Achieving Covertness and Secrecy: The Interplay between Detection and Eavesdropping Attacks

Huihui Wu, *Member, IEEE*, Yuanyu Zhang, *Member, IEEE*, Yulong Shen, *Member, IEEE*, Xiaohong Jiang, *Senior Member, IEEE* and Tarik Taleb, *Senior Member, IEEE*

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

***Index Terms*—Internet of Things, wireless communication, covertness, secrecy, physical layer security.**

I. Introduction

THE fundamental research of wireless communication security is of great importance for sensitive and confidential data collection in the Internet of Things (IoT) [1], [2]. It is notable that in modern secure wireless communication of the IoT, covertness and secrecy serve as two typical properties [3], [4]. Covertness concerns with the protection of wireless communication from detection attacks that attempt to detect the existence of the communication [5], [6], while secrecy deals with the protection of wireless communication from eavesdropping attacks [7], [8] which manage to intercept the information conveyed by the communication. With the wide application of the IoT (e.g., e-health, intelligent transportation systems and wearable devices), how to ensure the covertness and secrecy of wireless communication in the data collection process has become an increasingly urgent demand.

Thanks to the rapid progress of information and communication technologies, physical layer security (PLS) technique is now regarded as a highly promising approach to counteract the detection and eavesdropping attacks and thus to ensure the covertness and secrecy properties of wireless IoT data collection. The basic principle behind the PLS technology is to exploit the inherent physical layer randomness of wireless channels (e.g., noise and fading) to implement the secure and covert communications [9]. 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. In addition, the PLS technology serves as an effective supplement for the traditional security technologies (e.g., cryptography and spread spectrum) to significantly improve the covertness and secrecy of wireless data collection in the resource-limited wireless networks, such as sensor networks and IoT networks [6], [10].

By now, extensive research efforts have been devoted to the study of covertness or secrecy guarantee for wireless communication based on the PLS technology. In [11]–[16], the AN technique or cooperative jamming technique was adopted for covert wireless communication in the typical three-node scenario with a transmitter, a receiver and a malicious detector. In these works, the AN may be initiated by the transmitter [11], [12], by the (full-duplex) receiver [13], [14], or by some external helper nodes [15], [16] to avoid the communication signal from being detected by the detector. The works in [12], [17]–[19] show that the covert wireless communication can be implemented by exploiting the detector's uncertainty about its channel state information, like the statistical characteristics of the fading channel [12], background noise [17], [18] or available blocklength for transmission [19]. Such uncertainty makes it difficult for the detector to determine the received signal power or the background noise power, and thus unable to distinguish between the scenarios with or without wireless communication by examining the power difference in these scenarios. Some recent works also explored the possibility of ensuring covertness based on other PLS technologies, such as multi-antenna technique [20], [21], coding scheme [22], [23], relay selection [24], [25] and resource (i.e., channel use) allocation [26].

The PLS technology has also been widely adopted for achieving secrecy in various wireless communication scenarios, such as ad-hoc networks [27], [28], device-to-device (D2D) communications [29], [30], cellular networks [31], [32] and the Internet of Things (IoT) [4], [33]. These works mainly exploited the application of AN technique to create a relatively better channel to the receiver than that to the eavesdropper with the aim of achieving a positive secrecy rate. In [34], [35],

Huihui Wu is with Beijing National Research Center for Information Science and Technology (BNRist), Department of Automation, Tsinghua University, Beijing 100084, China (email: hhwu1994@mail.tsinghua.edu.cn).

Y. Zhang and Y. Shen are with the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China (emails: yy90zhang@ieee.org, ylshen@mail.xidian.edu.cn).

X. Jiang is with the School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido, Japan (email: jiang@fun.ac.jp).

T. Taleb is with the Information Technology and Electrical Engineering, University of Oulu, Oulu 90570, Finland, and also with the Department of Computer and Information Security, Sejong University, Seoul 05006, South Korea (email: tarik.taleb@oulu.fi).

the beamforming technique was explored for secure wireless communication in multi-antenna scenarios, where the transmit power of signals was concentrated toward the direction of intended receiver such that a much better signal quality at the receiver can be created than that at the eavesdropper. The work in [36] further combined the beamforming and AN techniques to achieve a significant signal advantage at the receiver, while the works in [37], [38] considered the multi-user scenarios and applied relay selection technique to create a transmitter-receiver channel advantage over the transmitter-eavesdropper channel. Some other works in [39]–[41] also studied the secure wireless communication based on the technique of resource allocation (e.g., power allocation, time slot allocation, energy allocation).

The above works help us understand the great potentials of the PLS technology in ensuring the covertness or secrecy of wireless communication. In addition, Artificial Intelligence (AI)/Machine Learning (ML)-based technique has emerged as a promising solution, which can be exploited for the aided design of PLS technology (e.g., antenna selection, relay nodes selection, beamforming and resource allocation) and the acquisition of channel state information (CSI), and thus benefits covertness or secrecy guarantees of wireless communications [42]–[44]. It is notable that these works mainly focus on the traditional secure wireless communication where only one type of attack may exist, be it detection or eavesdropping, and concern with either the covertness guarantee or secrecy guarantee for wireless communications. In practice, however, both detection and eavesdropping attacks may coexist during the data collection process of the IoT, especially in some critical communication scenarios consisting of multiple groups with common or conflicting interests, like wireless body area networks (WBANs) [45]–[48]. The WBANs are networks of intelligent and low-power sensor devices positioned on or around the human body to collect biomedical data and then transmit the privacy information to medical servers via open wireless networks. Due to the inadequate computing resources, the devices in WBANs prefer to adopt PLS technology to address the covertness or secrecy issues during data transmission process. Therefore, in this paper we are motivated to explore the joint guarantees of covertness and secrecy for wireless communications in the IoT where the PLS technology is applied to counteract both the detection and eavesdropping attacks.

Recently, Forouzesh *et al.* have made some initial attempts to provide both covertness and secrecy guarantees for wireless communications. They first considered a three-node model with a transmitter, a receiver and an attacker, where an AN-aided security scheme has been adopted to ensure covertness or secrecy respectively in wireless communication scenarios [49]. They also make a comparison between the performance metrics (i.e., covertness rate and secrecy rate) in each scenario, and propose a guideline for employing covert/secrecy wireless communication under different parameters (e.g., the noise around the attacker and the distance from the transmitter to the attacker). Moreover, Wang *et al.* also studied the covertness or secrecy guarantees in a multi-hop network respectively, where a pair of source and destination nodes with a long distance under the transmission detection or signal eavesdropping attacks by an unmanned aerial vehicle (UAV) [50]. In order to counteract the attacks, they employed a multi-hop relaying strategy to assist the secure transmissions, and maximized the throughput by optimizing the network parameters under the covertness and secrecy constraints, respectively. After discussing the differences between covertness guarantee and secrecy guarantee in wireless communications, Forouzesh *et al.* investigated both covertness and secrecy guarantees in wireless communications in [51], [52]. They considered a two-hop transmission system with an *untrusted* relay and a detector [51]. To achieve covertness and secrecy, they adopted an AN-aided security scheme, where the non-transmitting node (i.e., the receiver in the first hop or the transmitter in the second hop) radiates AN to resist against both the eavesdropping of the untrusted relay and the detection of the detector. They also explored the optimal secrecy rate in the system under the covertness constraints in two hops. In their next work, they focused on a single-input multi-output (SIMO) system [52], where a transmitter concurrently sends different signals to two receivers, one of which suffers from the detection attack while the other suffers from the eavesdropping attack. Through a proper transmission power allocation in this system, the signal of one transmission can act as the AN for the other transmission to counteract the detection or eavesdropping attack. They further investigated the sum rate optimization issue of the SIMO system under the covertness and secrecy constraints.

The above works represent a significant research progress in the joint guarantees of covertness and secrecy for wireless communications, and help us to have a basic understanding on the coexistence of detection and eavesdropping attacks. Towards this end, there is a strong requirement to jointly consider covertness and secrecy in wireless communication systems, which will find extensive usage in numerous IoT scenarios such as WBANs. Compared to the above works, the main novelty of this work is that this work represents the first attempt to explore a general secure wireless communication model where the communication process is subjected to the simultaneous detection and eavesdropping attacks. In particular, to explore the fundamental interplay between these attacks, we study both the covertness and secrecy guarantees in this model under two attack relationships of independent relationship and friend relationship, as well as two classical secure transmission schemes in [53] which are AN-based one with friendly jamming and power control (PC)-based one with power constraint. This new secure wireless communication model also brings some technical challenges. First, to understand the fundamental security performance under the new secure wireless communication model, a new performance metric is needed to define the overall system transmission rate performance with the considerations of both covertness and secrecy guarantees. Second, a new theoretical framework needs to be developed to depict the joint covertness, secrecy and transmission performances in such secure communication system. Third, a deep analysis is needed to reveal both the performance optimization and possible performance degradation arouse from the interplay between detection and eavesdropping

attacks. The main contributions of this paper are summarized as follows.

