Achieving Covertness and Secrecy: A New Paradigm for Secure Wireless Communication

Huihui Wu, Yuanyu Zhang, Member, IEEE, Yulong Shen, Member, IEEE, Xiaohong Jiang, Senior Member, IEEE, and Weidong Yang

Abstract

This paper explores a novel secure wireless communication paradigm where the physical layer security technology is applied to counteract both detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the communication are jointly guaranteed. To understand the fundamental security performance under this paradigm, we first define a new metric-covert secrecy rate (CSR) to represent the maximum transmission rate subject to the constraints of both covertness and secrecy, and then provide theoretical modeling for covertness outage probability and secrecy outage probability to depict the covertness and secrecy performances of the paradigm. We further conduct detailed theoretical analysis to identify the CSR under various scenarios characterized by the detector-eavesdropper relationships and the secure transmission schemes adopted in transmitters. Finally, numerical results are provided to illustrate the achievable performances under the new paradigm.

Index Terms

Wireless communication, covertness, secrecy, physical layer security.

I. INTRODUCTION

Due to the broadcast nature of wireless medium, wireless communications suffer from various security attacks, among which two typical ones are detection and eavesdropping [1], [2]. In the
detection attack, malicious detectors attempt to detecting the existence of signals transmitted from certain transmitters, impairing the covertness of the transmissions [3], [4]. In the eavesdropping attack, eavesdroppers manage to intercept the information conveyed by the transmitted signals, degrading the secrecy of the transmissions [5], [6].

Classical technologies for guaranteeing the covertness and secrecy properties of wireless communications are usually implemented at the upper layers of the protocol stack [1]. The most representative ones are steganography [7] and cryptography [8]. The steganography technology conceals messages in covertext objects (e.g., image, voice and video files) to achieve covertness [9]. However, the messages remain in the covertext objects permanently and will be eventually recovered by adversaries with high probability. Besides, the messages cannot be transmitted without the covertext objects, which poses a significant challenge to the covert message delivery when the transmissions of covertext objects are prohibited. The cryptography technology achieves secrecy by using secret keys and complex encryption algorithms to convert plaintext messages into ciphertexts [10]. The management of the secret keys and execution of the encryption algorithms usually require a large amount of resources (e.g., bandwidth and computation power), making the cryptography technology too expensive for resource-limited wireless networks, such as sensor networks and the Internet of Things [11], [12].

To propose more promising solutions, security researchers have recently shifted their focus to the physical layer security (PLS) technology. The fundamental principle behind the PLS technology is to exploit the inherent physical layer randomness of wireless channels (e.g., noise and fading) to achieve covertness and secrecy [13]. For example, transmitters can intentionally inject artificial noise (AN) into their channels to hide their signals from detectors or to add uncertainty to the information intercepted by eavesdroppers. Compared with the steganography technology, the PLS technology directly hides the transmitted signals into channels without relying on the covertext objects, thus improving the covertness and flexibility of the message delivery. Compared with the cryptography technology, the PLS technology achieves a stronger form of secrecy (i.e., information-theoretic security) at lower resource cost and thus is more appealing for wireless communications [14]. Moreover, the PLS technology can also be used as an effective supplement for the cryptography technology to significantly enhance the secrecy of wireless communications [15].

Extensive works have been done to investigate either the covertness or secrecy issue of wireless communications based on the PLS technology. For the introduction of these works, please refer to
the Related Work section. These works focus on the traditional paradigms where only one attack type exists, be it detection or eavesdropping. However, in practice, both attack types may coexist, especially in some critical scenarios containing multiple groups with common or conflicting goals, like military communications and coastal surveillance. Therefore, this paper aims to explore a novel secure wireless communication paradigm where the PLS technology is applied to counteract both the detection and eavesdropping attacks. To the best of our knowledge, this is the first paper that jointly studies the covertness and secrecy issues of wireless communications at the physical layer. We anticipate that this work can open a new avenue for the research on secure wireless communications and inspire extensive high-quality subsequent works. The main contributions of this paper are summarized as follows.

- **A novel secure wireless communication paradigm**: In this paradigm, the PLS technology is applied to guarantee the covertness and secrecy properties of wireless communications against both the detection and eavesdropping attacks. To demonstrate the novel paradigm, we consider six representative communication scenarios, which are characterized by the detector-eavesdropper relationships (i.e., independence, friend and enemy) and the secure transmission schemes adopted by the transmitters (i.e., a power control (PC)-based scheme and an AN-based scheme). In the independence relationship, the detector group and eavesdropper group focus on their own attack without caring about the other. In the friend relationship, the two groups exchange their signals received from target transmitters to improve the attack abilities of both sides, while in the enemy relationship, the two group intentionally send ANs to degrade the attack ability of the other. This new paradigm is expected to serve as the benchmark model in this new research avenue.

- **A new security metric characterizing both covertness and secrecy**: Covert rate and secrecy rate are typical metrics to characterize the covertness and secrecy properties of wireless communications, respectively, while they fail to model the fundamental security performance under the novel paradigm, where the two properties must be jointly guaranteed. This paper therefore defines a new security metric called covert secrecy rate (CSR) to represent the maximum transmission rate subject to the constraints of both overtiness and secrecy. This new metric is anticipated to serve as the fundamental security criterion in this new research avenue.

- **CSR analysis for the new paradigm**: For the modeling of the CSR performance, the
covertness outage probability (COP), i.e., the probability that detectors detect the transmitted signals, and secrecy outage probability (SOP), i.e., the probability that eavesdroppers recover the information conveyed by the signals, are first derived to characterize the covertness and secrecy performances, respectively. Under the constraints of COP and SOP, an optimization problem is then formulated and solved to obtain the CSR. Following these steps, we analyze the CSR performances for the six representative communication scenarios. Finally, extensive numerical results are provided to illustrate the CSR performances of the various scenarios.

The rest of this paper is organized as follows. Section II introduces the related work. Section III presents an example system for the new paradigm and the definition of CSR. Theoretical analyses for the CSR performance under the six communication scenarios are given in Section IV, Section V and Section VI respectively. Section VII provides numerical results to illustrate the CSR performances and Section VIII concludes this paper.

II. RELATED WORK

Available works have been focusing on traditional paradigms, where only the detection or eavesdropping attack is counteracted. However, none of them jointly considered protecting transmissions from both attacks as in our novel secure communication paradigm. This significantly distinguishes our work from the available ones. In what follows, we introduce the available works related to this paper with a particular focus on the three-node scenario consisting of one transmitter, one receiver and one attacker (i.e., detector or eavesdropper).

To secure transmissions from the detection attack in the three-node scenario, Bash et al. [16] proposed a PC-based scheme to make the detector unable to distinguish between message signals and background noise. Based on this scheme, they derived the scaling-law results of the covert rate, i.e., the maximum number of bits transmitted per channel use without being detected. This work was originally done for additive Gaussian white noise (AGWN) channels with a static detector, and was later extended to the scenario with a mobile detector [17] and other channel models such as binary symmetric channels (BSCs) [18] and discrete memoryless channels (DMCs) [19], [20]. These scaling-law results show how the covert rate scales up as the number of channel uses tends to infinity, while they fail to reflect the exact covertness performances of more practical scenarios with finite parameters.

Thus, researchers began to devote their efforts to the exact covertness analysis. A variant three-node scenario was considered in [21], where a greedy relay wishes to transmit its own
covert messages to the receiver while forwarding the transmitter’s messages. To avoid being detected by the transmitter, the relay adopts the PC-based scheme to control its transmit power. For the covertness modeling, the authors derived the detection error probability of the transmitter and also the covert rate. The authors in [22] considered a full-duplex receiver, which generates AN while receiving signals from the transmitter in a Rayleigh fading channel, and obtained the maximum detection error probability of the detector under a given constraint of the minimum required covert rate. For scenarios with a half-duplex receiver, the covert rate performances were analyzed under the PC-based scheme and various assumptions. For example, the detector was assumed to have no knowledge about the time slots in which the transmitter sends messages to the receiver [23], [24], about the instantaneous channel coefficient or statistical characteristic of its channel [25], [26], and about the exact background noise power [27]–[29]. As building blocks, the results in these three-node scenarios can also be extended to other scenarios, like the multiple access channels (MACs) [30], broadcast channels [31], [32], relay channels [33], [34] and multi-detector scenarios [35].

The study of securing wireless communications against the eavesdropping attack at the physical layer was pioneered by [36], where the classic wiretap channel model and the notion of secrecy rate were introduced. The results in [36] reveal that positive secrecy rates can be achieved when the transmitter-eavesdropper channel is a degraded version of the transmitter-receiver channel. This work was later extended to other channel models, like the Gaussian wiretap channel [37], the BSC [38] and the type-II wiretap channel [39]. Recent studies in this filed for three-node scenarios mainly focused on the fading channel model and adopted the SOP [40] as one of the main performance metrics and the AN-based scheme as one of the fundamental PLS techniques. The authors in [41] adopted an AN-based scheme where the transmitter splits its power between message transmission and AN transmission. Different from our AN-based scheme, the receiver in [41] is assumed to be able to cancel the AN out from the received signals. The optimal power allocation parameters were determined to minimize the SOP and maximize the secrecy rate, respectively. A similar AN-based scheme was adopted in [42] for a scenario with an active full-duplex eavesdropper, which also transmits AN while intercepting messages. Same to our AN-based scheme, the cancellation of the AN from the transmitter is not available at the receiver side. The SOP and secrecy rate performances were also optimized over the power allocation parameter, respectively. Helper nodes can also be added to the three-node scenario to take over the job of AN generation from the transmitter [43], [44]. The secrecy performance analyses in
the three-node scenario can also be extended to other large-scale scenarios, e.g., like Ad Hoc networks \[45\], \[46\], device-to-device (D2D) communications \[47\], \[48\], cellular networks \[49\], \[50\] and the Internet of Things (IoT) \[51\].

