), and Energy and CompLexity EffiCienT mIllimeter-wave Large-Array Communications (ECLECTIC).

ABSTRACT An alternative or supplementary approach named as physical layer security has been recently proposed to afford an extra security layer on top of the conventional cryptography technique. In this paper, an overview of secrecy performance investigations over the classic Alice-Bob-Eve wiretap fading channels is conducted. On the basis of the classic wiretap channel model, we have comprehensively listed and thereafter compared the existing works on physical layer secrecy analysis considering the small-scale, large-scale, composite, and cascaded fading channel models. Exact secrecy metrics expressions, including secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and average secrecy capacity (ASC), and secrecy bounds, including the lower bound of SOP and ergodic secrecy capacity, are presented. In order to encompass the aforementioned four kinds of fading channel models with a more *generic* and *flexible* distribution, the mixture gamma (MG), mixture of Gaussian (MoG), and Fox's H-function distributions are three useful candidates to largely include the above-mentioned four kinds of fading channel models. It is shown that all they are flexible and general when assisting the secrecy analysis to obtain closed-form expressions. Their advantages and limitations are also highlighted. Conclusively, these three approaches are proven to provide a unified secrecy analysis framework and can cover all types of independent wiretap fading channel models. Apart from those, revisiting the existing secrecy enhancement techniques based on our system configuration, the on-off transmission scheme, artificial noise (AN) & artificial fast fading (AFF), jamming approach, antenna selection, and security region are presented.

INDEX TERMS 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), Wyner's wiretap fading model, jamming, antenna selection.

I. INTRODUCTION

The exposure of confidential messages into the wireless transmission medium makes the legitimate transmission vulnerable due to (i) the openness of wireless transmission medium; and (ii) the standardization of wireless transmission schemes, e.g., coding and modulation schemes. The conventionally widely used approach called the cryptography technique is placed at the upper layer under the significant assumptions of (i) error-free links at physical layer; and (ii) eavesdroppers' incapability of the accomplishment of secret-key decryption with limited computational power. It is predicted that the quantum computing will be functional enough to be able to break easily the current strong public-key cryptosystems in the future [1]. Besides, issues like computational complexity and key distribution and management in some emerging decentralized networks (e.g., sensor or radio-frequency identification (RFID) networks) makes it difficult to deploy public-key infrastructure [2]. Against this background, many research results suggest that there is much security to be achieved by making full use of the impairments (i.e., noise and fading) of wireless communication links [3]. In other words, private messages can be transmitted securely to the legitimate receivers at the physical layer under the cover of noise and interference against an unauthorized devices or a potential malicious eavesdropper. Consequently, research efforts were shifted to seek a cost-efficient and effective solution to address the secrecy concern from the physical layer of the layer-structure protocol.

An appealing countermeasure, known as physical layer security (PLS), was found suitable for preventing eavesdropping attacks on the secure and reliable wireless communication from the information-theoretic perspective. Two pioneering works were respectively laid by Shannon [4] and Wyner [5], where the notion of perfect secrecy and wiretap channel model were respectively introduced. It is noteworthy to point out that Wyner's result established the PLS from the system model level, where he considered the three-user scenario, consisting of a source (Alice), an intended legitimate user (Bob), and an eavesdropper (Eve) over the discrete memoryless wiretap channel. In [6], Wyner's wiretap model was extended to the Gaussian wiretap channel, Leung *et al.* also defined the secrecy capacity as the difference between the channel capacity of the main channel (Alice to Bob) and that of the wiretap channel (Alice to Eve). The conceptual beauty of secrecy capacity indicates that only when the legitimate link experiences better quality of received signals compared to the wiretap channel, positive secrecy can thereafter be surely guaranteed. In the recent few decades, a growing body of secrecy metrics investigations over wiretap fading channels were conducted, e.g., [7], [8]. The insights drawn from these works offer mathematical proofs that the fading property of wireless channels can be reversely used to enhance secrecy. To this end, various researchers from both the wireless communication and signal processing communities were inspired to explore the effective secrecy enhancements solutions.

Observing the existing surveys and tutorial works regarding the PLS [2], [9]–[14], techniques like information-theoretic security, artificial-noise aided security, security-oriented beamforming, security diversity methods, and physical layer secret key generation are listed in [11] by Zou *et al*. As an organic part of PLS techniques, information-theoretic security have been classified into three categories: (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, see references [7], [8], [15]. To be specific, Bloch *et al.* in [7] examined the impact of the fading property of wireless channels on the secrecy issue and thereafter proposed the feasibility of the average secure communication rate and the outage probability as secrecy metrics. Later on, Gopala *et al.* in [8] established the perfect secrecy capacity over the fading wiretap channel model when (i) the full channel state information (CSI) are available at the transmitter; and (ii) only the main channel CSI is perfectly known at the transmitter. In addition, the on/off power allocation strategy was proposed as a transmission policy, i.e., Alice can perform information transmission as long as the channel gain of the legitimate user is larger than a predetermined positive threshold.