- ***A new secure wireless communication scenario*:** In this new scenario, the PLS technology is applied to counteract both the detection from a detector and the eavesdropping from an eavesdroppers, where the detector and eavesdropper can be friends, sharing their signals received from the target transmitter with the aim of enhancing the attack performance of both sides, and can also be independent, conducting their own attack individually without sharing signals. This is motivated by the fact that the detectors and eavesdroppers may have common interests as the members in the same alliance or have unrelated goals in different organizations. In addition, both PC-based and AN-based security schemes are adopted to enhance the covertness and secrecy performances in the scenario.
- ***Theoretical modeling for the new scenario*:** To depict the covertness, secrecy and transmission performances of the new scenario, for each concerned communication scenario (i.e., friend-PC, friend-AN, independence-PC, independence-AN) we provide the corresponding theoretical modeling of covertness outage probability (COP) (i.e., the probability that detectors detect the transmitted signals), the secrecy outage probability (SOP) (i.e., the probability that eavesdroppers recover the conveyed information) and the transmission probability (TP) (i.e., the probability of conducting transmissions), respectively.
- ***A novel security metric characterizing the covertness, secrecy and transmission performances*:** This paper defines a novel security metric-*covert secrecy rate* (CSR), which characterizes the maximum transmission rate subject to the constraints of COP, SOP and TP, and thus can serve as the fundamental security criterion for this new communication scenario. We further conduct detailed theoretical analysis to identify the CSR for each of the four communication scenarios. Finally, extensive numerical results are provided to illustrate the CSR performances under the new secure communication scenario.

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

II. System Model and Security Metric

To demonstrate the new secure wireless communication scenario, we consider a system for collecting data in the IoT (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 detect 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. Alice is assumed to be equipped with one omnidirectional antenna in PC-based scheme and two in AN-based scheme, while Bob, Eve and Willie are assumed to be equipped with a single omnidirectional antenna in each scheme. 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 the same 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 [54], the corresponding channel gain $|h_{ij}|^2$ follows the exponential distribution with unit mean. We assume that Alice and Bob know the *instantaneous* channel coefficient and *statistical* characteristics of Alice-Bob channel but only *statistical* characteristics of other channels including those to Eve and Willie. We also assume that Eve knows the *instantaneous* channel coefficient h_{ae}, while Willie knows only the *statistical* characteristics of h_{aw} and h_{ew}. These assumptions are widely used in previous research related to PLS and covert communication.

A. Secure Transmission Schemes

Alice employs two transmission schemes based on power control (PC) and artificial noise (AN), 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. More specifically, AN can be regarded as a partial cover for message signals, which can be utilized to increase the uncertainty of the background noise, and thus is widely used to enhance the covertness/secrecy performance [36], [55], [56]. 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 strategies of transmit power, Alice also adopts the Wyner encoding scheme [57] 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 for the whole transmitted symbol. The difference $R_t - R_s$ represents the rate sacrificed to confuse Eve.

The goal of Alice is to ensure a positive and *constant* secrecy rate R_s. Thus, Alice will send messages to Bob only when the instantaneous capacity C_b of the Alice-Bob channel can support the secrecy rate R_s (i.e., $C_b \geq R_s$). In this situation, Alice will set R_t arbitrarily close to C_b to cause as much confusion to Eve as possible, while ensuring reliable message transmission to Bob. Thus, the probability of Alice transmitting messages in a certain time slot can be defined as

$$p_{tx} = \mathbb{P}(C_b \geq R_s). \tag{1}$$

Note that the ***transmission probability*** **(TP)** p_{tx} can be interpreted as a metric to measure the transmission performance.

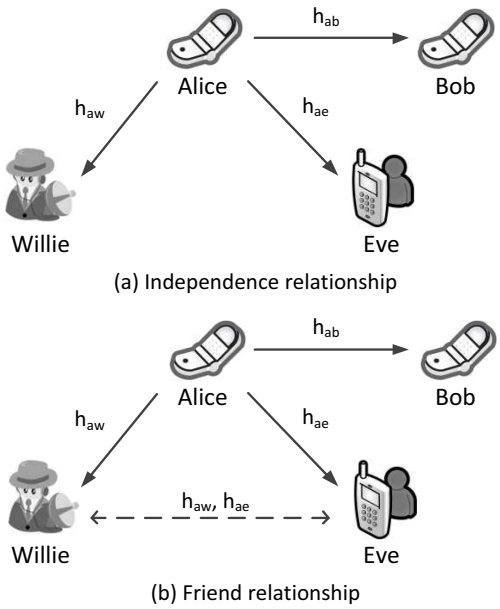


Fig. 1. Two relationships between Willie and Eve.

B. Attacking Model

In practice, Willie and Eve can belong to different organizations with unrelated or common goals, resulting in various relationships between them. In this paper, we consider two representative relationships, i.e., *independence* and *friend*. 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.

To detect the existence of signals transmitted from Alice in each slot, Willie adopts the commonly-used likelihood ratio test [58], in which he first determines a threshold θ 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

$$\bar{P}_w \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta. \tag{2}$$

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 nor 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

$$p_{co} = 1 - (p_{FA} + p_{MD}). \tag{3}$$

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 (i.e., the instantaneous secrecy capacity C_s [59] of the Alice-Bob channel falls below the target secrecy rate R_s), the transmission from Alice to Bob is said to suffer from secrecy outage. Note that secrecy outage occurs only when Alice actually transmits a message (i.e., $C_b \geq R_s$). Thus, we can define the ***secrecy outage probability*** **(SOP)** as the following conditional probability:

$$p_{so} = \mathbb{P}(C_s < R_s \mid C_b \geq R_s). \tag{4}$$

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 scenario, we propose a novel metric, called ***covert secrecy rate*** **(CSR)**, by jointly considering the covertness, secrecy and transmission performances. The CSR is defined as the maximum transmission rate under which the constraints of COP, SOP and TP 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

$$\textbf{P1 (PC-based):} \quad R_{cs} = \max_{P_a, R_s} \; R_s p_{tx}(P_a, R_s), \tag{5a}$$
$$\text{s.t.} \quad p_{co}(P_a) \leq \epsilon_c, \tag{5b}$$
$$p_{so}(R_s) \leq \epsilon_s, \tag{5c}$$
$$p_{tx}(P_a, R_s) \geq 1 - \epsilon_t, \tag{5d}$$

and

$$\textbf{P2 (AN-based):} \quad R_{cs} = \max_{\rho \in [0,1], R_s} R_s p_{tx}(\rho, R_s), \tag{6a}$$
$$\text{s.t.} \quad p_{co}(\rho) \leq \epsilon_c, \tag{6b}$$
$$p_{so}(\rho, R_s) \leq \epsilon_s, \tag{6c}$$
$$p_{tx}(\rho, R_s) \geq 1 - \epsilon_t, \tag{6d}$$

where R_{cs} denotes the CSR, ϵ_c, ϵ_s and ϵ_t denote the constraints of COP, SOP and TP. Note that Problem P1 optimizes the transmission rate over the transmit power P_a and the secrecy rate R_s, while Problem P2 conducts the optimization over the power allocation parameter ρ and the secrecy rate R_s.

Remark 1. *We can see from* (5) *and* (6) *that CSR is subjected to the constraints of COP and SOP, so it is related to both COP and SOP metrics. Since COP and SOP define respectively the covertness and secrecy performances, then CSR here represents the quality of both concealment and confidentiality.*

III. CSR Analysis: 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 III-A and III-B, respectively.

A. PC-Based Transmission Scheme

As mentioned in Section II-A, Alice decides to transmit in a certain time slot only when the instantaneous capacity C_b of Alice-Bob channel can support the secrecy rate R_s. To do this, Alice measures the instantaneous channel coefficient $|h_{ab}|^2$ and determines the Alice-Bob channel capacity C_b based on the well-known Shannon Capacity formula [60], i.e.,

$$C_b = \log\left(1 + \frac{P_a|h_{ab}|^2}{\sigma_b^2}\right), \tag{7}$$

where log is to the base of 2. Since $|h_{ab}|^2$ is exponentially distributed, the transmission probability p_{tx} of Alice under the PC-based transmission scheme is

$$p_{tx}^{\mathrm{IP}}(P_a,R_s) = \mathbb{P}(C_b \geq R_s) = \exp\left(-\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right). \tag{8}$$

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

$$\mathbf{y}_\kappa = \sqrt{P_a} h_{a\kappa}\mathbf{x} + \mathbf{n}_\kappa, \tag{9}$$

where the subscript $\kappa \in \{b, w, e\}$ stands for Bob, Willie or Eve, a represents Alice, and $\mathbf{n}_\kappa$ denotes the noise at κ with the i-th element $\mathbf{n}_\kappa[i]$ being the complex additive Gaussian noise with zero mean and variance σ_κ^2, i.e., $\mathbf{n}_\kappa[i] \sim \mathcal{CN}(0, \sigma_\kappa^2)$.