### III. NOVEL PARADIGM AND ITS SECURITY METRIC

To demonstrate the novel secure wireless communication paradigm, we consider a system (as illustrated in Fig. 1) where a transmitter Alice sends messages to a receiver Bob in the presence of a detector Willie and an eavesdropper Eve. Willie attempts to detecting the existence of the signals transmitted from Alice, while Eve targets the messages contained in the signals. Alice and Bob operate in the half-duplex mode, while Willie and Eve can operate in the full-duplex mode when necessary. All nodes are assumed to be equipped with a single omnidirectional antenna. For notation simplicity, we use \( a \), \( b \), \( e \) and \( w \) to represent Alice, Bob, Eve and Willie, respectively, throughout this paper.

Time is divided into successive slots with equal duration that is long enough for Alice to transmit multiple symbols. To characterize the channels, we adopt the quasi-static Rayleigh fading channel model, where the channel coefficients remain constant in one slot and change independently from one slot to another at random. We use \( h_{ij} \) to denote the coefficient of the channel from \( i \) to \( j \), where \( i \in \{a, b, e, w\} \) and \( j \in \{a, b, e, w\} \). As assumed in \[21\], the corresponding channel gain \( |h_{ij}|^2 \) follows the exponential distribution with unit mean. We assume that Alice knows the instantaneous channel coefficient \( h_{ab} \) but only the statistical characterizations of \( h_{aw}, h_{ae}, h_{ew} \) and \( h_{we} \). We also assume that Eve knows the statistical characterization of \( h_{ae} \) and Willie knows the statistical characterizations of \( h_{aw} \) and \( h_{ew} \).

#### A. Secure Transmission Schemes

To counteract the attacks from Willie and Eve, Alice first adopts a random on-off transmission scheme, where she decides to transmit with probability \( q \) and thus suspends her transmission with probability \( 1 - q \) in each time slot. We assume that this decision is only known to Alice and Bob. When Alice transmits, she then employs two transmission schemes based on power control (PC) and artificial noise (AN) injection, respectively. In the PC-based scheme, Alice controls her transmit power \( P_a \) in order to hide the message signals into the background noise to achieve covertness and secrecy. In the AN-based scheme, Alice intentionally injects AN into the message signals to confuse Willie and Eve so as to reduce their attack effects. Different
from the PC-based scheme, in the AN-based scheme, Alice uses a constant transmit power, also denoted by $P_a$, and splits the power between message and noise transmissions. We use $\rho \in (0, 1]$ to denote the fraction of transmit power used for the message transmission. In addition to the above strategies on transmit power, Alice also adopts the Wyner encoding scheme [36] to resist the eavesdropping of Eve. To transmit a message, Alice chooses a target secrecy rate $R_s$ for this message and another rate $R_t > R_s$ for the whole transmitted symbol. The difference $R_t - R_s$ represents the rate sacrificed to confuse Eve. We assume that $R_s$ is fixed for all transmissions throughout this paper.

**B. Attacking Model**

In practice, Willie and Eve can belong to different organizations with common or conflicting goals, resulting in various relationships between them. In this paper, we consider three representative relationships, i.e., independence, friend and enemy. As shown in Fig. 1 in the independence relationship, Eve and Willie care only about their own attack without helping or hindering the other. In the friend relationship, Willie and Eve will share their signals received from Alice to help improve the attack power of the other. In the enemy relationship, Willie and Eve intentionally radiate AN to degrade the attack power of the other.

To detect the existence of signals transmitted from Alice in each slot, Willie adopts the commonly-used likelihood ratio test [52], in which he first determines a threshold $\theta$ and then measures the average power $\bar{P}_w$ of the symbols received from Alice in this slot. If $\bar{P}_w \geq \theta$, Willie accepts a hypothesis $\mathcal{H}_1$ that Alice transmitted messages to Bob in this slot. If $\bar{P}_w \leq \theta$, Willie accepts a hypothesis $\mathcal{H}_0$ that Alice did not transmit messages. Formally, the likelihood ratio test can be given by

$$\bar{P}_w \overset{\mathcal{H}_1}{\gtrless} \theta.$$  \hspace{1cm} (1)

In general, the likelihood test introduces two types of detection errors. One is called *false alarm*, which means that Willie reports a detected transmission whilst the transmission does not exist in fact. The other is called *missed detection*, which means that Willie reports no detected transmission whilst the transmission exists indeed. We use $p_{FA}$ and $p_{MD}$ to denote the probabilities of false alarm and missed detection, respectively. If neither false alarm or missed
detection occurs, the transmission from Alice to Bob is said to suffer from covertness outage. Thus, the **covertness outage probability (COP)** is given by

\[
p_{co} = 1 - (p_{FA} + p_{MD}).
\]  

(2)

The smaller the COP is, the higher the covertness of the transmission is. Note that \(1 - p_{co}\) can be interpreted as the detection error probability of Willie.

Compared with the detection of Willie, the eavesdropping attack of Eve is relatively simpler. To intercept the transmitted messages, Eve tries to decode the signals received from Alice. If Eve is able to recover the messages, the transmission from Alice to Bob is said to suffer from secrecy outage. According to [40], the **secrecy outage probability (SOP)** can be formulated as the probability that the instantaneous secrecy capacity \(C_s\) [53] of the Alice-Bob channel falls below the target secrecy rate \(R_s\). We use \(p_{so}\) to denote the SOP, which can be given by

\[
p_{so} = P(C_s < R_s).
\]  

(3)
Similarly, the smaller the SOP is, the stronger the secrecy of the transmission is.

C. Covert Secrecy Rate

To understand the fundamental security performance under the new paradigm, this paper defines a new metric, called covert secrecy rate (CSR), by jointly combining the covertness and secrecy. The CSR is defined as the maximum transmission rate under which both covertness and secrecy can be ensured. To obtain the CSR, we formulate two optimization problems for the PC-based and AN-based transmission schemes, respectively, which are given by

\[
P_1 \text{(PC-based): } R_{cs} = \max_{P_a} q(1 - p_{so}(P_a))R_s, \tag{4a}
\]

\[
\text{s.t. } p_{co}(P_a) \leq \epsilon_c, \tag{4b}
\]

\[
p_{so}(P_a) \leq \epsilon_s, \tag{4c}
\]

and

\[
P_2 \text{(AN-based): } R_{cs} = \max_{\rho \in [0,1]} q(1 - p_{so}(\rho))R_s, \tag{5a}
\]

\[
\text{s.t. } p_{co}(\rho) \leq \epsilon_c, \tag{5b}
\]

\[
p_{so}(\rho) \leq \epsilon_s, \tag{5c}
\]

where \( R_{cs} \) denotes the CSR, \( \epsilon_c \) and \( \epsilon_s \) denote the requirements of covertness and secrecy. Note that Problem P1 optimizes the transmission rate over the transmit power \( P_a \), while Problem P2 conducts the optimization over the power allocation parameter \( \rho \).

IV. CSR Analysis: The Independence Relationship Case

In this section, we investigate the CSR performance under the independence relationship case, for which we focus on the PC-based and AN-based transmission schemes in Subsections [IV-A] and [IV-B] respectively.

A. PC-Based Transmission Scheme

When Alice decides to transmit in a certain time slot, she sends \( n \) symbols to Bob, represented by a complex vector \( x \), where each symbol \( x[i] \) \((i = 1, 2, \cdots, n)\) is subject to the unit power constraint, i.e., \( \mathbb{E}[|x[i]|^2] = 1 \). Thus, the signal vectors received at Bob, Willie and Eve are given by

\[
y_\kappa = \sqrt{P_a}h_{ae}\kappa + n_\kappa, \tag{6}
\]
where the subscript $\kappa \in \{b, w, e\}$ stands for Bob, Willie or Eve, $a$ represents Alice, and $n_\kappa$ denotes the noise at $\kappa$ with the $i$-th element $n_\kappa[i]$ being the complex additive Gaussian noise with zero mean and variance $\sigma^2_\kappa$, i.e., $n_\kappa[i] \sim CN(0, \sigma^2_\kappa)$.