Since then, numerous works have analyzed the secrecy performance over a diverse body of fading channels, just to name some, Rayleigh [7], Nakagami-m, Weibull [16], Rician (Nakagami-q) [17], Hoyt (Nakagami-n) [18], [19], Lognormal [20], $\alpha-\mu$ (equivalently generalized gamma) [21]–[25], $\kappa-\mu$ [26]–[29], $\eta-\mu$ [30], generalized-$\mathcal{K}$ [31]–[34], extend generalized-$\mathcal{K}$ (EGK) [35], Fisher-Snedecor $\mathcal{F}$ [36], gamma-gamma [37], shadowed $\kappa-\mu$ [38], double shadowed Rician [39], Fox's H-function [35], cascaded Rayleigh/Nakagami-$m/\alpha-\mu$ [40]–[42], $\alpha-\kappa-\mu/\alpha-\eta-\mu$ [43], $\alpha-\kappa-\eta-\mu$ [44], [45], two-wave with diffuse power (TWDP) [15], N-wave with diffuse power [46], $\kappa-\mu$/Gamma [47], Fluctuating Beckmann [48], correlated Rayleigh [49], correlated $\alpha-\mu$ [50], correlated shadowed $\kappa-\mu$ [51], mixed $\eta-\mu$ and Málaga [52], Málaga [53], [54], fluctuating two-ray (FTR) channels [55], [56]. The usage of these fading channels are examined practical and feasible in various wireless communications, such as, cellular device-to-device (D2D), vehicle-to-vehicle (V2V) communications [27], mmWave communications [55], underwater acoustic communications (UAC), body-centric fading channels, unmanned aerial vehicle (UAV) systems, land mobile satellite (LMS), etc [38], [57].

To the authors' best knowledge, no survey papers so far have focused on the secrecy metrics analysis over various fading channels. To this end, the main contributions of this work are listed as follows:

1) presenting the state-of-the-art of information-theoretic secrecy analysis works over four kinds of wiretap fading models, (i) small-scale, (ii) large-scale, (iii) composite, and (iv) cascaded.
2) summarizing and comparing three useful secrecy analysis approaches, i.e., mixture gamma (MG), mixture of Gaussian (MoG), and Fox's H-function based solutions. The insights drawn herein show that these three tools can encompass most existing secrecy analysis works by properly configuring the channel characteristics.
3) providing a list set of secrecy enhancement solutions, including the on-off transmission scheme, artificial noise (AN) & artificial fast fading (AFF), jamming approach, antenna selection, and security region for the classical wiretap channel model.

The remainder of this paper is organized as follows: Section II presents the classic wiretap model and the problem formulation. In III, we divide the secrecy metrics analysis works into four categories according to the fading channel model and consequently present three useful and proven tools used to assist the secrecy metrics analysis. In Section IV, we introduce the secrecy enhancement schemes based

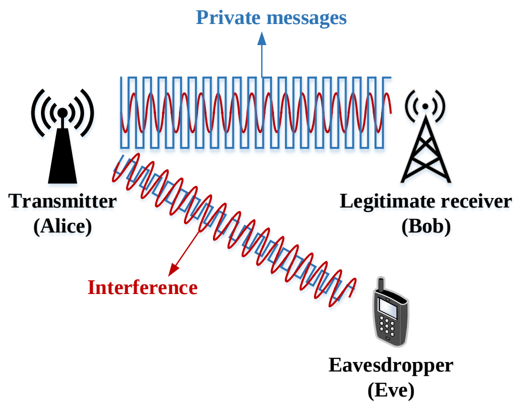


FIGURE 1: A three-node wireless system wiretap model.

on the classical wiretap fading channels. Finally, Section V concludes this paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. SYSTEM MODEL

Consider the classic Alice-Bob-Eve wiretap channel model, as shown in Fig. 1, where a transmitter (Alice) intends to send confidential messages to the legitimate receiver (Bob) in the presence of a malicious eavesdropper (Eve). The link between Alice and Bob is called the main channel, while the one between Alice and Eve is the wiretap channel. The instantaneous signal-to-noise ratio (SNR) at Bob (B) and Eve (E) are 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 modeled by any of the previously mentioned fading distributions.

B. SECRECY METRICS

Assuming the availability of perfect CSI at all terminals. According to [7], the instantaneous secrecy capacity for one realization of (γ_B, γ_E) pair over quasi-static wiretap fading channels is given by

$$C_s(\gamma_B, \gamma_E) = \left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]^+, \quad (1)$$

where $[x]^+ \triangleq \max(x, 0)$.

Based on the definition of instantaneous secrecy capacity, secrecy metrics including secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), average secrecy capacity (ASC), and ergodic secrecy capacity are henceforth developed for the sake of evaluating the security of all kinds of wireless systems.

1) Secrecy outage probability (SOP)

The SOP is commonly seen as a crucial secrecy indicator, and widely used when analyzing PLS over fading channels. The SOP is the probability that the instantaneous secrecy capacity is lower than a predetermined secrecy rate R_t,

$$\mathcal{P}_{out} = Pr\left(C_s \leq R_t\right). \quad (2)$$

2) The probability of non-zero secrecy capacity (PNZ)

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

$$\mathcal{P}_{nz} = Pr\left(C_s > 0\right) = Pr(\gamma_B > \gamma_E). \quad (3)$$

3) Average secrecy capacity (ASC)

The ASC is a secrecy metric that evaluates how much achievable secrecy rate can be guaranteed for the whole system. It is mathematically defined as

$$\bar{C} = \mathcal{E}[C_s(\gamma_B, \gamma_E)], \quad (4)$$

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

4) Ergodic secrecy capacity

As an appropriate secrecy measure to characterize the time-varying feature of wireless channels, the ergodic secrecy capacity is resultantly utilized to quantify the ergodic features of wireless channels [25], [58]–[61]. The ergodic secrecy capacity is mathematically evaluated by averaging the channel capacity over all fading channel realizations, and is computed as

$$\mathcal{E}(C_s) = \left[\mathcal{E}[\log_2(1+\gamma_B)] - \mathcal{E}[\log_2(1+\gamma_E)\right]^+. \quad (5)$$

III. SECRECY CHARACTERIZATION

A. EXACT SECRECY ANALYSIS

In wireless communication systems, the transmitted signals are reflected, diffracted, and scattered from objects that are present on their path to the receiver. 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 is to reversely use 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 secrecy analysis over wiretap fading channels according to the existing fading channel categories.