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

$$\begin{aligned}\bar{P}_w &= \frac{\sum_{i=1}^{n}|\mathbf{y}_w[i]|^2}{n} = \lim_{n\to\infty}(P_a|h_{aw}|^2 + \sigma_w^2)\chi_{2n}^2/n \\ &= P_a|h_{aw}|^2 + \sigma_w^2,\end{aligned} \tag{10}$$

where χ_{2n}^2 is a chi-squared random variable with $2n$ degrees of freedom. By the Strong Law of Large Numbers [61], $\frac{\chi_{2n}^2}{n}$ converges in probability to 1 as n tends to infinity. If $\bar{P}_w \leq \theta$, Willie accepts the hypothesis $\mathcal{H}_0$ that Alice did not transmit messages, leading to a missed detection. Thus, the probability of missed detection p_{MD} is given by

$$\begin{aligned}p_{MD} &= \mathbb{P}\left(P_a|h_{aw}|^2 + \sigma_w^2 \leq \theta\right) \\ &= \begin{cases}1 - \exp\left(-\frac{\theta-\sigma_w^2}{P_a}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2.\end{cases}\end{aligned} \tag{11}$$

The eavesdropping result of Eve depends on the instantaneous secrecy capacity C_s of the Alice-Bob channel, which is non-negative and can be defined as the difference between the channel capacity of the Alice-Bob channel and that of the Alice-Eve channel [59]. Thus, C_s is formulated as

$$C_s = \log\left(1 + \frac{P_a|h_{ab}|^2}{\sigma_b^2}\right) - \log\left(1 + \frac{P_a|h_{ae}|^2}{\sigma_e^2}\right). \tag{12}$$

Note that $|h_{ab}|^2$ and $|h_{ae}|^2$ are random variables here. Based on the definition of the SOP in Subsection II-B, the SOP under the PC-based scheme can be given by

$$\begin{aligned}p_{so}^{\mathrm{IP}}(R_s) &= \frac{\mathbb{P}\left(R_s < C_b < C_e + R_s\right)}{\mathbb{P}\left(C_b > R_s\right)} = 1 - \frac{\mathbb{P}\left(C_s > R_s\right)}{\mathbb{P}\left(C_b > R_s\right)} \\ &= 1 - e^{\frac{(2^{R_s}-1)\sigma_b^2}{P_a}}\mathbb{P}\left(\frac{P_a|h_{ab}|^2}{\sigma_b^2} - \frac{2^{R_s}P_a|h_{ae}|^2}{\sigma_e^2} > 2^{R_s} - 1\right) \\ &= \frac{2^{R_s}\sigma_b^2}{2^{R_s}\sigma_b^2 + \sigma_e^2}.\end{aligned} \tag{13}$$

When Alice does not transmit, security performance is not a concern and thus we only focus on the covertness performance. In this case, Willie receives only noise, i.e., $\mathbf{y}_w = \mathbf{n}_w$ and thus the the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_w$ is $\bar{P}_w = \sigma_w^2$. If $\bar{P}_w \geq \theta$, Willie accepts the hypothesis $\mathcal{H}_1$ that Alice transmitted messages, leading to a false alarm. Thus, the probability of false alarm p_{FA} is given by

$$p_{FA} = \mathbb{P}\left(\sigma_w^2 \geq \theta\right) = \begin{cases}0, & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2.\end{cases} \tag{14}$$

Combining the p_{MD} in (11) and the p_{FA} in (14), we obtain the COP under the PC-based scheme as

$$p_{co}^{\mathrm{IP}}(P_a, \theta) = \begin{cases}\exp\left(-\frac{\theta-\sigma_w^2}{P_a}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2.\end{cases} \tag{15}$$

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 θ, denoted by θ_{IP}^*. We can see from (15) that p_{co}^{IP} is a decreasing function of θ and is larger than or equal to 0 for $\theta > \sigma_w^2$. Thus, the optimal θ_{IP}^* exists in (σ_w^2, ∞) and is thus given by $\theta_{\mathrm{IP}}^* = \upsilon + \sigma_w^2$, where $\upsilon > 0$ is an arbitrarily small value.

Under the condition that Willie chooses the optimal detection threshold θ_{IP}^*, Alice solves the optimization problem in (5) 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 can be given by* (16)*, where*

$$R_{s,\mathrm{IP}}^{SOP} = \log\left(\frac{\sigma_e^2\epsilon_s}{(1-\epsilon_s)\sigma_b^2}\right), \tag{17}$$

$$R_{s,\mathrm{IP}}^{TP} = \log\left(1 - \frac{P_{a,\mathrm{IP}}^*\ln(1-\epsilon_t)}{\sigma_b^2}\right), \tag{18}$$

$$R_{s,\mathrm{IP}}^{0} = \frac{1}{\ln 2}\mathrm{W}_0\left(\frac{P_{a,\mathrm{IP}}^*}{\sigma_b^2}\right), \tag{19}$$

$\mathrm{W}_0(\cdot)$ *is the principal branch of Lambert's W function, and* $P_{a,\mathrm{IP}}^* = -\frac{\upsilon}{\ln\epsilon_c}$ *is the optimal transmit power.*

Proof: As can be seen from (5a), the optimal transmit power P_a and optimal target secrecy rate R_s are required to solve the optimization problem P1. We first derive the optimal P_a. It is easy to see from (8) and (15) that both p_{tx}^{IP} and p_{co}^{IP}

$$R_{cs}^{\mathrm{IP}}=\begin{cases}\frac{1}{\ln 2}\mathrm{W}_0\left(-\frac{\upsilon}{\sigma_b^2\ln\epsilon_c}\right)\exp\left(-\frac{1}{\mathrm{W}_0\left(-\frac{\upsilon}{\sigma_b^2\ln\epsilon_c}\right)}-\frac{\sigma_b^2\ln\epsilon_c}{\upsilon}\right), & R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{0}\le\min\left\{R_{s,\mathrm{IP}}^{\mathrm{SOP}},R_{s,\mathrm{IP}}^{\mathrm{TP}}\right\},\\ \log\left(\frac{\sigma_e^2\epsilon_s}{(1-\epsilon_s)\sigma_b^2}\right)\exp\left(\frac{\left(\sigma_e^2\epsilon_s-(1-\epsilon_s)\sigma_b^2\right)\ln\epsilon_c}{(1-\epsilon_s)\upsilon}\right), & R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{\mathrm{SOP}}\le\min\left\{R_{s,\mathrm{IP}}^{0},R_{s,\mathrm{IP}}^{\mathrm{TP}}\right\},\\ (1-\epsilon_t)\log\left(1+\frac{\upsilon\ln(1-\epsilon_t)}{\sigma_b^2\ln\epsilon_c}\right), & R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{\mathrm{TP}}\le\min\left\{R_{s,\mathrm{IP}}^{0},R_{s,\mathrm{IP}}^{\mathrm{SOP}}\right\},\end{cases}\tag{16}$$

monotonically increase as P_a increases. Thus, the covertness constraint in (5b) results in an upper bound on P_a, which is

$$P_{a,\mathrm{IP}}^{\max}=-\frac{\upsilon}{\ln\epsilon_c},\tag{20}$$

and the TP constraint in (5d) leads to a lower bound on P_a, which is

$$P_{a,\mathrm{IP}}^{\min}=-\frac{(2^{R_s}-1)\sigma_b^2}{\ln(1-\epsilon_t)}.\tag{21}$$

Note that the inequality $P_{a,\mathrm{IP}}^{\min}\le P_{a,\mathrm{IP}}^{\max}$ must hold, which gives the following condition on R_s:

$$R_s\le\log\left(1+\frac{\upsilon\ln(1-\epsilon_t)}{\sigma_b^2\ln\epsilon_c}\right).\tag{22}$$

Since the objective function in (5a) is an increasing function of P_a, the optimal P_a is the upper bound, i.e., $P_{a,\mathrm{IP}}^{*}=P_{a,\mathrm{IP}}^{\max}$.

Next, we derive the optimal R_s by analyzing the feasible region of R_s and the monotonicity of the objective function with respect to R_s. We can see that as R_s increases, p_{tx}^{IP} in (8) monotonically decreases while p_{so}^{IP} in (13) monotonically increases. Thus, based on the constraints (5c) and (5d), the regions of R_s for ensuring secrecy and transmission performances are $[0,R_{s,\mathrm{IP}}^{\mathrm{SOP}}]$ and $[0,R_{s,\mathrm{IP}}^{\mathrm{TP}}]$ with $R_{s,\mathrm{IP}}^{\mathrm{SOP}}$ and $R_{s,\mathrm{IP}}^{\mathrm{TP}}$ given by (17) and (18), respectively. Note that $R_{s,\mathrm{IP}}^{\mathrm{TP}}$ is obtained at $P_a=P_{a,\mathrm{IP}}^{*}=-\frac{\upsilon}{\ln\epsilon_c}$ and thus the region $[0,R_{s,\mathrm{IP}}^{\mathrm{TP}}]$ is equivalent to (22). Hence, the feasible region of R_s is $[0,\min\{R_{s,\mathrm{IP}}^{\mathrm{SOP}},R_{s,\mathrm{IP}}^{\mathrm{TP}}\}]$. Taking the first derivative of the objective function in (5a) in terms of R_s gives

$$\frac{\partial R_{cs}}{\partial R_s}=\left(1-\frac{R_s2^{R_s}\sigma_b^2\ln 2}{P_a}\right)\exp\left(-\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right).\tag{23}$$

Solving $\frac{\partial R_{cs}}{\partial R_s}=0$, we can obtain the stationary point $R_{s,\mathrm{IP}}^{0}$ in (19). We can see that the objective function is increasing over $[0,R_{s,\mathrm{IP}}^{0})$ and decreasing over $[R_{s,\mathrm{IP}}^{0},\infty)$. This implies that if $R_{s,\mathrm{IP}}^{0}$ falls inside the feasible region of R_s, i.e., $R_{s,\mathrm{IP}}^{0}\le\min\{R_{s,\mathrm{IP}}^{\mathrm{SOP}},R_{s,\mathrm{IP}}^{\mathrm{TP}}\}$, the optimal R_s is $R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{0}$. Otherwise, the optimal R_s is $R_{s,\mathrm{IP}}^{*}=\min\{R_{s,\mathrm{IP}}^{\mathrm{SOP}},R_{s,\mathrm{IP}}^{\mathrm{TP}}\}$. Finally, substituting the optimal P_a and R_s into the objective function in (5a) completes the proof. ∎