According to the detection scheme in Subsection III-B, Willie makes a decision on the existence of transmitted signals based on the average power $\bar{P}_w$ of the received symbols $y_w$. In this case, $\bar{P}_w$ is given by

$$\bar{P}_w = \frac{\sum_{i=1}^{n} |y_w[i]|^2}{n} = \lim_{n \to \infty} (P_a|h_{aw}|^2 + \sigma^2_w)\chi^2_{2n}/n = P_a|h_{aw}|^2 + \sigma^2_w, \quad (7)$$

where $\chi^2_{2n}$ represents a chi-squared random variable with $2n$ degrees of freedom. By the Strong Law of Large Numbers [54], $\chi^2_{2n}/n$ converges in probability to $1$ as $n$ tends to infinity. If $\bar{P}_w \leq \theta$, Willie accepts the hypothesis $H_0$ that Alice did not transmit messages, leading to a missed detection. Thus, the probability of missed detection $p_{MD}$ is given by

$$p_{MD} = P(\sigma^2_w \leq \theta) = \begin{cases} 1 - \exp\left(\frac{-\theta - \sigma^2_w}{P_a}\right), & \theta > \sigma^2_w, \\ 0, & \theta \leq \sigma^2_w. \end{cases} \quad (8)$$

The eavesdropping effect of Eve depends on the instantaneous secrecy capacity $C_s$ of the Alice-Bob channel. According to [53], $C_s$ is the difference between the channel capacity of the Alice-Bob channel and that of the Alice-Eve channel. Thus, $C_s$ can be formulated as

$$C_s = \log \left(1 + \frac{P_a|h_{ab}|^2}{\sigma^2_b} \right) - \log \left(1 + \frac{P_a|h_{ae}|^2}{\sigma^2_e} \right), \quad (9)$$

where $\log$ is to the base of 2. Note that $|h_{ab}|^2$ is known to Alice and thus is treated as a constant. The only random variable here is $|h_{ae}|^2$. Based on the definition of the SOP in Section III-B, the SOP $p_{so}$ under the PC-based scheme can be given by

$$p_{so}(P_a) = P\left(\frac{P_a|h_{ab}|^2}{\sigma^2_b} - \frac{2R_s P_a|h_{ae}|^2}{\sigma^2_e} < 2R_s - 1\right) = \exp\left(-\frac{\sigma^2_e}{2R_s} \left(\frac{|h_{ab}|^2}{\sigma^2_b} - \frac{2R_s - 1}{P_a}\right)\right). \quad (10)$$

When Alice does not transmit, only noises are received at Bob, Willie and Eve. In this case, the secrecy of the transmission is not a concern. Thus, we focus only on the received signal of Willie, i.e., $y_w = n_w$. We can see that the average power $\bar{P}_w$ of the received symbols $y_w$ is $P_w = \sigma^2_w$. If $P_w \geq \theta$, Willie accepts the hypothesis $H_1$ that Alice transmitted messages, leading to a false alarm. Thus, the probability of false alarm $p_{FA}$ is given by

$$p_{FA} = P(\sigma^2_w \geq \theta) = \begin{cases} 0, & \theta > \sigma^2_w, \\ 1, & \theta \leq \sigma^2_w. \end{cases} \quad (11)$$
Combining the $p_{MD}$ in (8) and the $p_{FA}$ in (11), we obtain the COP under the PC-based scheme as

$$p_{co}^{IP}(P_a, \theta) = \begin{cases} \exp \left( -\frac{\theta - \sigma_w^2}{P_a} \right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \quad (12)$$

Note that the COP is identical for Alice and Willie, since they have the same knowledge about $|h_{aw}|^2$, i.e., the statistical $|h_{aw}|^2$. To maximize the COP $p_{co}^{IP}$, Willie will choose the optimal detection threshold $\theta$, denoted by $\theta_{IP}^*$. We can see from (12) that $p_{co}^{IP}$ is a decreasing function of $\theta$ and is larger than or equal to 0 for $\theta > \sigma_w^2$. Thus, the optimal $\theta_{IP}^*$ exists in $(\sigma_w^2, \infty)$ and is thus given by $\theta_{IP}^* = \nu + \sigma_w^2$, where $\nu > 0$ is an arbitrarily small value.

Under the condition that Willie chooses the optimal detection threshold $\theta_{IP}^*$, Alice solves the optimization problem in (4) to obtain the CSR. The main result is summarized in the following theorem.

**Theorem 1.** Under the scenario where Willie and Eve are in the independence relationship and Alice adopts the PC-based secure transmission scheme, the CSR of the system is

$$R_{cs}^{IP} = qR_s \left( 1 - p_{so}^{IP} \left( -\frac{\nu}{\ln \epsilon_c} \right) \right), \quad (13)$$

under the following condition:

$$R_s \leq \log \left( \frac{\sigma_w^2 \sigma_b^2 \ln \epsilon_c - |h_{ab}|^2 \sigma_e^2 \nu}{\sigma_e^2 \sigma_b^2 \ln \epsilon_c + \sigma_b^2 \nu \ln \epsilon_s} \right), \quad (14)$$

where $p_{so}^{IP}(\cdot)$ is given by (10). Otherwise, the CSR is not available.

**Proof.** We can see from (10) and (12) that, as $P_a$ increases, $p_{so}^{IP}$ monotonically decreases while $p_{co}^{IP}$ monotonically increases. Thus, according to the constraint (4b), the maximum allowable $P_a$ is given by

$$P_{a,IP}^{max} = -\frac{\nu}{\ln \epsilon_c}. \quad (15)$$

According to the constraint (4c), the minimum allowable $P_a$ is given by

$$P_{a,IP}^{min} = \frac{(2R_s - 1)\sigma_e^2 \sigma_b^2}{2R_s \sigma_e^2 \ln \epsilon_s + |h_{ab}|^2 \sigma_e^2}. \quad (16)$$

Note that the inequality $P_{a,IP}^{min} \leq P_{a,IP}^{max}$ must hold, which gives the condition on $R_s$ in (14). Since the objective function in (4a) is an increasing function of $P_a$, the CSR $R_{cs}^{IP}$ is thus obtained at $P_a = P_{a,IP}^{max}$, which is given by (13).

$\square$
B. AN-Based Transmission Scheme

Under the AN-based transmission scheme, when Alice transmits, in addition to the message symbols, she also injects AN, represented by a complex vector $z_i$ ($i = 1, 2, \ldots, n$) subject to the unit power constraint, i.e., $\mathbb{E}[|z_i|^2] = 1$. Alice uses a fraction $\rho$ of her transmit power $P_a$ for message transmission and the remaining power for AN transmission. Thus, the signal vectors received at Bob, Willie and Eve are given by

$$y_\kappa = \sqrt{\rho P_a h_{\kappa}} x + \sqrt{(1-\rho) P_a h_{\kappa}} z + n_\kappa,$$  \hspace{1cm} (17)

where the subscript $\kappa \in \{b, w, e\}$ stands for Bob, Willie or Eve and $a$ represents Alice.

From (17), we can see that the average power $\bar{P}_w$ of the received symbols $y_\kappa$ at Willie is the same as that given in (7). Thus, the probability of missed detection $p_{MD}$ under the AN-based scheme can also be given by (8).

Based on (17), we can formulate the secrecy capacity $C_s$ under the AN-based scheme as

$$C_s = \log \left( 1 + \frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} \right) - \log \left( 1 + \frac{\rho P_a |h_{ae}|^2}{(1-\rho) P_a |h_{ae}|^2 + \sigma_e^2} \right).$$  \hspace{1cm} (18)

Thus, following the definition of SOP in (3), we derive the SOP under the AN-based scheme as

$$p_{so}^{IA}(\rho) = \mathbb{P} \left( \frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} - \frac{2^{R_s} \rho P_a |h_{ae}|^2}{(1-\rho) P_a |h_{ae}|^2 + \sigma_e^2} < 2^{R_s} - 1 \right) = \exp \left( - \frac{2^{R_s} \rho P_a |h_{ab}|^2 \sigma_b^2 - \mu \sigma_e^2}{\rho P_a (2^{R_s} \sigma_b^2 - \mu)} + \mu P_a \right),$$  \hspace{1cm} (19)

where $\mu = (2^{R_s} - 1)(P_a |h_{ab}|^2 + \sigma_b^2)$.

On the other hand, when Alice does not transmit messages, she still generates AN to confuse Willie, which is different from the PC-based scheme. Thus, the signal vector $y_w$ received by Willie consists of both the AN $z$ and background noise, i.e.,

$$y_w = \sqrt{(1-\rho) P_a h_{aw}} z + n_w.$$  \hspace{1cm} (20)

In this case, the average power of the received symbols of Willie is $\bar{P}_w = (1-\rho) P_a |h_{aw}|^2 + \sigma_w^2$, and thus the probability of false alarm is given by

$$p_{FA} = \mathbb{P} \left( (1-\rho) P_a |h_{aw}|^2 + \sigma_w^2 \geq \theta \right) = \begin{cases} \exp \left( - \frac{(\theta - \sigma_w^2)}{(1-\rho) P_a} \right), & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2. \end{cases}$$  \hspace{1cm} (21)
Combining the \( p_{FA} \) in (21) and the \( p_{MD} \) in (8), we obtain the COP \( p_{co}^{IA} \) under the AN-based scheme as

\[
p_{co}^{IA}(\rho, \theta) = \begin{cases} 
\exp \left( -\frac{(\theta - \sigma_w^2)}{P_a} \right) - \exp \left( -\frac{(\theta - \sigma_w^2)}{(1-\rho)P_a} \right), & \theta > \sigma_w^2, \\
0, & \theta \leq \sigma_w^2.
\end{cases}
\] (22)

We can see from (22) that the optimal detection threshold \( \theta_{IA}^* \) for Willie exists when \( \theta > \sigma_w^2 \) and can be obtained by solving \( \frac{\partial p_{co}^{IA}}{\partial \theta} = 0 \). Thus, the optimal detection threshold \( \theta_{IA}^* \) is given by

\[
\theta_{IA}^* = \sigma_w^2 + \frac{(\rho - 1)P_a}{\rho} \ln(1 - \rho).
\] (23)

By solving the optimization problem in (5) with \( \theta = \theta_{IA}^* \), we can obtain the CSR, which is given in the following theorem.