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 as small-scale fading. The well-known small-scale fading models are Rayleigh, Nakagami-m, Rician, $\alpha - \mu$ (equivalently, generalized gamma or Stacy), 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 [7], [17], [21]–[24], where SOP, PNZ, and ASC are analyzed by devising 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 performance analysis. Another fading model, namely the TWDP fading, also is of high flexibility as it includes Rayleigh, Rician, and hyper-Rayleigh fading as special cases. It characterizes the propagating scenario where the received signal contains two strong, specular multipath waves. The PLS investigation over TWDP wiretap fading channels was studied in [15]. Apart from the aforementioned works, in [62], the authors studied the effect of eavesdroppers' location uncertainty on the SOP metric, where Eve is supposed to be 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 complex mathematical representation of the joint PDF of γ_B and γ_E makes it intractable and highly difficult to obtain exact closed-form secrecy performances, instead of deriving the secrecy bounds (see references [49], [50]).

2) Large-scale fading channels

The so-called large-scale fading results from signal attenuation due to signal propagation over large distances and diffraction around large objects (i.e., hills, mountains, forests, billboards, buildings, etc.) in the propagation path. One widely studied example of large-scale fading channels is the lornormal distribution, however its complex mathematical form hinders the derivation of exact reliability and secrecy performance expressions. For instance, Pan *et al.* in [20] investigated the PLS over non-small scale fading channels, wherein independent/correlated lognormal fading channels and composite fading channels were considered and highly accurate approximated secrecy representations were derived.

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 [27] presented the SOP, PNZ, and ASC over $\kappa-\mu$ fading channels and explored the obtained results in a diverse range of wireless communication scenarios, including cellular D2D, BAN, and V2V. Moualeu and Hamouda in [29] subsequently extended the results in [27] 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, in [39], [51], the authors investigated the secrecy performance over the shadowed Rician and $\kappa - \mu$ wiretap fading channels.

Other widely used models, e.g., Rayleigh/Lognormal (RL), Nakagami-m/Lognormal (NL), generalized-$\mathcal{K}$, gamma-gamma, and Fisher-Snedecor $\mathcal{F}$, are examined in the realistic wireless communication scenarios to model the channel-induced physical layer dynamics. To be specific, the Fisher-Snedecor $\mathcal{F}$ fading was proposed to characterize device-to-device (D2D) communications, where its simplicity and feasibility are compared with the generalized-$\mathcal{K}$ fading model in [63]. Similarly, the gamma-gamma, mixed η–μ and Málaga, Málaga distributions were shown feasible to accurately model the radio frequency-free space optical (RF-FSO) links, and the secrecy performance over those fading models are respectively provided in [52]–[54], [64]. To encompass more special fading models in one distribution, secrecy analysis over $\alpha - \eta - \mu$, $\alpha - \kappa - \mu$, and $\alpha - \eta - \kappa - \mu$ are taken into consideration in [43]–[45]. Though general and flexible, it is difficult to derive the exact secrecy expressions.

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, and the keyhole/pinhole phenomena in MIMO systems, as well as the quite recent proposed intelligent reflective surface (IRS) scenario. For vehicular networks, the secrecy performance has been investigated considering the double Rayleigh fading channels. For other works over cascaded Nakagami-m/Fisher-Snedecor $\mathcal{F}/\alpha-\mu$ wiretap fading channels, the readers are referred to [40]–[42], [65], [66]. As discussed earlier, the cascaded $\alpha-\mu$ fading channel similarly includes the cascaded Rayleigh, cascaded Nakagami-m, cascaded Weibull, and cascaded gamma distributions. We have in [42] studied the SOP, PNZ, and ASC performances with closed-form expressions, which are given in terms of Fox's H-function. Obviously, the results therein are identical to the analytical representations given in [65], [66].

The majority of information-theoretic security analysis works over wiretap fading channels are summarized and their contributions are highlighted in Table 1.

B. SECRECY BOUNDS

Due to the difficulty in deriving exact closed-form SOP and ASC expressions, the lower bound of the SOP and ergodic secrecy capacity are often regarded as effective alternatives.

1) 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 close 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

$$\mathcal{P}_{out}^{L} = \int_0^{\infty} F_B\left(2^{R_t}\gamma\right) f_E(\gamma) d\gamma. \tag{6}$$

Such an alternative has been widely investigated in many works (see references [21], [22], [31], [36], [42]), and was shown to provide a fairly excellent approximation.