B. AN-Based Transmission Scheme

Suppose Alice transmits, in addition to the message symbols, she will also inject AN, represented by a complex vector $\mathbf{z}$, where each symbol $\mathbf{z}[i]$ $(i=1,2,\cdots,n)$ is subject to the unit power constraint, i.e., $\mathbb{E}[|\mathbf{z}[i]|^2]=1$. Alice will use a fraction ρ of her transmit power P_a for message transmission and the remaining power for AN radiation. Thus, the signal vectors received at Bob will be given by

$$\mathbf{y}_b=\sqrt{\rho P_a}h_{ab}\mathbf{x}+\sqrt{(1-\rho)P_a}h_{ab}\mathbf{z}+\mathbf{n}_b.\tag{24}$$

Based on (24), Alice measures the instantaneous Alice-Bob channel capacity C_b as

$$C_b=\log\left(1+\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}\right),\tag{25}$$

and decides to transmit when $C_b\ge R_s$. Thus, the transmission probability under the AN-based scheme can be given by

$$\begin{aligned}p_{tx}^{\mathrm{IA}}(\rho,R_s)&=\mathbb{P}\left(C_b\ge R_s\right)\\&=\mathbb{P}\left(\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}\ge 2^{R_s}-1\right)\\&=\exp\left(-\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a-(2^{R_s}-1)(1-\rho)P_a}\right).\end{aligned}\tag{26}$$

Next, we analyze the secrecy and covertness performances when Alice transmits messages. In this situation, the signal vectors received at Willie and Eve have the same form of that received at Bob, which are given by

$$\mathbf{y}_\kappa=\sqrt{\rho P_a}h_{a\kappa}\mathbf{x}+\sqrt{(1-\rho)P_a}h_{a\kappa}\mathbf{z}+\mathbf{n}_\kappa,\tag{27}$$

where the subscript $\kappa\in\{w,e\}$ stands for Willie or Eve. From (27), we can see that the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_\kappa$ at Willie is the same as that given in (10). Thus, the probability of missed detection p_{MD} under the AN-based scheme can also be given by (11).

According to (27), the secrecy capacity C_s under the AN-based scheme can be formulated as

$$C_s=\log\left(1+\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}\right)-\log\left(1+\frac{\rho P_a|h_{ae}|^2}{(1-\rho)P_a|h_{ae}|^2+\sigma_e^2}\right).\tag{28}$$

Thus, following the definition of SOP in (4), we derive the SOP under the AN-based scheme as

$$\begin{aligned}p_{so}^{\mathrm{IA}}(\rho,R_s)=&1-\exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a-(2^{R_s}-1)(1-\rho)P_a}\right)\\&\times\mathbb{P}\left(\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}-\frac{2^{R_s}\rho P_a|h_{ae}|^2}{(1-\rho)P_a|h_{ae}|^2+\sigma_e^2}>2^{R_s}-1\right)\\=&1-\exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a-(2^{R_s}-1)(1-\rho)P_a}-\frac{(2^{R_s}+\rho-1)\sigma_b^2}{(1-2^{R_s})(1-\rho)P_a}\right)\\&\int_0^{\phi}\exp\left(\frac{\frac{(2^{R_s}+\rho-1)(1-(1-\rho)2^{R_s})\sigma_b^2\sigma_e^2}{(1-2^{R_s})(1-\rho)}-(2^{R_s}-1)\sigma_b^2\sigma_e^2}{(1-2^{R_s})(1-\rho)P_a^2y+(1-(1-\rho)2^{R_s})P_a\sigma_e^2}-y\right)\mathrm{d}y,\end{aligned}\tag{29}$$

where $\phi=\frac{(1-2^{R_s}(1-\rho))\sigma_e^2}{(2^{R_s}-1)(1-\rho)P_a}$.

Finally, we analyze the covertness performance when Alice does not transmit messages. In this situation, Alice still generates AN to confuse Willie, which is different from the PC-based scheme. Thus, the signal vector $\mathbf{y}_w$ received by Willie consists of both the AN $\mathbf{z}$ and background noise, i.e.,

$$\mathbf{y}_w = \sqrt{(1-\rho)P_a}h_{aw}\mathbf{z} + \mathbf{n}_w. \tag{30}$$

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

$$\begin{aligned} p_{FA} &= \mathbb{P}\left((1-\rho)P_a|h_{aw}|^2 + \sigma_w^2 \geq \theta\right) \\ &= \begin{cases} \exp\left(-\frac{(\theta-\sigma_w^2)}{(1-\rho)P_a}\right), & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2. \end{cases} \end{aligned} \tag{31}$$

Combining the p_{FA} in (31) and the p_{MD} in (11), we obtain the COP p_{co}^{IA} under the AN-based scheme as

$$p_{co}^{\mathrm{IA}}(\rho,\theta) = \begin{cases} \exp\left(-\frac{(\theta-\sigma_w^2)}{P_a}\right) - \exp\left(-\frac{(\theta-\sigma_w^2)}{(1-\rho)P_a}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \tag{32}$$

We can see from (32) that the optimal detection threshold θ_{IA}^* for Willie exists when $\theta > \sigma_w^2$ and can be obtained by solving $\frac{\partial p_{co}^{\mathrm{IA}}}{\partial \theta} = 0$. Thus, θ_{IA}^* is given by

$$\theta_{\mathrm{IA}}^* = \sigma_w^2 + \frac{(\rho-1)P_a}{\rho}\ln(1-\rho). \tag{33}$$

By solving the optimization problem in (6) with $\theta = \theta_{\mathrm{IA}}^*$, 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*

$$R_{cs}^{\mathrm{IA}} = R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)\exp\left(-\frac{(2^{R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)}-1)\sigma_b^2}{\rho_{\mathrm{IA}}^* P_a - (2^{R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)}-1)(1-\rho_{\mathrm{IA}}^*)P_a}\right), \tag{34}$$

where ρ_{IA}^* is the optimal power allocation parameter and $R_{s,\mathrm{IA}}^*$ is the optimal secrecy rate. Here, ρ_{IA}^* can be obtained by solving $p_{co}^{\mathrm{IA}}(\rho,\theta_{\mathrm{IA}}^*) = \epsilon_c$ with θ_{IA}^* given by (33). $R_{s,\mathrm{IA}}^*$ is given by

$$R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*) = \begin{cases} R_{s,\mathrm{IA}}^0(\rho_{\mathrm{IA}}^*), R_{s,\mathrm{IA}}^* = R_{s,\mathrm{IA}}^0 \leq \min\left\{R_{s,\mathrm{IA}}^{SOP}, R_{s,\mathrm{IA}}^{TP}\right\}, \\ R_{s,\mathrm{IA}}^{SOP}(\rho_{\mathrm{IA}}^*), R_{s,\mathrm{IA}}^* = R_{s,\mathrm{IA}}^{SOP} \leq \min\left\{R_{s,\mathrm{IA}}^0, R_{s,\mathrm{IA}}^{TP}\right\}, \\ R_{s,\mathrm{IA}}^{TP}(\rho_{\mathrm{IA}}^*), R_{s,\mathrm{IA}}^* = R_{s,\mathrm{IA}}^{TP} \leq \min\left\{R_{s,\mathrm{IA}}^0, R_{s,\mathrm{IA}}^{SOP}\right\}, \end{cases} \tag{35}$$

where the stationary point $R_{s,\mathrm{IA}}^0$ can be obtained by solving $\frac{\partial R_{cs}}{\partial R_s} = 0$, $R_{s,\mathrm{IA}}^{SOP}$ is the solution of $p_{so}^{\mathrm{IA}}(R_s) = \epsilon_s$ and $R_{s,\mathrm{IA}}^{TP}$ is given by

$$R_{s,\mathrm{IA}}^{TP}(\rho_{\mathrm{IA}}^*) = \log\left(\frac{P_a\ln(1-\epsilon_t) - \sigma_b^2}{(1-\rho_{\mathrm{IA}}^*)P_a\ln(1-\epsilon_t) - \sigma_b^2}\right). \tag{36}$$

Proof: The proof follows the same idea as the one for Theorem 1. The only difference is to derive the optimal power allocation parameter ρ instead of optimal transmit power P_a. Here, we focus on the derivation of the optimal ρ and omit the analysis of the optimal R_s. We can see that the objective function in (6a) is an increasing function of ρ, implying that the upper bound on ρ is needed. Substituting $\theta = \theta_{\mathrm{IA}}^*$ into (32) yields

$$p_{co}^{\mathrm{IA}} = \rho(1-\rho)^{\frac{1-\rho}{\rho}}. \tag{37}$$

Taking the first derivative of (37) in terms of ρ, we have

$$\frac{\partial p_{co}^{\mathrm{IA}}}{\partial \rho} = \frac{-\ln(1-\rho)}{\rho}(1-\rho)^{\frac{1-\rho}{\rho}} > 0, \tag{38}$$

which shows that p_{co}^{IA} is an increasing function of ρ. We can see from (26) and (29) that p_{tx}^{IA} is also an increasing function of ρ, while $\rho_{\mathrm{IA}}^{\mathrm{SOP}}$ is a decreasing function. Thus, only the covertness constraint (6b) gives an upper bound $\rho_{\mathrm{IA}}^{\max}$ on ρ, while the TP and SOP constraints in (6d) and (6c) give two lower bounds $\rho_{\mathrm{IA}}^{\mathrm{TP}}$ and $\rho_{\mathrm{IA}}^{\mathrm{SOP}}$ respectively. Hence, the optimal ρ is $\rho_{\mathrm{IA}}^* = \rho_{\mathrm{IA}}^{\max}$. Note that $\rho_{\mathrm{IA}}^{\max} \geq \max\left\{\rho_{\mathrm{IA}}^{\mathrm{TP}}, \rho_{\mathrm{IA}}^{\mathrm{SOP}}\right\}$ must hold, which imposes a constraint (or region) on R_s. However, this region is equivalent to the one obtained from the TP and SOP constraints in (6d) and (6c), and thus can be neglected in the analysis of optimal R_s. ■

IV. CSR Analysis: 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 IV-A and IV-B, respectively. To depict 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 [62].