**Theorem 2.** Under the scenario where Willie and Eve are in the independence relationship and Alice adopts the AN-based secure transmission scheme, the CSR of the system is

\[
R_{cs}^{IA} = qR_s \left( 1 - p_{so}^{IA}(\rho_{IA}^*) \right),
\] (24)

where \( p_{so}^{IA}(\cdot) \) is given by (19) and the optimal power allocation parameter \( \rho_{IA}^* \) solves \( p_{co}^{IA}(\rho, \theta_{IA}^*) = \epsilon_c \) with \( \theta_{IA}^* \) given by (23). Note that \( \rho_{IA}^* \) must satisfy the condition \( \rho_{IA}^* \geq \rho_{IA}^{min} \) with \( \rho_{IA}^{min} \) given by

\[
\rho_{IA}^{min} = \frac{\mu \sigma_e^2 - \mu P_a \ln \epsilon_s}{2R_s P_a (\sigma_e^2 \ln \epsilon_s + |h_{ab}|^2 \sigma_e^2) - \mu P_a \ln \epsilon_s}.
\] (25)

Otherwise, the CSR is not available.

**Proof.** Taking the derivative of the \( p_{so}^{IA} \) in (19) gives

\[
\frac{\partial p_{so}^{IA}}{\partial \rho} = \frac{(1-2R_s)P_a \sigma_e^2 (P_a |h_{ab}|^2 + \sigma_b^2) - \frac{\sigma_e^2}{(2R_s-1)(1-\rho)P_a |h_{ab}|^2 + (2R_s-1+\rho)P_a \sigma_b^2} \exp \left( -\frac{(\rho^2R_sP_a |h_{ab}|^2 - \mu)\sigma_e^2}{(\mu+\rho \sigma_b^2)P_a - (2R_s-1)\rho P_a^2 |h_{ab}|^2} \right)},
\] (26)

which implies that, as \( \rho \) increases, \( p_{so}^{IA} \) decreases while the objective function in (5a) increases. Thus, the maximum allowable \( \rho \) is the optimal power allocation parameter \( \rho_{IA}^* \).

Substituting \( \theta = \theta_{IA}^* \), where \( \theta_{IA}^* \) is given by (23), into (22) yields

\[
p_{co}^{IA} = \rho (1 - \rho)^{\frac{1-\rho}{\rho}}.
\] (27)

Next, taking the derivative of the \( p_{co}^{IA} \) in (27) in terms of \( \rho \), we have

\[
\frac{\partial p_{co}^{IA}}{\partial \rho} = -\ln(1 - \rho) \left( 1 - \rho \right)^{\frac{1-\rho}{\rho}} > 0,
\] (28)
which shows that $p^{IA}_{co}$ is a decreasing function of $\rho$. Thus, according to the constraint (5b), the maximum allowable $\rho$ (i.e., the $\rho^*_{IA}$) solves the equation $p^{IA}_{co}(\rho) = \epsilon_c$. Substituting the $\rho^*_{IA}$ into (19) gives the CSR in (24). In addition, based on the constraint (5c) and the monotonicity of $p^{IA}_{co}$ with respect to $\rho$, the minimum power allocation parameter $\rho^\text{min}_{IA}$ can be given by (25). Note that $\rho^*_{IA} \geq \rho^\text{min}_{IA}$ must hold. Otherwise, the CSR is not available.

V. CSR Analysis: The Friend Relationship Case

The CSR performance of the friend relationship case is investigated in this section, for which the CSR analyses for the PC-based and AN-based transmission schemes are provided in Subsections V-A and V-B, respectively. To characterize the friend relationship, we interpret Willie and Eve as two antennas of a super attacker. This model is widely used to characterize the collusion among eavesdroppers in PLS-related research [55].

A. PC-Based Transmission Scheme

When Alice transmits a signal vector $x$, Bob receives the same signal vector $y_b$ as that given in (6) under the independence relationship case. However, since Willie and Eve share their received signals in this case, the signal vectors received at Willie and Eve are given by

$$y_\kappa = \sqrt{P_a|h_{aw}|^2}x + \sqrt{P_a|h_{ae}|^2}x + n_e + n_w,$$

where the subscript $\kappa \in \{w, e\}$ stands for Willie or Eve and $a$ represents Alice.

Following the analysis in Subsection IV-A, the average power $\bar{P}_w$ of the received symbols $y_w$ at Willie is given by

$$\bar{P}_w = P_a|h_{aw}|^2 + P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2.$$  

(30)

Note that $|h_{aw}|^2$ and $|h_{ae}|^2$ are random variables for Willie. Thus, the probability of missed detection $p_{MD}$ is given by

$$p_{MD} = \mathbb{P}(P_a|h_{aw}|^2 + P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2 \leq \theta)$$

$$= \begin{cases} 
1 - \frac{P_a + \theta - \sigma_e^2 - \sigma_w^2}{P_a} \exp\left(-\frac{\theta - \sigma_e^2 - \sigma_w^2}{P_a}\right), & \theta > \sigma_e^2 + \sigma_w^2, \\
0, & \theta \leq \sigma_e^2 + \sigma_w^2.
\end{cases}$$

(31)

According to (29), we can formulate the secrecy capacity $C_s$ as

$$C_s = \log\left(1 + \frac{P_a|h_{ab}|^2}{\sigma_b^2}\right) - \log\left(1 + \frac{P_a|h_{ae}|^2 + P_a|h_{aw}|^2}{\sigma_e^2 + \sigma_w^2}\right).$$

(32)
Note that from the viewpoint of Alice, the random variables here are $|h_{ae}|^2$ and $|h_{aw}|^2$, which are independent. Based on (32) and the definition of SOP in (3), the SOP under the PC-based scheme is given by

$$p_{so}^{FP}(P_a) = \mathbb{P}\left(\frac{P_a|h_{ab}|^2}{\sigma_b^2} - 2R_s P_a|h_{ae}|^2 + P_a|h_{aw}|^2 \sigma_e^2 + \sigma_w^2 < 2R_s - 1\right)$$

$$= \left(1 + \frac{\sigma_e^2 + \sigma_w^2}{2R_s} \left(\frac{|h_{ab}|^2}{\sigma_b^2} - 2R_s - 1\right)\right) \exp \left(-\frac{\sigma_e^2 + \sigma_w^2}{2R_s} \left(\frac{|h_{ab}|^2}{\sigma_b^2} - 2R_s - 1\right)\right).$$

(33)

Next, we consider the case where Alice suspends her transmission. Since the decision of suspending transmission is not known to Willie and Eve, they still share their signals, which contain only background noises in this case. Thus, the received signal at Willie is given by

$$y_w = n_e + n_w.$$  

(34)

Hence, the average power $\bar{P}_w$ of the received signal of Willie is $\bar{P}_w = \sigma_e^2 + \sigma_w^2$ and the probability of false alarm $p_{FA}$ can be given by

$$p_{FA} = \mathbb{P}\left(\sigma_e^2 + \sigma_w^2 \geq \theta\right) = \begin{cases} 0, & \theta > \sigma_e^2 + \sigma_w^2; \\ 1, & \theta \leq \sigma_e^2 + \sigma_w^2. \end{cases}$$

(35)

Combining the $p_{FA}$ in (35) and the $p_{MD}$ in (31), we obtain the COP as

$$p_{co}^{FP}(P_a, \theta) = \begin{cases} \frac{P_a + \theta - \sigma_e^2 - \sigma_w^2}{P_a} \exp \left(-\frac{\theta - \sigma_e^2 - \sigma_w^2}{P_a}\right), & \theta > \sigma_e^2 + \sigma_w^2; \\ 0, & \theta \leq \sigma_e^2 + \sigma_w^2. \end{cases}$$

(36)

Taking the derivative of the $p_{co}^{FP}$ in (36) gives

$$\frac{\partial p_{co}^{FP}}{\partial \theta} = -\frac{\theta - \sigma_e^2 - \sigma_w^2}{P_a^2} \exp \left(-\frac{\theta - \sigma_e^2 - \sigma_w^2}{P_a}\right),$$

which proves that $p_{co}^{FP}$ is a decreasing function of $\theta$ when $\theta > \sigma_e^2 + \sigma_w^2$. Thus, the optimal detection threshold is

$$\theta_{FP}^* = \nu + \sigma_e^2 + \sigma_w^2,$$

(38)

where $\nu > 0$ is an arbitrarily small value.

Given the $\theta_{FP}^*$, the SOP in (33) and the COP in (36), the problem in (4) can now be solved to obtain the CSR. The result is given in the following theorem.