2) Ergodic secrecy capacity

To overcome the incapability of obtaining a closed-form ASC expression, the ergodic secrecy capacity is a widely

TABLE 1: Major information-theoretic secrecy analysis works over the classical wiretap fading channels

Year	References	Contributions
2008	Bloch et al. [7]	derived simple and exact SOP, PNZ, and ASC closed-form expressions over **Rayleigh** fading channels
2013	Liu [16], [17]	derived the PNZ over **Rician** and **Weibull** fading channels
2014	Wang et al. [15]	derived the ASC and SOP over **TWDP** fading channels
2015-2018	Lei et al. [21], [23], Kong et al. [22], [24]	analyzed the SOP, lower bound of SOP, PNZ, and ASC over $\alpha-\mu$ wiretap fading channels.
2016	Pan et al. [20]	proposed an highly accurate approximated secrecy solution over the **lognormal** fading channels.
	Bhargav et al. [27]	derived the lower bound of SOP and PNZ over $\kappa-\mu$ fading channels.
	Lei et al. [31]–[33]	analyzed the secrecy metrics over **generalized-$\mathcal{K}$** fading channels.
2017	Saber and Sadough [53]	derived the SOP, PNZ, and ASC over the **Málaga** wiretap fading channels.
2018	Kong & Kaddoum [36]	derived the SOP, lower bound of SOP, PNZ and ASC over **Fisher-Snedecor $\mathcal{F}$** wiretap fading channels.
	Kong et al. [42]	derived closed-form expressions for the SOP, PNZ, and ASC over **cascaded** $\alpha-\mu$ wiretap fading channels.
	Mathur et al. [45]	derived the ASC and SOP over $\alpha-\eta-\kappa-\mu$ wiretap fading channels.
2019	Kong & Kaddoum [19]	analyzed the secrecy metrics with the assistance of the **MG** distribution.
	Kong et al. [35]	analyzed the secrecy metrics over a general and flexible **Fox's H-function** wiretap fading channels.
	Moualeu et al. [43]	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. [55], Zhao et al. [56]	analyzed the secrecy metrics over the **FTR** wiretap fading channels.
2020	Kong et al. [67]	proposed a unified secrecy analysis framework with the help of **MoG** distribution.
	Sánchez et al. [38]	derived the closed-form expressions of SOP and ASC metrics over **shadowed** $\kappa-\mu$ fading channels.
	Sánchez et al. [46]	derived the exact and asymptotic SOP behavior over **N-wave with diffuse power** fading channels.

adopted alternative in open literature to measure the average ability of secrecy transmission over fading channels [14]. For instance, in [68], the authors investigated the ergodic secrecy rate of the downlink multiple-input multiple-output (MIMO) systems with limited CSI feedback. Moreover in [60], we have investigated the upper and lower bounds of the ergodic secrecy capacity of MIMO system where zero-forcing (ZF) beamforming at Alice and ZF detectors at Bob and Eve are exploited.

C. SECRECY ANALYSIS TOOLS

With the above in mind and under the assumption that the main channel and wiretap channel undergo independent fading conditions, this subsection will present three useful tools used to assist the secrecy analysis.

1) Mixture Gamma (MG) distribution

According to [69], [70], 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 with probability density function (PDF):

$$f(\gamma)=\sum_{l=1}^{L}\alpha_l\gamma^{\beta_l-1}\exp(-\zeta_l\gamma), \tag{7}$$

here 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.

The work in [32] used the MG distribution to assist the information-theoretic secrecy analysis. Motivated by [19], the secrecy metrics over the FTR and Málaga turbulence fading channels [53], [55] also can be similarly derived using the MG distribution.

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 the fading channel are unavailable. In [71], the authors modeled the RL, NL, $\eta-\mu$, $\kappa-\mu$, and shadowed $\kappa-\mu$ fading channels using the MoG distribution. The findings of [71] showcases 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 γ follows the MoG distribution with PDF:

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

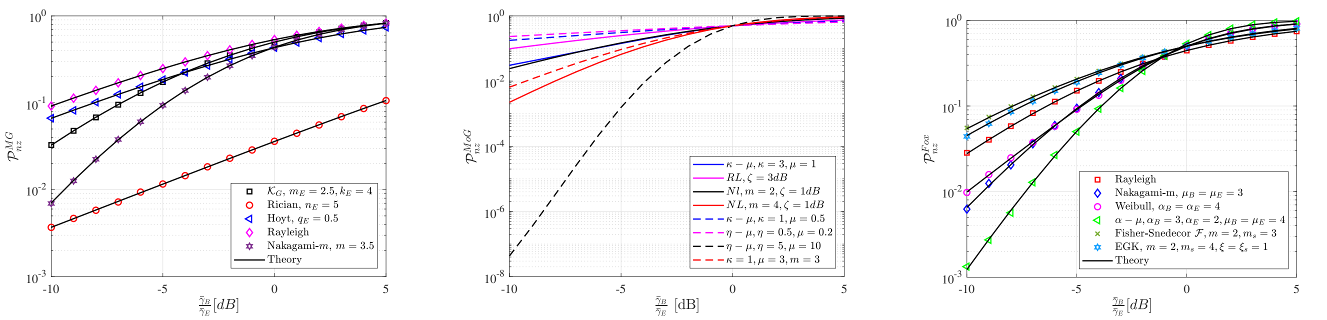
where C represents the number of Gaussian components. $w_l>0$, μ_l, and η_l are the lth mixture component's weight, mean, and variance with $\sum_l^C w_l=1$.

3) Fox's H-function distribution

For the known fading characteristics, the Fox's H-function distribution is a general and flexible tool to model the instantaneous received SNR. It is reported in [35], [72]–[74] 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. Examples are suggested to refer to Table. 2.

TABLE 2: Fox's H-equivalents of typical and generalized statistical models

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



(a) $\mathcal{P}_{nz}^{MG}$ (b) $\mathcal{P}_{nz}^{MoG}$ (c) $\mathcal{P}_{nz}^{Fox}$

FIGURE 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 $\bar{\gamma}_E$ = 0dB, (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.