A. PC-Based Transmission Scheme

Alice follows the same decision process as introduced in Section III-A to decide whether to transmit messages or not. Note that the instantaneous Alice-Bob channel capacity C_b in this case is identical to that in (7), which means that the transmission probability is also the same. Thus, the transmission probability p_{tx}^{FP} in the friend relationship scenario under the PC-based scheme is given by (8).

Next, we analyze the covertness and secrecy performances when Alice transmits messages. When Alice chooses to transmit a signal vector $\mathbf{x}$, Willie and Eve receive the same signal vectors $\mathbf{y}_w$ and $\mathbf{y}_e$ as that given in (9). Since Willie and Eve share their received signals in this case, the signal vectors received at Willie and Eve contain the one from the other side. Thus, based on the signal vector $\mathbf{y}_\kappa$ in (9), the average power of the received symbols at Willie can be given by $\bar{P}_w = \sum_{\kappa\in\{w,e\}}|\mathbf{y}_\kappa|^2 = P_a|h_{aw}|^2 + P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2$. 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

$$\begin{aligned} p_{MD} &= \mathbb{P}\left(P_a|h_{aw}|^2 + P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2 \leq \theta\right) \\ &= \begin{cases} 1 - \frac{P_a+\theta-\sigma_e^2-\sigma_w^2}{P_a}\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right), & \theta > \sigma_e^2+\sigma_w^2, \\ 0, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases} \end{aligned} \tag{39}$$

According to [4], the signal sharing results in an improved Signal-to-Noise Ratio (SNR) for Eve, which is

$\frac{P_a|h_{ae}|^2+P_a|h_{aw}|^2}{\sigma_e^2+\sigma_w^2}$. Thus, the secrecy capacity C_s is

$$C_s = \log\left(1+\frac{P_a|h_{ab}|^2}{\sigma_b^2}\right) - \log\left(1+\frac{P_a|h_{ae}|^2+P_a|h_{aw}|^2}{\sigma_e^2+\sigma_w^2}\right). \tag{40}$$

Since $|h_{ab}|^2$, $|h_{ae}|^2$ and $|h_{aw}|^2$ are independent, the SOP under the PC-based scheme is given by

$$\begin{aligned} p_{so}^{\mathrm{FP}}(R_s) &= 1 - \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right) \\ &\quad \times \mathbb{P}\left(\frac{P_a|h_{ab}|^2}{\sigma_b^2} - 2^{R_s}\frac{P_a|h_{aw}|^2+P_a|h_{ae}|^2}{\sigma_w^2+\sigma_e^2} > 2^{R_s}-1\right) \\ &= \frac{2^{R_s}\sigma_b^2(2^{R_s}\sigma_b^2+2\sigma_w^2+2\sigma_e^2)}{(2^{R_s}\sigma_b^2+\sigma_w^2+\sigma_e^2)^2}. \end{aligned} \tag{41}$$

Finally, we focus on the covertness performance when Alice suspends her transmission. Since the decision of suspending transmission is *unknown* to Willie and Eve, they still share their signals, which contain only background noises. Thus, the received signal at Willie is given by $\mathbf{y}_w = \mathbf{n}_e + \mathbf{n}_w$ and the average received power is $\bar{P}_w = \sigma_e^2 + \sigma_w^2$. Hence, the probability of false alarm p_{FA} can be given by

$$p_{FA} = \mathbb{P}\left(\sigma_e^2+\sigma_w^2 \geq \theta\right) = \begin{cases} 0, & \theta > \sigma_e^2+\sigma_w^2, \\ 1, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases} \tag{42}$$

Combining the p_{FA} in (42) and the p_{MD} in (39), we obtain the COP as

$$p_{co}^{\mathrm{FP}}(P_a,\theta) = \begin{cases} \frac{P_a+\theta-\sigma_e^2-\sigma_w^2}{P_a}\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right), & \theta > \sigma_e^2+\sigma_w^2, \\ 0, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases} \tag{43}$$

Taking the derivative of the p_{co}^{FP} in (43) gives

$$\frac{\partial p_{co}^{\mathrm{FP}}}{\partial \theta} = -\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a^2}\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right). \tag{44}$$

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

$$\theta_{\mathrm{FP}}^* = \upsilon + \sigma_e^2 + \sigma_w^2, \tag{45}$$

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

Given the θ_{FP}^*, the p_{tx} in (8), the SOP in (41) and the COP in (43), the problem in (5) 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 given in* (46)*. Here,*

$$R_{s,\mathrm{FP}}^{SOP} = \log\left(\frac{(1-\sqrt{1-\epsilon_s})(\sigma_w^2+\sigma_e^2)}{\sigma_b^2\sqrt{1-\epsilon_s}}\right), \tag{47}$$

$R_{s,\mathrm{FP}}^{TP}$ and $R_{s,\mathrm{FP}}^{0}$ are the same as those given in (18) and (19), respectively, with the optimal transmit power $P_{a,\mathrm{FP}}^*$ given by

$$P_{a,\mathrm{FP}}^* = -\frac{\upsilon}{1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{e})}. \tag{48}$$

$\mathrm{W}_0(\cdot)$ and $\mathrm{W}_{-1}(\cdot)$ are the principal branch and the non-principle branch of Lambert's W function, respectively, and e is Euler's number.

Proof: Please refer to Appendix A. ∎

B. AN-Based Transmission Scheme

We first derive the transmission probability to characterize the transmission performance of the transmission. Suppose Alice transmits under the AN-based scheme, Bob will receive the same signal as that given in (27), yielding the same instantaneous Alice-Bob channel capacity C_b as that given in (25). This means that the transmission probability p_{tx}^{FA} under the AN-based scheme in the friend relationship scenario is identical to that in the independence scenario, which is given in (26).

We proceed to analyze the miss detection probability and SOP when Alice transmits messages. When Alice transmits a signal vector $\mathbf{x}$, the signal vectors at Willie and Eve are the same as that given in (27). After receiving the shared signals from Eve, the average power $\bar{P}_w$ of the received symbols at Willie is given by $\bar{P}_w = \sum_{\kappa\in\{w,e\}}|\mathbf{y}_\kappa|^2 = P_a|h_{ae}|^2 + P_a|h_{aw}|^2 + \sigma_e^2 + \sigma_w^2$, which is identical to (10), i.e., the average power in the independence case. Thus, the probability of missed detection p_{MD} can be given by (39).

After Eve receives the signals from Willie, the Signal-to-Noise-plus-Interference Ratio (SINR) is

$$\frac{\rho P_a|h_{ae}|^2+\rho P_a|h_{aw}|^2}{(1-\rho)P_a|h_{ae}|^2+(1-\rho)P_a|h_{aw}|^2+\sigma_e^2+\sigma_w^2}. \tag{49}$$

Thus, the secrecy capacity C_s under the AN-based scheme is

$$\begin{aligned} C_s &= \log\left(1+\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}\right) \\ &\quad - \log\left(1+\frac{\rho P_a|h_{ae}|^2+\rho P_a|h_{aw}|^2}{(1-\rho)P_a|h_{ae}|^2+(1-\rho)P_a|h_{aw}|^2+\sigma_e^2+\sigma_w^2}\right), \end{aligned} \tag{50}$$

According to the definition in (4), the SOP is given by (51).