**Theorem 3.** Under the scenario where Willie and Eve are in the friend relationship and Alice adopts the PC-based secure transmission scheme, the CSR of the system is

$$R_{cs}^{FP} = qR_s(1 - p_{so}^{FP}(P_{a,FP}^*)),$$

(39)
where \( p_{so}^{FP}(\cdot) \) is given by (33) and the optimal transmit power \( P_{a,FP}^* \) solves \( p_{so}^{FP}(P_a, \theta_{FP}^*) = \epsilon_c \) with \( \theta_{FP}^* \) given by (38). Note that the inequality \( P_{a,FP}^* \geq P_{a,FP}^{min} \) must hold, where \( P_{a,FP}^{min} \) solves \( p_{so}^{FP}(P_a) = \epsilon_s \). Otherwise, the CSR is not available.

Proof. The proof is similar to that of Theorem 1 and thus omitted here. \( \square \)

B. AN-Based Transmission Scheme

When Alice transmits under the AN-based scheme, the received signal vector at Bob is identical to (17), while the signal vectors at Willie and Eve also contain the signal shared by the other side. Thus, the signal vectors received at Willie and Eve are given by

\[
y_{\kappa} = \sqrt{\rho P_a h_{aw}} x + \sqrt{(1-\rho) P_a h_{aw}} z + \sqrt{\rho P_a h_{ae}} x + \sqrt{(1-\rho) P_a h_{ae}} z + n_e + n_w, \tag{40}
\]

where the subscript \( \kappa \in \{w, e\} \) stands for Willie or Eve and \( a \) represents Alice.

In this case, the average power \( \bar{P}_w \) of the received symbols \( y_{\kappa} \) at Willie is the same as that given in (30), and thus the probability of missed detection \( p_{MD} \) can be given by (31).

Based on (40), the secrecy capacity \( C_s \) under the AN-based scheme can be formulated by

\[
C_s = \log \left( 1 + \frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} \right) - \log \left( 1 + \frac{\rho P_a |h_{ae}|^2 + \rho P_a |h_{aw}|^2}{(1-\rho) P_a |h_{ae}|^2 + (1-\rho) P_a |h_{aw}|^2 + \sigma_e^2 + \sigma_w^2} \right), \tag{41}
\]

where the random variables are \( |h_{ae}|^2 \) and \( |h_{aw}|^2 \) for Alice. According to the definition in (3), the SOP is given by

\[
p_{so}^{FA}(\rho) = \mathbb{P} \left( \frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} - \frac{2^{R_s} (\rho P_a |h_{ae}|^2 + \rho P_a |h_{aw}|^2)}{(1-\rho) P_a |h_{ae}|^2 + (1-\rho) P_a |h_{aw}|^2 + \sigma_e^2 + \sigma_w^2} < 2^{R_s} - 1 \right) \\
= \left( 1 + \frac{\phi (\sigma_e^2 + \sigma_w^2)}{((1+\phi) \rho - \phi) P_a} \right) \exp \left( - \frac{\phi (\sigma_e^2 + \sigma_w^2)}{((1+\phi) \rho - \phi) P_a} \right), \tag{42}
\]

where \( \phi = \left( \frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} - 2^{R_s} + 1 \right) / 2^{R_s} \).

When Alice does not transmit messages, she still sends AN to confuse Willie. Thus, the signal vector \( y_w \) contains both the signals (i.e., AN and background noise) shared by Eve, AN and background noise, which is given by

\[
y_w = \sqrt{(1-\rho) P_a h_{aw}} z + \sqrt{(1-\rho) P_a h_{ae}} z + n_e + n_w. \tag{43}
\]
In this case, the average power of the received symbols at Willie is 
\[ P_w = (1 - \rho)P_a|h_{aw}|^2 + (1 - \rho)P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2. \]
Thus, the probability of false alarm \( p_{FA} \) is given by
\[
\begin{align*}
\frac{\partial p_{FA}}{\partial \rho} &= 0, \\
\theta_{FA}^* &= \sigma_e^2 + \sigma_w^2 + 2(\rho - 1)P_a \ln(1 - \rho). \tag{46}
\end{align*}
\]
Given the \( \theta_{FA}^* \) in (46), we solve the optimization problem in (5) to obtain the CSR, which is given in the following theorem.

**Theorem 4.** Under the scenario where Willie and Eve are in the friend relationship and Alice adopts the AN-based secure transmission scheme, the CSR of the system is
\[
R_{cs}^{FA} = qR_s(1 - p_{so}^{FA}(\rho_{FA}^*)), \tag{47}
\]
where \( p_{so}^{FA}(\cdot) \) is given by (42) and the optimal power allocation parameter \( \rho_{FA}^* \) solves \( p_{co}^{FA}(\rho, \theta_{FA}^*) = \epsilon_c \) with \( \theta_{FA}^* \) given by (46). Note that \( \rho_{FA}^* \) must satisfy the following constraints:
* \( p_{so}^{FA}(\rho_{FA}^*, \theta_{FA}^*) \leq \left(1 - \frac{\sigma_e^2 + \sigma_w^2}{P_a}\right) \exp\left(\frac{\sigma_e^2 + \sigma_w^2}{P_a}\right); \)
* \( \rho_{FA}^* \geq \rho_L \), where \( \rho_L \) is the larger one of the two solutions of \( p_{so}^{FA}(\rho, \theta_{FA}^*) = \epsilon_s. \)

Otherwise, the CSR is not available.

**Proof.** Substituting the \( \theta_{FA}^* \) in (46) into (45), and then taking the derivative of (45) regarding \( \rho \) shows that \( p_{co}^{FA} \) increases monotonically as \( \rho \) increases. Thus, according to the constraint (5b), the region of \( \rho \) for ensuring covertness is \((0, \rho_{FA}^*]\), where \( \rho_{FA}^* \) is the solution of \( p_{co}^{FA}(\rho, \theta_{FA}^*) = \epsilon_c. \)

Taking the derivative of \( p_{so}^{FA} \) in (42) regarding \( \rho \), we can see that as \( \rho \) increases, \( p_{so}^{FA} \) first increases and then decreases. Thus, the objective function in (5a) first decreases and then increases as \( \rho \) increases. Next, based on the secrecy constraint in (5c), we determine the feasible
region of $\rho$ as well as the optimal $\rho_{FA}^*$, which will be discussed under three cases as depicted in Fig. 2, Fig. 3 and Fig. 4.

In Case 1, the secrecy constraint in (5c) yields two feasible regions of $\rho$ for ensuring secrecy, i.e., $(0, \rho_S]$ and $[\rho_L, 1]$ as shown in Fig. 2 where $\rho_S$ and $\rho_L$ denote the smaller and larger solutions of $p_{FA}^{\rho_{FA}}(\rho, \theta_{FA}^*) = \epsilon_s$. The feasible region of $\rho$ (depicted by the gray region in Fig. 2) is thus the overlap between the covertness region $(0, \rho_{FA}^*)$ and the secrecy regions. Fig. 2 shows that the feasible region varies with the value of $\rho_{FA}^*$. We can observe that if $\rho_{FA}^* \leq \rho_S < \rho_L$ or
\( \rho_S < \rho_{FA}^* < \rho_L \), the optimal \( \rho \) is asymptotically approaching zero but not available. For \( \rho_S < \rho_L \leq \rho_{FA}^* \), the optimal \( \rho \) can be \( \rho_{FA}^* \) if \( \rho_{FA}^{FA}(\rho_{FA}^*) = \lim_{\rho \to 0} \rho_{FA}(\rho) = \left(1 - \frac{\sigma_w^2 + \sigma_e^2}{P_a}\right) \exp\left(\frac{\sigma_w^2 + \sigma_e^2}{P_a}\right) \).
Otherwise, the optimal \( \rho \) is not available and neither is the CSR. For the other two cases with only one solution to the equation \( \rho_{FA}^{FA}(\rho, \theta_{FA}^*) = \epsilon_s \), be it \( \rho_S \) or \( \rho_L \) (as shown in Fig. 3 and Fig. 4), the optimal \( \rho_{FA}^* \) can be found following the same approach. Thus, the discussions are omitted here. Summarizing the results of the three cases completes the proof.

\( \square \)

VI. CSR ANALYSIS: THE ENEMY RELATIONSHIP

This section focuses on the CSR analysis for the enemy relationship case. The results under the PC-based scheme and AN-based scheme are given in Subsections VI-A and VI-B, respectively.