Assuming γ follows Fox's H-function distribution, its PDF is given by

$$f(\gamma)=\mathcal{K}H_{p,q}^{m,n}\left[\mathcal{C}\gamma\left|\begin{array}{l}(a_1,A_1),\cdots,(a_p,A_p)\\(b_1,B_1),\cdots,(b_q,B_q)\end{array}\right.\right], \quad (9)$$

where $H_{p,q}^{m,n}[.]$ is the univariate Fox's H-function [75, 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 $\mathcal{H}_{p,q}^{m,n}(\mathcal{K},\mathcal{C},\mathfrak{a},\mathscr{A},\mathfrak{b},\mathscr{B})$.

For the purposes of comparing the secrecy analysis by 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 given in terms of the Gauss Hypergeometric function [19, Eq. (7)], error function [67, Eq. (9)], and Fox's H-function [35, 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 [19], [35], [67].

Remark: Conclusively speaking, the MG, MoG, and Fox's H-function distributions have demonstrated their feasibility and applicability when analyzing secrecy metrics. They all are valid when the main channel and wiretap channel are subjected to different wireless channels as shown in Fig. 2. (a). Their advantages and limitations are listed in Table. 3. ***Note that the three aforesaid solutions are unfeasible to the correlated wiretap fading scenario***.

D. OUTDATED & IMPERFECT & CORRELATED CSI

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

In [76], the effects of outdated CSI on secrecy performance was investigated over multiple-input single-output (MISO) systems when the transmit antenna selection (TAS) scheme is applied at Alice. The obtained analytical results show

TABLE 3: Comparisons among the MG, MoG, and Fox's H-function distributions

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

that the diversity gain of using multiple antenna techniques cannot be achieved when the CSI is outdated during the TAS process. Later on in [77], 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 an unrealistic assumption. The impacts of imperfect CSI have been widely explored in diverse research topics, e.g., imperfect CSI in the artificial-noise-assisted training and communication [78], imperfect CSI with an active full-duplex eavesdropper [79], imperfect CSI in a mixed RF/FSO system [37], etc.

Apart from the above two scenarios, the correlation between the main channel and wiretap channel is also attracting a growing body of research interests. In [49], Jeon *et al.* explored the secrecy capacity bounds considering correlated Rayleigh fading channels. The results quantitatively showcased how much of secrecy capacity is lost due to channel correlation. In continuation of this work, the secrecy analysis exploration over correlated Nakagami-m, correlated $\alpha-\mu$, correlated shadowed $\kappa-\mu$ fading channels can be respectively found in [50], [51], [80].

IV. 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 secrecy. In this section, we mainly focus on comparing the existing secrecy enhancement techniques suitable for classical wiretap channels.

A. ON-OFF TRANSMISSION SCHEME

Considering imperfect channel estimation, He and Zhou in [59] 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 ($\hat{\gamma}_B$) and Eve ($\hat{\gamma}_E$) and two given corresponding thresholds i.e., μ_B and μ_E, to be specific, only when $\hat{\gamma}_B \geq \mu_B$ and $\hat{\gamma}_E \leq \mu_E$, the 'on' mode at Alice is activated, otherwise, Alice is in "off" mode. Building on He's work, the on-off transmission is widely investigated in the following secrecy works [77], [81]–[83].

B. ARTIFICIAL NOISE & ARTIFICIAL FAST FADING

Assuming the transmitter has more antennas than the eavesdropper, Goel and Negi proposed the concept of the artificial noise (AN) in [84]. The principle behind AN is that the transmitter uses some of its available power to generate AN to confuse the passive eavesdroppers. Consequently, Wang *et al.* in [85] proposed the artificial fast fading (AFF) secrecy enhancement scheme, where the randomized beamforming is employed at the transmitter in order to 'upgrade' the main channel to an AWGN one and degrade the wiretap channel to a fast fading channel.

C. JAMMING APPROACH

Different from the aforementioned transmitting beamforming-based techniques, namely 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 surveys in [86], [87], one can conclude that jamming is another useful means to further enhance PLS. Considering three-node wiretap fading channel, jamming can be realized by a full-duplex Bob, where Bob would receive signals from Alice and send jamming signals (i.e., noise) to Eve in order to reduce Eve's received SNR quality [88], or a transmitter with directional antennas. Bob and Eve usually only act purely as a legitimate receiver or an illegitimate eavesdropper. However, practically speaking, they might behave with multiple roles. For instance, in [79], an active eavesdropper operates in full-duplex mode so that it can send jamming signals to degrade the legitimate receiver's SNR, while in [89], [90], an untrustworthy relay works as a relay and eavesdropper simultaneously in a bidirectional cooperative network.

D. ANTENNA SELECTION TECHNIQUE

In multiple-antenna systems, TAS is seen as an effective way for reducing hardware complexity whilst boosting diversity benefits. In [80], [83], [91]–[95], TAS is deployed as a secrecy enhancement solution in MIMO systems. There exist three kinds of TAS schemes: (i) the antenna that maximizes the output instantaneous SNR at Bob is selected (see [91], [92]); (ii) more than one single antenna are selected (see [93]); and (iii) a general order of antenna are selected (see [95]).

Different from the works [91]–[94] assuming that the multi-antenna channels are independent, quite recently, Si *et al.* considered antenna correlation in [83], 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 was extended in [80], where continuously took consideration of the joint antenna and channel correlation, while the relationship between the correlation and the SOP is analytically established.