When Alice does not transmit messages, we consider only the covertness of the transmission by analyzing the probability of false alarm. In this case, Alice still sends AN to confuse Willie. Thus, based on (30), the signal vector $\mathbf{y}_w$ contains both the signals (i.e., AN and background noise) shared by Eve, AN and background noise. In this case, the average power of the received symbols at Willie is $\bar{P}_w = (1-\rho)P_a|h_{aw}|^2 + (1-\rho)P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2$. Thus, the probability of false alarm p_{FA} is given by

$$\begin{aligned} p_{FA} &= \mathbb{P}\left((1-\rho)P_a|h_{aw}|^2+(1-\rho)P_a|h_{ae}|^2+\sigma_e^2+\sigma_w^2 \geq \theta\right) \\ &= \begin{cases} \left(1+\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right)\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right), & \theta > \sigma_e^2+\sigma_w^2, \\ 1, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases} \end{aligned} \tag{52}$$

Combining the p_{FA} in (52) and the p_{MD} in (39), the COP can be given by

$$p_{co}^{\mathrm{FA}}(\rho,\theta) = \begin{cases} \left(1+\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right)\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right) \\ -\left(1+\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right)\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right), & \theta > \sigma_e^2+\sigma_w^2, \\ 0, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases} \tag{53}$$

We can see from (53) that the optimal detection threshold θ_{FA}^* can be obtained by solving $\frac{\partial p_{co}^{\mathrm{FA}}}{\partial \theta} = 0$, which is

$$\theta_{\mathrm{FA}}^* = \sigma_e^2 + \sigma_w^2 + \frac{2(\rho-1)P_a}{\rho}\ln(1-\rho). \tag{54}$$

$$R_{cs}^{\mathrm{FP}}=\begin{cases}\frac{1}{\ln 2}\mathrm{W}_0\left(-\frac{\upsilon}{\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{e})\right)\sigma_b^2}\right)\exp\left(-\frac{1}{\mathrm{W}_0\left(-\frac{\upsilon}{\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{e})\right)\sigma_b^2}\right)}-\frac{\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{e})\right)\sigma_b^2}{\upsilon}\right), & R_{s,\mathrm{FP}}^*=R_{s,\mathrm{FP}}^0\le\min\left\{R_{s,\mathrm{FP}}^{\mathrm{SOP}},R_{s,\mathrm{FP}}^{\mathrm{TP}}\right\},\\ \log\left(\frac{(1-\sqrt{1-\epsilon_s})(\sigma_w^2+\sigma_e^2)}{\sigma_b^2\sqrt{1-\epsilon_s}}\right)\exp\left(\frac{\left((1-\sqrt{1-\epsilon_s})(\sigma_w^2+\sigma_e^2)-\sqrt{1-\epsilon_s}\sigma_b^2\right)\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{e})\right)}{\upsilon\sqrt{1-\epsilon_s}}\right), & R_{s,\mathrm{FP}}^*=R_{s,\mathrm{FP}}^{\mathrm{SOP}}\le\min\left\{R_{s,\mathrm{FP}}^0,R_{s,\mathrm{FP}}^{\mathrm{TP}}\right\},\\ (1-\epsilon_t)\log\left(1+\frac{\upsilon\ln(1-\epsilon_t)}{\sigma_b^2\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{e})\right)}\right), & R_{s,\mathrm{FP}}^*=R_{s,\mathrm{FP}}^{\mathrm{TP}}\le\min\left\{R_{s,\mathrm{FP}}^0,R_{s,\mathrm{FP}}^{\mathrm{SOP}}\right\}.\end{cases}\tag{46}$$

$$\begin{aligned}p_{so}^{\mathrm{FA}}(\rho,R_s)&=1-\exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a-(2^{R_s}-1)(1-\rho)P_a}\right)\mathbb{P}\left(\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}-\frac{2^{R_s}(\rho P_a|h_{ae}|^2+\rho P_a|h_{aw}|^2)}{(1-\rho)P_a|h_{ae}|^2+(1-\rho)P_a|h_{aw}|^2+\sigma_e^2+\sigma_w^2}>2^{R_s}-1\right)\\&=1-\exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a-(2^{R_s}-1)(1-\rho)P_a}-\frac{(2^{R_s}+\rho-1)\sigma_b^2}{(1-2^{R_s})(1-\rho)P_a}\right)\times\int_0^{\frac{(1-2^{R_s}(1-\rho))(\sigma_w^2+\sigma_e^2)}{(2^{R_s}-1)(1-\rho)P_a}}\int_0^{\frac{(1-2^{R_s}(1-\rho))(\sigma_w^2+\sigma_e^2)}{(2^{R_s}-1)(1-\rho)P_a}-z}\\&\quad\times\exp\left(-y-\frac{(2^{R_s}-1)\sigma_b^2(\sigma_w^2+\sigma_e^2)-\frac{(2^{R_s}+\rho-1)(1-(1-\rho)2^{R_s})\sigma_b^2(\sigma_w^2+\sigma_e^2)}{(1-2^{R_s})(1-\rho)}}{(1-2^{R_s})(1-\rho)P_a^2(y+z)+(1-(1-\rho)2^{R_s})P_a(\sigma_w^2+\sigma_e^2)}-z\right)\mathrm{d}y\,\mathrm{d}z.\end{aligned}\tag{51}$$

Given the θ_{FA}^* in (54), we solve the optimization problem in (6) 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*

$$R_{cs}^{\mathrm{FA}}=R_{s,\mathrm{FA}}^*(\rho_{\mathrm{FA}}^*)\exp\left(-\frac{(2^{R_{s,\mathrm{FA}}^*(\rho_{\mathrm{FA}}^*)}-1)\sigma_b^2}{\rho_{\mathrm{FA}}^*P_a-(2^{R_{s,\mathrm{FA}}^*(\rho_{\mathrm{FA}}^*)}-1)(1-\rho_{\mathrm{FA}}^*)P_a}\right).\tag{55}$$

Here, the optimal power allocation parameter ρ_{FA}^* solves $p_{co}^{\mathrm{FA}}(\rho,\theta_{\mathrm{FA}}^*)=\epsilon_c$ with θ_{FA}^* given by (54). The optimal secrecy rate $R_{s,\mathrm{FA}}^*$ is given in (35), where $R_{s,\mathrm{FA}}^0$ can be obtained by solving $\frac{\partial R_{cs}}{\partial R_s}=0$, $R_{s,\mathrm{FA}}^{SOP}$ is the solution of $p_{so}^{\mathrm{FA}}(R_s)=\epsilon_s$ and $R_{s,\mathrm{FA}}^{TP}$ is given in (36).

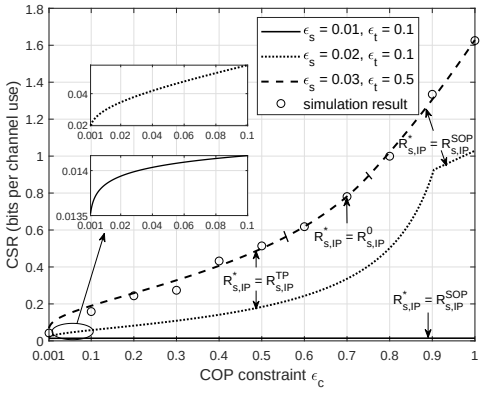
Proof: Please refer to Appendix B. ∎

V. Numerical Results

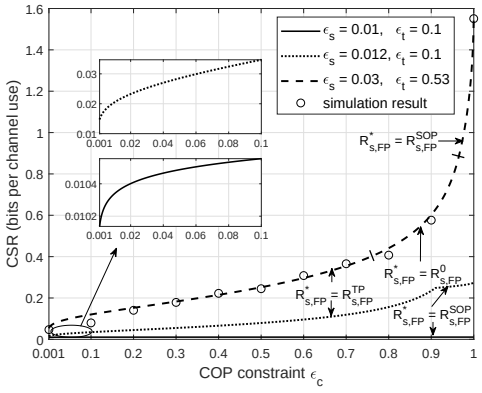
In this section, we provide extensive numerical results to illustrate the CSR performances of the wireless data collection process of the IoT in the four representative scenarios under the new secure communication scenario. We also show the impacts of various system parameters (e.g., COP constraint ϵ_c, SOP constraint ϵ_s, TP constraint ϵ_t and transmit power P_a) on the CSR performance. Unless otherwise stated, we set the parameter υ to $\upsilon=0.01$ and the noise powers at Bob, Willie and Eve to $\sigma_b^2=-20$ dB and $\sigma_w^2=\sigma_e^2=0$ dB.

A. Performance Analysis of CSR

To explore the impact of the COP constraint ϵ_c on the CSR performance for collecting data in the IoT, we show in Fig. 2 R_{cs} vs. ϵ_c in the independence relationship case under the PC-based and AN-based transmission schemes, respectively. The results for the friend relationship case under both transmission schemes are presented in Fig. 3. We set the transmit power of Alice to $P_a=-20$ dB in Fig. 3. In each subfigure

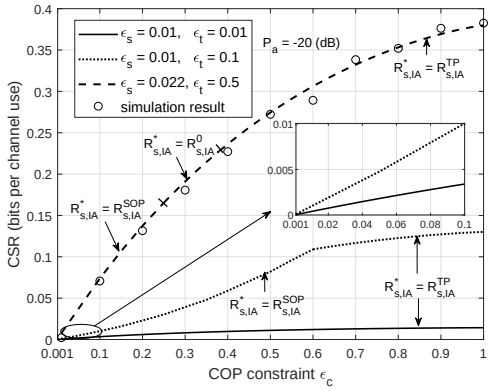


(a) Independence relationship scenario.

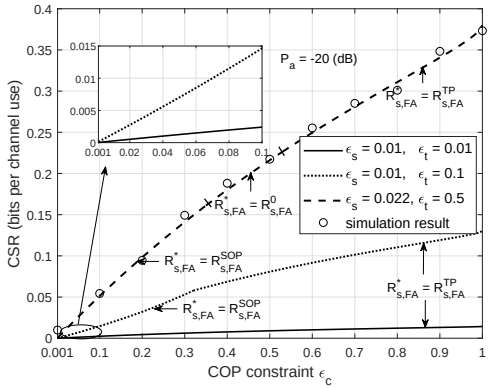


(b) Friend relationship scenario.

Fig. 2. CSR R_{cs} vs. COP constraint ϵ_c (PC-based transmission scheme).