A. PC-Based Transmission Scheme

In the enemy relationship case, Willie and Eve generate AN to reduce the attacking power of the other. Thus, under the PC-based transmission scheme, when Alice transmits, in addition to the information signals \( x \) from Alice, Bob also receives ANs \( v_w \) and \( v_e \) from both Willie and Eve, respectively. Each AN symbol \( v_w[i] \) (resp. \( v_e[i] \)) \((i = 1, 2, \cdots, n)\) is subject to the unit power constraint, i.e., \( \mathbb{E}[|v_w[i]|^2] = 1 \) (resp. \( \mathbb{E}[|v_e[i]|^2] = 1 \)). Thus, the received signal vector at Bob is given by

\[
y_b = \sqrt{P_a} h_{ab} x + \sqrt{P_w} h_{wb} v_w + \sqrt{P_e} h_{eb} v_e + n_b,
\]

(48)
where $P_w$ and $P_e$ denote the transmit powers of Willie and Eve, respectively. We assume that both Willie and Eve can eliminate the AN from itself. Thus, the received signal vectors at Willie and Eve are given by

$$y_w = \sqrt{P_a}h_{aw}x + \sqrt{P_e}h_{ew}v_e + n_w,$$  \hfill (49)  

and

$$y_e = \sqrt{P_a}h_{ae}x + \sqrt{P_w}h_{we}v_w + n_e.$$ \hfill (50)

According to (49), we can obtain the average power $\bar{P}_w$ of the received symbols $y_w$ at Willie as

$$\bar{P}_w = P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2.$$  \hfill (51)

Based on (51), the probability of missed detection $p_{MD}$ under the PC-based scheme can be given by

$$p_{MD} = \mathbb{P} \left( P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2 \leq \theta \right) = \begin{cases} 
1 + \frac{P_a}{P_e - \sigma_w^2} \exp \left( -\frac{\theta - \sigma_w^2}{P_e} \right) - \frac{P_a}{P_e - \sigma_w^2} \exp \left( \frac{-\theta - \sigma_w^2}{P_e} \right), & \theta > \sigma_w^2, \\
0, & \theta \leq \sigma_w^2.
\end{cases}$$ \hfill (52)

Based on (48) and (50), we can formulate the secrecy capacity $C_s$ as

$$C_s = \log \left( 1 + \frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2} \right) - \log \left( 1 + \frac{P_a|h_{ae}|^2}{P_w|h_{we}|^2 + \sigma_e^2} \right).$$ \hfill (53)

Thus, the SOP under the PC-based scheme can be given by

$$p_{sOP}^{EP}(P_a) = \mathbb{P} \left( \frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2} - \frac{2R_s P_a|h_{ae}|^2}{P_w|h_{we}|^2 + \sigma_e^2} < 2R_s - 1 \right)$$

$$= \int_0^{\frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2}} \frac{2R_s P_a}{P_w|h_{we}|^2} \frac{P_w|h_{we}|^2}{P_a^2 P_w |h_{ab}|^2 - (P_w(2R_s - 1) - 2R_s P_a)(P_w y + P_e z + \sigma_b^2)}$$

$$\times \exp \left[ - \left( \frac{|h_{ab}|^2 \sigma_b^2}{2R_s (P_w y + P_e z + \sigma_b^2)} + y - \frac{\sigma_e^2 (2R_s - 1)}{2R_s P_a} + z \right) \right] \, dy \, dz.$$ \hfill (54)

When Alice does not transmit, Willie receives the AN from Eve together with his background noise. Thus, the received signal vector at Willie is given by

$$y_w = \sqrt{P_e}h_{ew}v_e + n_w.$$ \hfill (55)

In this case, the average power $\bar{P}_w$ is given by

$$\bar{P}_w = P_e|h_{ew}|^2 + \sigma_w^2.$$ \hfill (56)
Based on (56), the probability of false alarm \( p_{FA} \) is given by

\[
p_{FA} = P\left(P_e|h_{ew}|^2 + \sigma_w^2 \geq \theta\right) = \begin{cases} \exp\left(-\frac{\theta - \sigma_w^2}{P_e}\right), & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2. \end{cases}
\]  
(57)

Combining the \( p_{MD} \) in (52) and the \( p_{FA} \) in (57) gives the COP \( p_{co}^{EP} \) under the PC-based scheme, which is

\[
p_{co}^{EP}(P_a, \theta) = \begin{cases} \frac{P_a}{P_a - P_e} \left[ \exp\left(-\frac{\theta - \sigma_w^2}{P_a}\right) - \exp\left(-\frac{\theta - \sigma_w^2}{P_e}\right) \right], & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases}
\]  
(58)

We can see from (58) that the optimal detection threshold \( \theta_{EP}^* \) exists when \( \theta > \sigma_w^2 \) and can be obtained by solving \( \frac{\partial p_{co}^{EP}}{\partial \theta} = 0 \). Thus, \( \theta_{EP}^* \) is given by

\[
\theta_{EP}^* = \frac{P_a P_e}{P_a - P_e} \ln \frac{P_a}{P_e} + \sigma_w^2.
\]  
(59)

By solving the optimization problem P1 with \( \theta = \theta_{EP}^* \), we obtain the CSR under the PC-based transmission scheme. The result is summarized in the following theorem.

**Theorem 5.** Under the scenario where Willie and Eve are in the enemy relationship and Alice adopts the PC-based secure transmission scheme, the CSR of the system is

\[
R_{cs}^{EP} = q R_s (1 - p_{so}^{EP}(P_{a,EP}^*)),
\]  
(60)

where \( p_{so}^{EP}(\cdot) \) is given by (54) and the optimal transmit power \( P_{a,EP}^* \) solves \( p_{co}^{EP}(P_a, \theta_{EP}^*) = \epsilon_c \) with \( \theta_{EP}^* \) given by (59). Note that the inequality \( P_{a,EP}^* \geq P_{a,EP}^{\min} \) must hold, where \( P_{a,EP}^{\min} \) solves \( p_{so}^{EP}(P_a) = \epsilon_s \). Otherwise, the CSR is not available.

**Proof.** The proof is similar to that of Theorem 1 and thus omitted here. \( \square \)

**B. AN-Based Transmission Scheme**

Under the AN-based scheme, when Alice transmits, the received signal vectors at Bob, Willie and Eve are respectively given by

\[
y_b = \sqrt{\rho P_a h_{ab}} x + \sqrt{(1 - \rho)P_a h_{ab}} z + \sqrt{P_a h_{wb}} v_w + \sqrt{P_e h_{eb}} v_e + n_b,
\]  
(61)

\[
y_w = \sqrt{\rho P_a h_{aw}} x + \sqrt{(1 - \rho)P_a h_{aw}} z + \sqrt{P_e h_{ew}} v_e + n_w,
\]  
(62)

and

\[
y_e = \sqrt{\rho P_a h_{ae}} x + \sqrt{(1 - \rho)P_a h_{ae}} z + \sqrt{P_w h_{we}} v_w + n_e.
\]  
(63)
Based on (67), we can derive the probability of false alarm \( p_{FA} \). In this case, the average power \( \bar{P}_w \) of the received symbols \( y_w \) at Willie is the same as that given in (61). Thus, the probability of missed detection \( p_{MD} \) under the AN-based scheme can be given by (52).

Based on (61) and (63), the secrecy capacity \( C_s \) can be given by

\[
C_s = \log \left( 1 + \frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a |h_{ab}|^2 + P_w |h_{wb}|^2 + P_e |h_{eb}|^2 + \sigma_b^2} \right) - \log \left( 1 + \frac{\rho P_a |h_{ae}|^2}{(1-\rho)P_a |h_{ae}|^2 + P_w |h_{we}|^2 + \sigma_e^2} \right).
\]

Thus, the SOP under the AN-based scheme can be derived as

\[
p_{SO}^{EA}(\rho) = \mathbb{P} \left( \frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a |h_{ab}|^2 + P_w |h_{wb}|^2 + P_e |h_{eb}|^2 + \sigma_b^2} < 2R_s - 1 \right)
\]

\[
= \int_0^\infty \int_0^\infty \left[ \frac{2R_s - 1}{\alpha_1(z)\gamma_1 + \gamma_1^2 y} + \frac{\gamma_1 - \delta_1}{\gamma_1} \right] \times \exp \left( -y - \frac{(2R_s - 1)P_e\sigma_e^2\gamma_2 + \alpha_2(z)\delta_2 + \beta_2\gamma_2}{\alpha_2(z)\gamma_2 + \gamma_2^2 y} + \frac{\delta_2}{\gamma_2} - z \right) \, dy \, dz,
\]

where

\[
\alpha_1(z) = 2R_s \rho P_a(P_e z + \nu) - ((1-\rho)P_a - P_w)[\rho P_a |h_{ab}|^2 - (2R_s - 1)(P_e z + \nu)],
\]

\[
\alpha_2(z) = 2R_s \rho P_a(P_e z + \nu) - (1-\rho)P_a \left[ \rho P_a |h_{ab}|^2 - (2R_s - 1)(P_e z + \nu) \right].
\]

Here, \( \beta_1 = \rho P_aP_w |h_{ab}|^2 - (2R_s - 1)((1-\rho)P_a |h_{ab}|^2 + \sigma_b^2)P_w \), \( \beta_2 = (\rho P_a |h_{ab}|^2 - (2R_s - 1)\nu)\sigma_e^2 \), \( \gamma_1 = 2R_s \rho P_aP_w + P_w(2R_s - 1)((1-\rho)P_a - P_w) \), \( \gamma_2 = 2R_s \rho P_aP_w + (2R_s - 1)(1-\rho)P_aP_w \), \( \delta_1 = (2R_s - 1)P_w^2 \), \( \delta_2 = (2R_s - 1)p_w^2 \sigma_e^2 \) and \( \nu = (1-\rho)P_a |h_{ab}|^2 + \sigma_b^2 \).