E. PROTECTED ZONES

Protected zones (equivalently, secrecy region) means a geometrical region (see [61], [96]), 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 [25], [97].

V. CONCLUDING REMARKS

In this paper, we have comprehensively summarized the development of PLS over various wiretap fading channels. The existing secrecy analysis works are classified into four categories based on the channel characteristics: (i) small-scale fading; (ii) large-scale fading; (iii) cascaded fading; and (iv) composite fading. By presenting and comparing some major information-theoretic secrecy analysis works, we found three useful and effective approaches, i.e., the MG, MoG, and Fox's H-function distributions, which are introduced to simplify the secrecy analysis. The three aforesaid approaches are beneficial since they can largely cover the existing fading models when the main channel and wiretap channel experience independent fading condition. In addition, we presented the existing secrecy enhancement techniques deployed for Wyner's wiretap channel model, including the on-off transmission, AN and AFF, jamming approach, TAS technique, and protected zones.

REFERENCES

[1] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," IEEE Access, vol. 8, pp. 21 091–21 116, 2020.

[2] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," Proceedings of the National Academy of Sciences, vol. 114, no. 1, pp. 19–26, 2017. [Online]. Available: https://www.pnas.org/content/114/1/19

[3] X. Zhou, L. Song, and Y. Zhang, Physical layer security in wireless communications. CRC Press, 2013.

[4] C. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[8] 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.

[9] Y. Shiu, S. Y. Chang, H. Wu, S. C. . Huang, and H. Chen, "Physical layer security in wireless networks: a tutorial," IEEE Wireless Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Communications Surveys Tutorials, vol. 16, no. 3, pp. 1550–1573, 3rd quarter 2014.

[11] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[12] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 1027–1053, 2nd quarter 2017.

[13] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, Apr. 2018.

[14] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," IEEE Internet Things J., vol. 7, no. 1, pp. 33–52, Jan. 2020.

[15] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," IEEE Trans. Inf. Forensics Security, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[16] X. Liu, "Probability of strictly positive secrecy capacity of the Weibull fading channel," in IEEE GLOBECOM, Atlanta, GA, USA, Dec. 2013, pp. 659–664.

[17] ——, "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.

[18] F. Jameel, Faisal, M. A. A. Haider, and A. A. Butt, "Physical layer security under Rayleigh/Weibull and Hoyt/Weibull fading," in IEEE ICET, Islamabad, Pakistan, Dec. 2017, pp. 1–5.

[19] L. Kong and G. Kaddoum, "Secrecy characteristics with assistance of mixture gamma distribution," IEEE Wireless Commun. Lett., vol. 8, no. 4, pp. 1086–1089, Aug. 2019.

[20] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over non-small-scale fading channels," IEEE Trans. Veh. Technol., vol. 65, no. 3, pp. 1326–1339, Mar. 2016.

[21] 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.

[22] L. Kong, H. Tran, and G. Kaddoum, "Performance analysis of physical layer security over α-μ fading channel," Electron. Lett., vol. 52, no. 1, pp. 45–47, Jan. 2016.

[23] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini, "Secrecy capacity analysis over $\alpha-\mu$ fading channels," IEEE Commun. Lett., vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[24] L. Kong, G. Kaddoum, and Z. Rezki, "Highly accurate and asymptotic analysis on the SOP over SIMO $\alpha-\mu$ fading channels," IEEE Commun. Lett., vol. 22, no. 10, pp. 2088–2091, Oct. 2018.

[25] 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. 11 654–11 666, Dec 2018.

[26] S. Kumar, G. Chandrasekaran, and S. Kalyani, "Analysis of outage probability and capacity for κ - μ/η - μ faded channel," IEEE Commun. Lett., vol. 19, no. 2, pp. 211–214, Feb. 2015.

[27] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," IEEE Trans. Commun., vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[28] S. Iwata, T. Ohtsuki, and P. Y. Kam, "Secure outage probability over κ-μ fading channels," in IEEE ICC, Paris, France, May 2017, pp. 1–6.

[29] J. M. Moualeu and W. Hamouda, "On the secrecy performance analysis of SIMO systems over $\kappa-\mu$ fading channels," IEEE Commun. Lett., vol. 21, no. 11, pp. 2544–2547, Nov. 2017.

[30] 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. 12 421–12 426, Dec. 2018.

[31] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical-layer security over SIMO generalized-K fading channels," IEEE Trans. Veh. Technol., vol. 65, no. 9, pp. 7780–7785, Sept. 2016.

[32] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Performance analysis of physical layer security over generalized-K fading channels using a mixture gamma distribution," IEEE Commun. Lett., vol. 20, no. 2, pp. 408–411, Feb. 2016.

[33] H. Lei, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Physical-layer security over generalised-K fading channels," IET Commun., vol. 10, no. 16, pp. 2233–2237, Nov. 2016.

[34] L. Wu, L. Yang, J. Chen, and M. Alouini, "Physical layer security for cooperative relaying over generalized-K fading channels," IEEE Wireless Commun. Lett., vol. 7, no. 4, pp. 606–609, Aug. 2018.

[35] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over fox's H-function wiretap fading channels," IEEE Trans. Veh. Technol., vol. 68, no. 7, pp. 6608–6621, Jul. 2019.

[36] L. Kong and G. Kaddoum, "On physical layer security over the Fisher-Snedecor $\mathcal{F}$ wiretap fading channels," IEEE Access, vol. 6, no. 1, pp. 39 466–39 472, 2018.