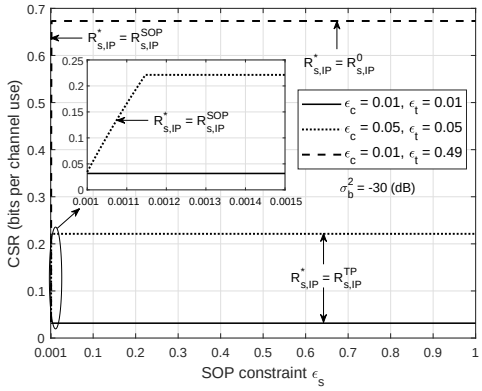


(a) Independence relationship scenario.

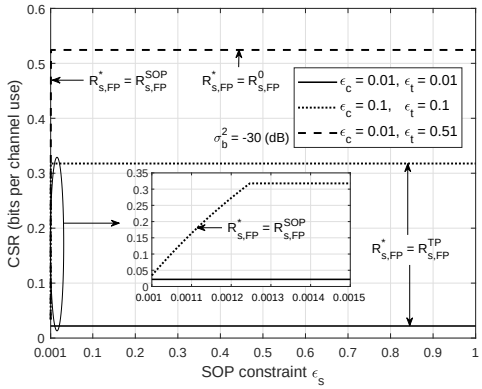


(b) Friend relationship scenario.

Fig. 3. CSR R_{cs} vs. COP constraint ϵ_c (AN-based transmission scheme).



(a) Independence relationship scenario.



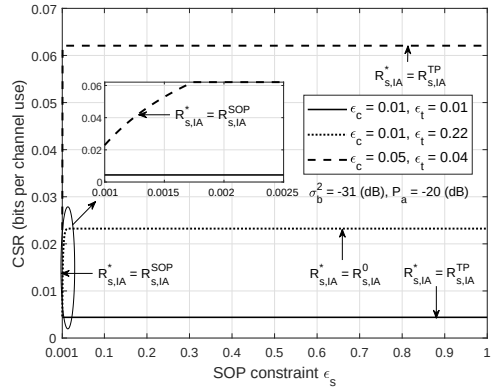
(b) Friend relationship scenario.

Fig. 4. CSR R_{cs} vs. SOP constraint ϵ_s (PC-based transmission scheme).

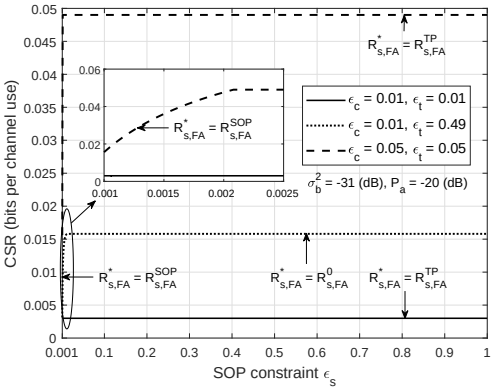
of Fig. 2 and Fig. 3, we also plot the CSR curves under different settings of SOP constraint ϵ_s and TP constraint ϵ_t. In addition, to prove the feasibility of the theoretical results of CSR, we conduct simulations of CSR for each concerned communication scenario under a given setting of ϵ_s and ϵ_t (i.e., $\epsilon_s = 0.03$ and $\epsilon_t = 0.5$ for the independence-PC scenario, $\epsilon_s = 0.03$ and $\epsilon_t = 0.53$ for the friend-PC scenario, as well as $\epsilon_s = 0.022$ and $\epsilon_t = 0.5$ for both the independence-AN and friend-AN scenarios), and plot in Fig. 2 and Fig. 3 the corresponding simulation and theoretical results of CSR. We can see from Fig. 2 and Fig. 3 the theoretical results of CSR match nicely with the corresponding theoretical ones, indicating that our theoretical models can efficiently capture the overall behaviors of CSR. We can see from Fig. 2 and Fig. 3 that the CSRs achieved under different SOP and TP constraints always increase as ϵ_c increases. This is because a looser COP 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 during the wireless data collection process in the IoT.

We can also observe from Fig. 2 and Fig. 3 that the shape of the CSR curve varies as the values of the SOP constraint ϵ_s and TP constraint ϵ_t change. For example, the CSR curve under the setting of $\epsilon_s = 0.03$ and $\epsilon_t = 0.5$ (dashed line) in Fig. 2 exhibits an exponential growth and that under the setting of $\epsilon_s = 0.02$ and $\epsilon_t = 0.1$ (dotted line) grows in a piecewise fashion. This is because different values of ϵ_s, ϵ_t and the COP constraint ϵ_c result in different $R^{\text{SOP}}_{s,\text{IP}}$, $R^{\text{TP}}_{s,\text{IP}}$ and $R^{0}_{s,\text{IP}}$ in (17-19) (resp. $R^{\text{SOP}}_{s,\text{FP}}$, $R^{\text{TP}}_{s,\text{FP}}$, $R^{0}_{s,\text{FP}}$ in (47,18,19), $R^{\text{SOP}}_{s,\text{IA}}$, $R^{\text{TP}}_{s,\text{IA}}$, $R^{0}_{s,\text{IA}}$ in (35) and $R^{\text{SOP}}_{s,\text{FA}}$, $R^{\text{TP}}_{s,\text{FA}}$, $R^{0}_{s,\text{FA}}$ in (35)), which further lead to different optimal target secrecy rates (as labeled in Fig. 2 and Fig. 3) and thus different CSR curves.

Next, we investigate the impact of the SOP constraint ϵ_s on the CSR performance of the wireless data collection process of the IoT, for which we show R_{cs} vs. ϵ_s in the independence and friend relationship cases under the PC-based transmission scheme in Fig. 4 and those under the AN-based transmission scheme in Fig. 5. We set the noise power at Bob to $\sigma_b^2 = -30$ dB in Fig. 4 and that to $\sigma_b^2 = -31$ dB in Fig. 5. We set the transmit power of Alice to $P_a = -20$ dB in Fig. 5. For both figures, we consider three different settings of COP constraint ϵ_c and TP constraint ϵ_t, respectively. We can see from Fig. 4 and Fig. 5 that, in the case when both ϵ_c and ϵ_t are relatively small (e.g., $\epsilon_c = 0.01$ and $\epsilon_t = 0.01$ in Fig. 4(a)), the CSR keeps constant as the SOP constraint ϵ_s increases. This is because that in such case, CSR is only determined by the optimal target secrecy rate $R^*_{s,\text{IP}} = R^{\text{TP}}_{s,\text{IP}}$ shown in (18) (as labeled in Fig. 4(a)), so CSR is independent of ϵ_s. On the other hand, in the case when either ϵ_c or ϵ_t is large (e.g., $\epsilon_c = 0.01$ and $\epsilon_t = 0.49$ in Fig. 4(a)), as ϵ_s increases, CSR first increases sharply and then remains constant. This is

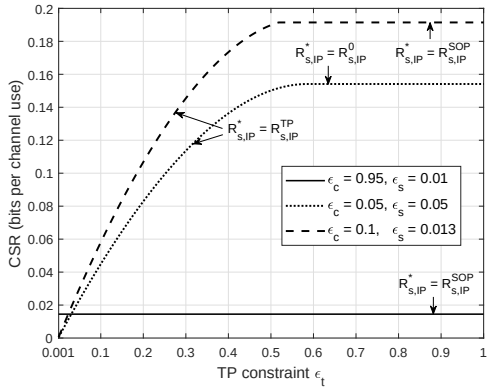


(a) Independence relationship scenario.

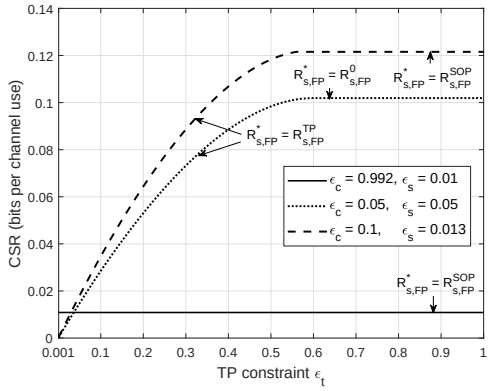


(b) Friend relationship scenario.

Fig. 5. CSR R_{cs} vs. SOP constraint ϵ_s (AN-based transmission scheme).



(a) Independence relationship scenario.



(b) Friend relationship scenario.

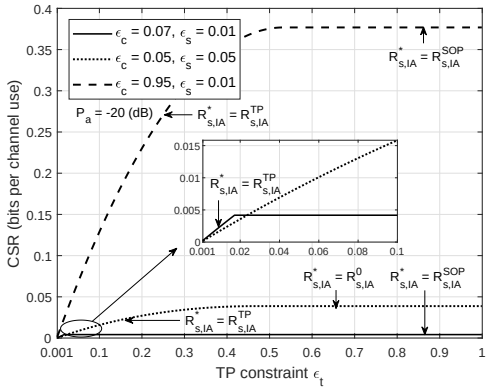
Fig. 6. CSR R_{cs} vs. TP constraint ϵ_t (PC-based transmission scheme).

because that in this case, when ϵ_s is small, CSR is determined by the optimal target secrecy $R^*_{s,\mathrm{IP}} = R^{\mathrm{SOP}}_{s,\mathrm{IP}}$ shown in (17), so CSR increases as ϵ_s increases. However, when ϵ_s increases beyond a threshold, CSR will be determined by the optimal target secrecy rate $R^*_{s,\mathrm{IP}} = R^0_{s,\mathrm{IP}}$ shown in (19), then CSR becomes independent of ϵ_s and thus keeps constant regardless the variation of ϵ_s. Such phenomenon indicates that, when either ϵ_c or ϵ_t is large, the CSR is sensitive to the change of the SOP constraint ϵ_s in an extremely small region, e.g., from 0 to about 0.00115 in Fig. 4(a). Similar phenomena can be observed from Fig. 4(b), Fig. 5(a) and Fig. 5(b).