When Alice does not transmit, the received signal vector at Willie is given by

\[
y_w = \sqrt{(1-\rho)P_a} h_{aw}z + \sqrt{P_e} h_{ew}v + n_w.
\]

In this case, the average power \( \bar{P}_w \) is given by

\[
\bar{P}_w = (1-\rho)P_a |h_{aw}|^2 + P_e |h_{ew}|^2 + \sigma_w^2.
\]

Based on (67), we can derive the probability of false alarm \( p_{FA} \) as

\[
p_{FA} = \mathbb{P} \left( (1-\rho)P_a |h_{aw}|^2 + P_e |h_{ew}|^2 + \sigma_w^2 \geq \theta \right)
\]

\[
= \begin{cases} 
\frac{(1-\rho)P_a}{(1-\rho)P_a - P_e} \exp \left( -\frac{\theta - \sigma_w^2}{(1-\rho)P_e} \right) - \frac{P_e}{(1-\rho)P_a - P_e} \exp \left( -\frac{\theta - \sigma_w^2}{P_e} \right), & \theta > \sigma_w^2, \\
1, & \theta \leq \sigma_w^2.
\end{cases}
\]
Combining the $p_{MD}$ in (52) and $p_{FA}$ in (68), we obtain the COP $P_{co}^{EA}$ under the AN-based scheme as

$$P_{co}^{EA}(\rho, \theta) = \begin{cases} 
\frac{P_a}{P_a-P_e} \exp\left(-\frac{\theta-\sigma_w^2}{P_a}\right) - \frac{(1-\rho)P_a}{(1-\rho)P_a-P_e} \exp\left(-\frac{\theta-\sigma_w^2}{(1-\rho)P_a}\right) + \frac{\rho P_a P_e}{(P_a-P_e)(1-\rho)P_a-P_e} \exp\left(-\frac{\theta-\sigma_w^2}{P_e}\right), & \theta > \sigma_w^2, \\
0, & \theta \leq \sigma_w^2.
\end{cases}$$

(69)

Note that the optimal detection threshold $\theta$ is difficult to obtain from (69). Thus, we resort to an approximation, which can be given by

$$\theta_{EA}^* \approx \sigma_w^2 + \frac{(\rho - 1)P_a}{\rho} \ln(1 - \rho) + \frac{\rho P_a P_e}{P_a - P_e} \ln \frac{P_a}{P_e}.$$  

(70)

We can see from Fig. 5 that the COPs achieved at the optimal $\theta$ under different settings of $P_a$ and $P_e$ are close to those achieved at the approximated optimal $\theta$ in (70). This implies that the approximation is accurate enough, and thus we use the approximated optimal $\theta$ in (70) to solve the optimization problem P1. After solving the optimization problem P1, we obtain the CSR under the PC-based transmission scheme, which is given in the following theorem.

**Theorem 6.** Under the scenario where Willie and Eve are in the enemy relationship and Alice adopts the AN-based secure transmission scheme, the CSR of the system is

$$R_{cs}^{EA} = q R_s (1 - p_{so}^{EA}(\rho_{EA}^*)),$$

(71)

where $p_{so}^{EA}(\cdot)$ is given by (65) and the optimal power allocation parameter $\rho_{EA}^*$ solves $P_{co}^{EA}(\rho, \theta_{EA}^*) = \epsilon_c$ with $\theta_{EA}^*$ given by (70). Note that the inequality $\rho_{EA}^* \geq \rho_{EA}^{min}$ must hold, where $\rho_{EA}^{min}$ solves $p_{so}^{EA}(\rho) = \epsilon_s$. Otherwise, the CSR is not available.
Fig. 6. Impacts of target secrecy rate $R_s$ on CSR $R_{cs}$: PC-based scheme vs. AN-based scheme.

**Proof.** The proof is similar to that of Theorem 2 and is thus omitted here. \qed

**VII. Numerical Results**

In this section, we provide extensive numerical results to illustrate the CSR performances of the six representative scenarios under the novel secure communication paradigm. We also show the impacts of various system parameters (e.g., the target secrecy rate $R_s$, covertness requirement $\epsilon_c$ and secrecy requirement $\epsilon_s$) on the CSR performances. Unless otherwise stated, we set the transmission probability of Alice to $q = 0.5$, the channel gain between Alice and Bob to $|h_{ab}|^2 = 1$, the parameter $\nu$ to $\nu = 0.001$, the transmit powers of Willie and Eve to $P_w = P_e = -5$ dB and the noise powers at Bob, Willie and Eve to $\sigma_b^2 = -20$ dB and $\sigma_w^2 = \sigma_e^2 = -5$ dB.

To explore the impacts of $R_s$ on the CSR performances, we first show in Fig. 6 the CSR $R_{cs}$ vs. $R_s$ in the three relationship cases under the constraints of $\epsilon_c = 0.1$ and $\epsilon_s = 0.1$. In each subfigure of Fig. 6, we also plot the CSR curves of the PC-based transmission scheme and the AN-based transmission scheme with various values of transmit power $P_a$. We can see from Fig. 6(a) that the CSRs achieved by both transmission schemes first increase and then decrease as $R_s$ increases in the independence relationship case. This implies that there exists an optimal $R_s$ that maximizes the CSR performance achieved by each transmission scheme.

Note that the message transmit power adopted by the AN-based scheme is $\rho_{IA}^* P_a$ and that adopted by the PC-based scheme is $P_{a,IP}^*$. Thus, comparing the curves in Fig. 6(a), we can observe that the AN-based scheme achieves a smaller CSR than the PC-based scheme, when the former adopts no more message transmit power than the latter (i.e., $\rho_{IA}^* P_a < P_{a,IP}^*$) and
\( \rho_{IA}^* P_a = P_{a,IP}^* \). When the AN-based scheme adopts a slightly larger message transmit power than the PC-based scheme (i.e., \( \rho_{IA}^* P_a > P_{a,IP}^* \)), the former scheme ensures a higher CSR than the latter. However, when the AN-based scheme adopts a much larger message transmit power than the PC-based scheme (i.e., \( \rho_{IA}^* P_a \gg P_{a,IP}^* \)), the CSR achieved by the former scheme is larger than that achieved by the latter scheme only when \( R_s \) is larger than a threshold (about 0.06 in Fig. 6(a)). Thus, based on the above observations, we can conclude that, given a target secrecy rate \( R_s \), the AN-based transmission scheme can achieve no worse CSR performance than the PC-based scheme by properly adjusting the message transmit power in the independence relationship scenario.

Similar behaviors of \( R_{cs} \) vs. \( R_s \) can be observed from Fig. 6(b). This is because the signals received by Willie and Eve in the friend relationship case can be treated as scaled versions of those in the independence relationship case due to the signal sharing between Willie and Eve. The behaviors of \( R_{cs} \) vs. \( R_s \) in the enemy relationship scenario are quite different from those in the other two scenarios, as shown in Fig. 6(c). First, we can see from Fig. 6(c) that the CSR of the PC-based scheme increases as \( R_s \) increases. This is not the case for the AN-based scheme. As \( R_s \) increases, the CSR of the AN-based scheme increases for small message transmit powers, while it first increases and then decreases for large message transmit powers (\( \rho_{EA}^* P_a \gg P_{a,EP}^* \)). Second, by comparing the curves, we can observe that the PC-based scheme always achieves better CSR performance than the AN-based scheme when the former adopts no more message transmit powers than the latter. However, when the PC-based scheme adopts more message transmit power.
transmit powers than the AN-based scheme, the CSR performance of the former is better than the latter only if $R_s$ is below a threshold (about 0.114 in Fig. 6(c)). Thus, we can conclude that the PC-based scheme outperforms the AN-based scheme for small values of $R_s$, while the latter outperforms the former for large values of $R_s$ in the enemy relationship scenario.

We next explore the impacts of the relationships between Willie and Eve on the CSR performance. Fig. 7(a) and Fig. 7(b) show the CSR $R_{cs}$ vs. $R_s$ in the three relationship cases for the PC-based and AN-based transmission schemes, respectively. We set the transmit power of Alice to $P_a = -10$ (dB) in Fig. 7(b). We can observe from both figures that the CSR in the independence relationship case is always larger than or equal to that in the friend relationship case. This is intuitive since Willie and Eve can improve their attacking abilities by sharing their signals. We can also observe from both figures that the CSR in the enemy relationship case is larger (resp. smaller) than those in the other two relationship cases when $R_s$ is larger (resp. smaller) than some threshold. The above observations indicate that being friends is the best choice for the eavesdropper group and detector group when the target secrecy rate $R_s$ is large, while being enemies is the best choice when $R_s$ is small.

To show the impacts of the covertness requirement $\epsilon_c$ on the CSR performance, we plot in Fig. 8(a) CSR vs. $\epsilon_c$ under the PC-based and AN-based transmission schemes in the three relationship cases, respectively. We set the transmit power of Alice under the AN-based scheme to $P_a = -10$ (dB) and the secrecy requirement to $\epsilon_s = 0.1$. As can seen from Fig. 8(a), the CSR increases as $\epsilon_c$ increases under both schemes in all relationship cases. The reason is that a looser
covertness constraint results in a larger optimal transmit power in the PC-based scheme (resp. a larger optimal power allocation parameter in the AN-based scheme) and thus a larger CSR. This shows a clear trade-off between the CSR performance and the covertness requirement.