[37] H. Lei, H. Luo, K. H. Park, Z. Ren, G. Pan, and M. S. Alouini, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," IEEE Photon. J., vol. 10, no. 3, pp. 1–13, Jun. 2018.

[38] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martínez, M. C. P. Paredes, and L. Urquiza-Aguiar, "Physical layer security of TAS/MRC over κ-μ shadowed fading channel," 2020.

[39] Y. Ai, L. Kong, and M. Cheffena, "Secrecy outage analysis of double shadowed Rician channels," Electron. Lett., vol. 55, no. 13, pp. 765–767, 2019.

[40] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," IEEE Wireless Commun. Lett., vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

[41] S. . Ata, "Secrecy performance analysis over double Nakagami-m fading channels," in IEEE TSP, July 2018, pp. 1–4.

[42] L. Kong, G. Kaddoum, and D. B. da Costa, "Cascaded $\alpha-\mu$ fading channels: Reliability and security analysis," IEEE Access, vol. 6, pp. 41 978–41 992.

[43] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias, and R. A. A. de Souza, "Physical layer security over α-κ-μ and α-η-μ fading channels," IEEE Trans. Veh. Technol., vol. 68, no. 1, pp. 1025–1029, Jan. 2019.

[44] S. Jia, J. Zhang, H. Zhao, and Y. Xu, "Performance analysis of physical layer security over $\alpha-\eta-\kappa-\mu$ fading channels," China Commun., vol. 15, no. 11, pp. 138–148, Nov. 2018.

[45] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On physical layer security of $\alpha-\eta-\kappa-\mu$ fading channels," IEEE Commun. Lett., vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[46] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martínez, M. C. Paredes, and L. Urquiza-Aguiar, "On the secrecy performance over N-wave with diffuse power fading channel," 2020.

[47] R. Singh and M. Rawat, "Secrecy capacity of physical layer over $\kappa-\mu$ /gamma composite fading channel," in IEEE TENCON, Oct 2019, pp. 1472–1477.

[48] H. Al-Hmood and H. Al-Raweshidy, "Performance analysis of physical-layer security over fluctuating Beckmann fading channels," IEEE Access, vol. 7, pp. 119 541–119 556, 2019.

[49] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[50] A. Mathur, Y. Ai, M. Cheffena, and G. Kaddoum, "Secrecy performance of correlated α - μ fading channels," IEEE Commun. Lett., vol. 23, no. 8, pp. 1323–1327, Aug. 2019.

[51] J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, and K. M. Rabie, "Secrecy performance analysis of SIMO systems over correlated κ – μ shadowed fading channels," IEEE Access, vol. 7, pp. 86 090–86 101, 2019.

[52] L. Yang, T. Liu, J. Chen, and M. Alouini, "Physical-layer security for mixed η–μ and $\mathcal{M}$-distribution dual-hop RF/FSO systems," IEEE Trans. Veh. Technol., vol. 67, no. 12, pp. 12 427–12 431, Dec. 2018.

[53] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over Málaga turbulence channels," IEEE Wireless Commun. Lett., vol. 6, no. 2, pp. 274–277, Apr. 2017.

[54] J. Wang, C. Liu, J. Wang, J. Dai, M. Lin, and M. Chen, "Secrecy outage probability analysis over Malaga-Malaga fading channels," in IEEE ICC, Kansas City, MO, USA, May 2018, pp. 1–6.

[55] 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.

[56] H. Zhao, L. Yang, G. Pan, and M. Alouini, "Secrecy outage analysis over fluctuating two-ray fading channels," Electron. Lett., vol. 55, no. 15, pp. 866–868, Jul 2019.

[57] Y. J. Chun, S. L. Cotton, H. S. Dhillon, F. J. Lopez-Martinez, J. F. Paris, and S. K. Yoo, "A comprehensive analysis of 5G heterogeneous cellular systems operating over κ – μ shadowed fading channels," IEEE Trans. Wireless Commun., vol. 16, no. 11, pp. 6995–7010, Nov. 2017.

[58] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," IEEE Trans. Wireless Commun., vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[59] B. He and X. Zhou, "Secure On-Off transmission design with channel estimation errors," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[60] L. Kong, G. Kaddoum, D. B. da Costa, and E. Bou-Harb, "On secrecy bounds of MIMO wiretap channels with ZF detectors," in IEEE IWCMC, Limassol, Cyprus, Jun. 2018, pp. 724–729.

[61] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," IEEE Trans. Veh. Technol., vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[62] D. S. Karas, A. A. Boulogeorgos, and G. K. Karagiannidis, "Physical layer security with uncertainty on the location of the eavesdropper," IEEE Wireless Commun. Lett., vol. 5, no. 5, pp. 540–543, Oct. 2016.

[63] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, and G. K. Karagiannidis, "The Fisher-Snedecor $\mathcal{F}$ distribution: A simple and accurate composite fading model," IEEE Commun. Lett., vol. 21, no. 7, pp. 1661–1664, Jul. 2017.

[64] H. Lei, Z. Dai, I. S. Ansari, K. H. Park, G. Pan, and M. S. Alouini, "On secrecy performance of mixed RF-FSO systems," IEEE Photon. J., vol. 9, no. 4, pp. 1–14, Aug. 2017.

[65] S. . Ata, "Secrecy performance analysis over cascaded fading channels," IET Commun., vol. 13, no. 2, pp. 259–264, 2019.