Another careful observation from Fig. 8(a) indicates that the AN-based scheme outperforms the PC-based scheme in the independence relationship case, while the latter outperforms the former in the enemy relationship case, which is consistent with the observations from Fig. 6(a) and Fig. 6(c). However, in the friendship scenario, the PC-based scheme achieves better CSR performance than the AN-based scheme under stringent covertness constraints. Conversely, under loose covertness constraints, the AN-based scheme achieves better CSR performance than the PC-based scheme. The reason behind these observations is that more stringent covertness constraints result in smaller optimal power allocation parameters for the AN-based scheme. As a result, less power is used for message transmissions and more power is for AN transmissions, which thus leads to a smaller CSR than that of the PC-based scheme.

Finally, we explore the impacts of the secrecy requirement $\epsilon_s$ on the CSR performance, for which we show in Fig. 8(b) the CSR vs. $\epsilon_s$ under the PC-based and AN-based transmission schemes in the three relationship cases, respectively. We set the transmit power of Alice under the AN-based scheme to $P_a = -10$ (dB) and the covertness requirement to $\epsilon_c = 0.1$. We can see from Fig. 8(b) that, as $\epsilon_s$ increases, the CSRs for both AN-based and PC-based schemes in the friend relationship case decrease, while they increase in the enemy relationship case. This is not the case for the independence relationship, where, as $\epsilon_s$ increases, the CSR under the AN-based scheme increases, while that under the PC-based scheme first increases and then decreases. We can also see from Fig. 8(b) that the AN-based scheme outperforms the PC-based scheme in the independence and friend relationship cases, while the PC-based scheme is better in the enemy relationship case, which is consistent with the findings in Fig. 6(a).

VIII. CONCLUSION

In this paper, we propose a novel secure wireless communication paradigm, where the physical layer security technology is applied to counteract both detection and eavesdropping attacks. To model the security performance of the novel paradigm, we conduct complete theoretical analyses to identify the covert secrecy rate (CSR), a novel metric proposed in this paper, under two transmission schemes (i.e., artificial noise (AN)-based and power control (PC)-based) in three detector-eavesdropper relationship cases (i.e., independence, friend and enemy). The results
in this paper showed that, in the independence and friend relationship cases, the AN-based transmission scheme can achieve better CSR performance than the PC-based scheme by properly adjusting the message transmit power. In the enemy relationship case, the AN-based transmission scheme outperforms the PC-based transmission scheme only in certain cases. Our results also showed that being friends (resp. enemies) is the best choice for the eavesdropper and detector, when the target secrecy rate is large (resp. small). In addition, looser covertness constraints result in larger CSRs for all scenarios, while this is not the case for secrecy constraints.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] D. Djenouri, L. Khelladi, and A. N. Badache, “A survey of security issues in mobile ad hoc and sensor networks,” *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, 2020.

[3] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, “Hiding information in noise: Fundamental limits of covert wireless communication,” *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, 2015.

[4] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, “Low probability of detection communication: Opportunities and challenges,” *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, 2019.

[5] D. Wang, B. Bai, W. Zhao, and Z. Han, “A survey of optimization approaches for wireless physical layer security,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[6] J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Link selection for security-QoS tradeoffs in buffer-aided relaying networks,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1347–1362, 2019.

[7] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, “Principles and overview of network steganography,” *IEEE Communications Magazine*, vol. 52, no. 5, pp. 225–229, 2014.

[8] B. A. Forouzan, *Cryptography & network security*. McGraw-Hill, Inc., 2007.

[9] M. Barni, “Steganography in digital media: Principles, algorithms, and applications (fridrich, j. 2010)[book reviews],” *IEEE Signal Processing Magazine*, vol. 28, no. 5, pp. 142–144, 2011.

[10] D. R. Stinson and M. Paterson, *Cryptography: theory and practice*. CRC Press, 2018.

[11] I. Khan, F. Belqasmi, R. Githo, N. Crespi, M. Morrow, and P. Polakos, “Wireless sensor network virtualization: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 553–576, 2015.

[12] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[13] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[14] Y. Liang, H. V. Poor, S. Shamai et al., “Information theoretic security,” *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[15] 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, 2014.

[16] B. A. Bash, D. Goeckel, and D. Towsley, “Limits of reliable communication with low probability of detection on AWGN channels,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013.
[17] Z. Liu, J. Liu, Y. Zeng, Z. Ma, J. Ma, and Q. Huang, “Challenges in covert wireless communications with active warden on AWGN channels,” arXiv preprint arXiv:1901.03185, 2019.

[18] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, “Reliable, deniable and hidable communication,” in Information Theory and Applications Workshop (ITA), 2014. IEEE, 2014, pp. 1–10.

[19] M. Bloch, “A channel resolvability perspective on stealth communications,” in 2015 IEEE International Symposium on Information Theory (ISIT). IEEE, 2015, pp. 2535–2539.

[20] L. Wang, G. W. Wornell, and L. Zheng, “Fundamental limits of communication with low probability of detection,” IEEE Transactions on Information Theory, vol. 62, no. 6, pp. 3493–3503, 2016.

[21] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, “Covert communication achieved by a greedy relay in wireless networks,” IEEE Transactions on Wireless Communications, vol. 17, no. 7, pp. 4766–4779, 2018.

[22] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, “Achieving covert wireless communications using a full-duplex receiver,” IEEE Transactions on Wireless Communications, vol. 17, no. 12, pp. 8517–8530, 2018.

[23] B. A. Bash, D. Goeckel, and D. Towsley, “Covert communication gains from adversary’s ignorance of transmission time,” IEEE Transactions on Wireless Communications, vol. 15, no. 12, pp. 8394–8405, 2016.

[24] D. Goeckel, B. Bash, S. Guha, and D. Towsley, “Covert communications when the warden does not know the background noise power,” IEEE Communications Letters, vol. 20, no. 2, pp. 236–239, 2016.

[25] B. He, S. Yan, X. Zhou, and V. K. Lau, “On covert communication with noise uncertainty,” IEEE Communications Letters, vol. 21, no. 4, pp. 941–944, 2017.

[26] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Li, “Covert wireless communications with channel inversion power control in rayleigh fading,” IEEE Transactions on Vehicular Technology, vol. 68, no. 12, pp. 12135–12149, 2019.

[27] K. S. K. Arumugam and M. R. Bloch, “Covert communication over a $k$-user multiple-access channel,” IEEE Transactions on Information Theory, vol. 65, no. 11, pp. 7020–7044, 2019.

[28] V. Y. Tan and S.-H. Lee, “Time-division is optimal for covert communication over some broadcast channels,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1377–1389, 2019.

[29] K. S. K. Arumugam and M. R. Bloch, “Embedding covert information in broadcast communications,” IEEE Transactions on Information Forensics and Security, 2019.

[30] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, “Covert communication with the help of relay and channel uncertainty,” IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 317–320, 2018.

[31] H. Wu, Y. Zhang, X. Liao, Y. Shen, and X. Jiang, “On covert throughput performance of two-way relay covert wireless communications,” Wireless Networks, pp. 1–15, 2020.

[32] A. Sheikholeslami, M. Ghaderi, D. Towsley, B. A. Bash, S. Guha, and D. Goeckel, “Multi-hop routing in covert wireless networks,” IEEE Transactions on Wireless Communications, 2018.

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

[34] S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456, 1978.
[38] A. Carleial and M. Hellman, “A note on Wyner's wiretap channel (corresp.),” *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 387–390, 1977.

[39] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II,” *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[40] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[41] H. Xing, L. Liu, and R. Zhang, “Secrecy wireless information and power transfer in fading wiretap channel,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180–190, 2015.

[42] S. Allipuram, P. Mohapatra, and S. Chakrabarti, “Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper,” *IEEE Communications Letters*, 2020.

[43] I. Bang, S. M. Kim, and D. K. Sung, “Artificial noise-aided user scheduling from the perspective of secrecy outage probability,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7816–7820, 2018.

[44] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y.-D. Yao, “Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks,” *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3482–3495, 2019.

[45] X. Li, Y. Zhang, S. Zhao, Y. Shen, and X. Jiang, “Exact secrecy throughput capacity study in mobile ad hoc networks,” *Ad Hoc Networks*, vol. 72, pp. 105–114, 2018.

[46] Y. Zhang, Y. Shen, and X. Jiang, “Friendship-based cooperative jamming for secure communication in poisson networks,” *Wireless Networks*, vol. 25, no. 7, pp. 4077–4095, 2019.

[47] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, “Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective,” *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2018.

[48] P. Zhang, Y. Shen, X. Jiang, and B. Wu, “Physical layer authentication jointly utilizing channel and phase noise in MIMO systems,” *IEEE Transactions on Communications*, 2020.

[49] Y. Zou, T. Wu, M. Sun, J. Zhu, M. Qian, and C. Liu, “Secrecy outage analysis of non-orthogonal spectrum sharing for heterogeneous cellular networks,” *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6626–6640, 2019.

[50] H. Ma, J. Cheng, and X. Wang, “Proportional fair secrecy beamforming for MISO heterogeneous cellular networks with wireless information and power transfer,” *IEEE Transactions on Communications*, vol. 67, no. 8, pp. 5659–5673, 2019.

[51] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, “On secure wireless communications for IoT under eavesdropper collusion,” *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, 2015.

[52] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, “Converting communication in the presence of an uninformed jammer,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.

[53] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[54] A. Browder, *Mathematical analysis: an introduction*. Springer Science & Business Media, 2012.

[55] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, “Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, 2013.