[66] L. Kong, Y. Ai, J. He, N. Rajatheva, and G. Kaddoum, "Intercept probability analysis over the cascaded Fisher-Snedecor $\mathcal{F}$ fading wiretap channels," in IEEE ISWCS, Oulu, Finland, Aug. 2019, pp. 672–676.

[67] L. Kong, S. Chatzinotas, and B. Ottersten, "Unified framework for secrecy characteristics with mixture of gaussian (MoG) distribution," submitted to IEEE Wireless Commun. Lett., 2020.

[68] N. Li, X. Tao, and J. Xu, "Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback," IEEE Commun. Lett., vol. 18, no. 6, pp. 969–972, Jun. 2014.

[69] S. Atapattu, C. Tellambura, and H. Jiang, "A mixture gamma distribution to model the SNR of wireless channels," IEEE Trans. Wireless Commun., vol. 10, no. 12, pp. 4193–4203, Dec. 2011.

[70] H. Al-Hmood and H. S. Al-Raweshidy, "Unified modeling of composite $\kappa-\mu$/gamma, $\eta-\mu$/gamma, and $\alpha-\mu$/gamma fading channels using a mixture gamma distribution with applications to energy detection," IEEE Antennas Wireless Propag. Lett, vol. 16, pp. 104–108, 2017.

[71] B. Selim, O. Alhussein, S. Muhaidat, G. K. Karagiannidis, and J. Liang, "Modeling and analysis of wireless channels via the mixture of gaussian distribution," IEEE Trans. Veh. Technol., vol. 65, no. 10, pp. 8309–8321, Oct. 2016.

[72] F. Yilmaz and 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., vol. 60, no. 7, pp. 1862–1876, Jul. 2012.

[73] H. R. Alhennawi, M. M. H. E. Ayadi, M. H. Ismail, and 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., vol. 65, no. 4, pp. 1957–1974, Apr. 2016.

[74] Y. Jeong, J. W. Chong, H. Shin, and M. Z. Win, "Intervehicle communication: Cox-Fox modeling," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 418–433, Sep. 2013.

[75] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, Integrals and Series: More special functions. Gordon and Breach Science Publishers, 1990, vol. 3.

[76] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," IEEE Commun. Lett., vol. 17, no. 5, pp. 864–867, May 2013.

[77] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On-off-based secure transmission design with outdated channel state information," IEEE Trans. Veh. Technol., vol. 65, no. 8, pp. 6075–6088, Aug. 2016.

[78] T. Liu, S. Lin, and Y. . P. Hong, "On the role of artificial noise in training and data transmission for secret communications," IEEE Trans. Inf. Forensics Security, vol. 12, no. 3, pp. 516–531, 2017.

[79] L. Kong, J. He, G. Kaddoum, S. Vuppala, and L. Wang, "Secrecy analysis of a MIMO full-duplex active eavesdropper with channel estimation errors," in IEEE VTC-Fall, Montreal, Quebec, Canada, Sept. 2016, pp. 1–5.

[80] J. Si, Z. Li, J. Cheng, and C. Zhong, "Asymptotic secrecy outage performance for TAS/MRC over correlated Nakagami-m fading channels," IEEE Trans. Commun., vol. 67, no. 11, pp. 7700–7714, Nov. 2019.

[81] P. Mu, Z. Li, and B. Wang, "Secure on–off transmission in slow fading wiretap channel with imperfect CSI," IEEE Trans. Veh. Technol., vol. 66, no. 10, pp. 9582–9586, Oct. 2017.

[82] J. Yao, X. Zhou, Y. Liu, and S. Feng, "Secure transmission in linear multihop relaying networks," IEEE Trans. Wireless Commun., vol. 17, no. 2, pp. 822–834, Feb. 2018.

[83] J. Si, Z. Li, J. Cheng, and C. Zhong, "Secrecy performance of multi-antenna wiretap channels with diversity combining over correlated Rayleigh fading channels," IEEE Trans. Wireless Commun., vol. 18, no. 1, pp. 444–458, Jan. 2019.

[84] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[85] H. Wang, T. Zheng, and X. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," IEEE Trans. Wireless Commun., vol. 14, no. 1, pp. 94–106, Jan. 2015.
[86] M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in IEEE ICUWB, Montreal, Quebec, Canada, Oct 2015, pp. 1–5.
[87] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," IEEE Wireless Commun., vol. 25, no. 1, pp. 148–153, Feb. 2018.
[88] 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.
[89] C. Jeong, I. Kim, and 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. Processing, vol. 60, no. 1, pp. 310–325, Jan. 2012.
[90] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," IEEE Wireless Commun. Lett., vol. 3, no. 3, pp. 289–292, Jun. 2014.
[91] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," IEEE Commun. Lett., vol. 17, no. 9, pp. 1754–1757, Spet. 2013.
[92] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," IEEE Trans. Wireless Commun., vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
[93] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," IEEE Trans. Commun., vol. 61, no. 1, pp. 144–154, Jan. 2013.
[94] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," IEEE Trans. Veh. Technol., vol. 65, no. 1, pp. 214–225, Jan. 2016.
[95] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," IEEE Trans. Commun., vol. 63, no. 8, pp. 2959–2971, Aug. 2015.
[96] T. X. Zheng, H. M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," IEEE Commun. Lett., vol. 18, no. 8, pp. 1299–1302, Aug. 2014.
[97] S. Vuppala, S. Biswas, and T. Ratnarajah, "Secrecy outage analysis of kth best link in random wireless networks," IEEE Trans. Commun., vol. 65, no. 10, pp. 4478–4491, Oct. 2017.