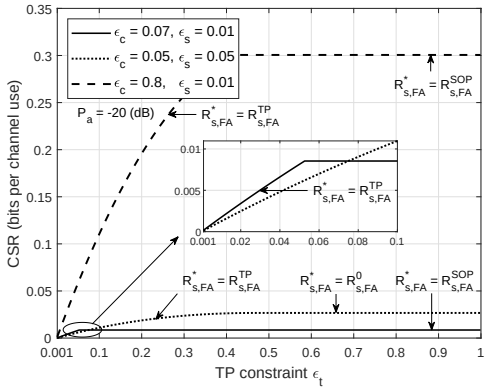
Finally, we show the impact of the TP constraint ϵ_t on the CSR performance of the wireless data collection process of the IoT in Fig. 6 and Fig. 7, where we plot R_{cs} vs. ϵ_t for the two relationship cases under the PC-based and AN-based transmission schemes, respectively. Three different settings of COP constraint ϵ_c and SOP constraint ϵ_s are adopted for each subfigure in Fig. 6 and Fig. 7. We set the transmit power of Alice to $P_a = -20$ dB in Fig. 7. We can see from Fig. 6(a) that in the case that the COP constraint ϵ_c is much larger than the SOP constraint ϵ_s (e.g., $\epsilon_c = 0.95$, $\epsilon_s = 0.01$ here), CSR keeps constant as ϵ_t increases. This is because that in such case, CSR is determined by the optimal target secrecy rate $R^*_{s,\mathrm{IP}} = R^{\mathrm{SOP}}_{s,\mathrm{IP}}$ shown in (17), so CSR is independent of ϵ_t but only dependent on the SOP constraint ϵ_s. Otherwise, in the case when the COP constraint ϵ_c is comparable with the SOP constraint ϵ_s (e.g., $\epsilon_c = 0.05$, $\epsilon_s = 0.05$ here), as ϵ_t increases, CSR first increases and then keeps constant. This is because that in this case, when ϵ_t is small, CSR is determined by the optimal target secrecy $R^*_{s,\mathrm{IP}} = R^{\mathrm{TP}}_{s,\mathrm{IP}}$ shown in (18), so CSR increases as ϵ_t increases. However, when ϵ_t increases beyond a threshold, CSR will be determined by the optimal target secrecy rate $R^*_{s,\mathrm{IP}} = R^0_{s,\mathrm{IP}}$ shown in (19), then CSR becomes independent of ϵ_t and thus keeps constant regardless the variation of ϵ_t. We can observe similar phenomena from Fig. 6(b), Fig. 7(a).

B. Comparisons of CSR in Two Relationship Scenarios

We proceed to compare the CSR performance of the wireless data collection process of the IoT achieved in the independence relationship scenario and that achieved in the friend relationship scenario, for which we show R_{cs} vs. ϵ_c for both relationship scenarios under the PC-based transmission scheme in Fig. 8(a) and those under the AN-based transmission scheme in Fig. 8(b), respectively. We set the SOP constraint and TP constraint to $\epsilon_s = \epsilon_t = 0.1$ in both figures. In addition, we set the parameter υ to $\upsilon = 0.01$ and 0.001 in Fig. 8(a) and the transmit power of Alice P_a to $P_a = -5$ dB and -20 dB in Fig. 8(b). We can observe from both subfigures that the CSRs in the independence relationship case are always larger than those in the friend relationship case under all the parameter settings and both transmission schemes. This

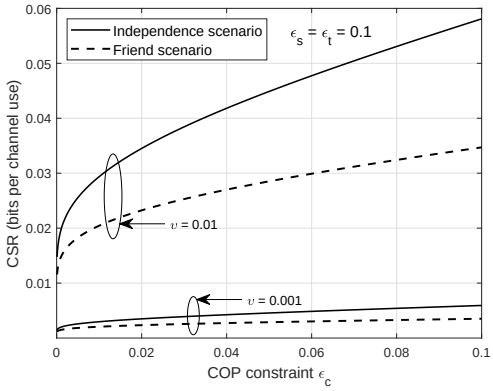


(a) Independence relationship scenario.

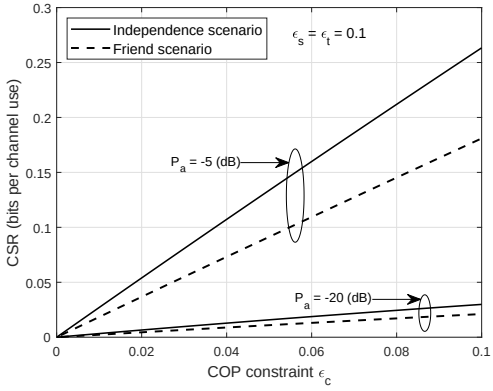


(b) Friend relationship scenario.

Fig. 7. CSR R_{cs} vs. TP constraint ϵ_t (AN-based transmission scheme).



(a) PC-based transmission scheme.



(b) AN-based transmission scheme.

Fig. 8. Comparisons of the CSR performances in two relationship cases.

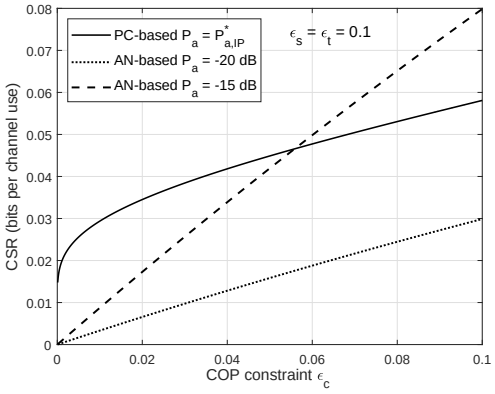
is intuitive since in the friend relationship case, Willie and Eve can share their received signals to improve their attack capability, which will result in a larger SOP/COP and thus a smaller CSR than that in the independence relationship case. The above observations indicate that being friends is the better choice than being independent for the eavesdropper group and detector group.

C. Comparisons of CSR in Two Transmission Schemes

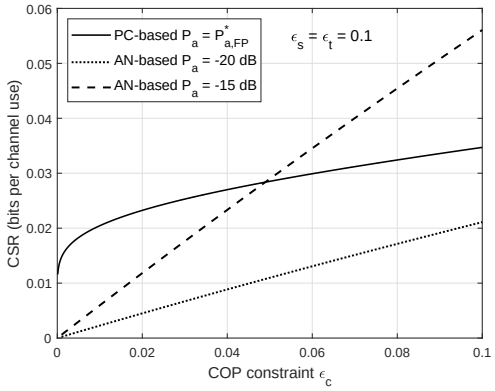
We compare the PC-based transmission scheme and the AN-based transmission scheme in terms of the CSR performance for collecting data in the IoT. To do so, we show R_{cs} vs. ϵ_c in Fig. 9 (resp. R_{cs} vs. ϵ_s in Fig. 10 and R_{cs} vs. ϵ_t in Fig. 11) under both transmission schemes in the independence and friend relationship scenarios, respectively. We set $\epsilon_s = \epsilon_t = 0.1$ in Fig. 9, $\epsilon_c = \epsilon_t = 0.1$ in Fig. 10 and $\epsilon_c = \epsilon_s = 0.1$ in Fig. 11. For each figure, we consider two different settings of the transmit power of Alice P_a for the AN-based scheme. We can observe from Fig. 9 that, in both relationship scenarios, the PC-based scheme achieves better CSR performance than the AN-based scheme, when a small transmit power (e.g., $P_a = -20$ dB) is adopted in the AN-based scheme. However, when the transmit power of AN-based scheme is relatively larger (e.g., $P_a = -15$ dB), the PC-based scheme achieves better CSR performance than the AN-based scheme under stringent COP constraints (e.g., less than about 0.055 in Fig. 9(a)), while the AN-based scheme achieves better CSR performance than the PC-based scheme under less strict COP constraints. This is because, when the constant total transmit power at Alice P_a is larger in the AN-based scheme, the looser COP constraint leads to a larger power allocation parameter ρ, and thus a larger CSR than that in the PC-based scheme.

Similar results can be obtained from Fig. 10, which shows that the PC-based scheme outperforms the AN-based scheme if either the transmit power of the AN-based scheme or the SOP constraint is small. Otherwise, the AN-based scheme outperforms the PC-based scheme. This is because, a larger total transmit power at Alice and a looser SOP constraint in the AN-based scheme leads to a larger optimal target secrecy rate, and thus a larger CSR than that in the PC-based scheme. However, the results obtained from Fig. 11 are different. We can see from Fig. 11 that the AN-based scheme outperforms the PC-based scheme when adopting a large transmit power (i.e., $P_a = -15$ dB), while it achieves worse CSR performance than the PC-based scheme when adopting a small transmit power (i.e., $P_a = -20$ dB). This is because, in this case, the constant total transmit power at Alice P_a in the AN-based scheme is the only one that affects the optimal target secrecy rate, and thus a larger P_a in the AN-based scheme results in a larger CSR than that in the PC-based scheme.

According to the above observations from Fig. 9, Fig. 10 and Fig. 11, we can conclude that when the transmit

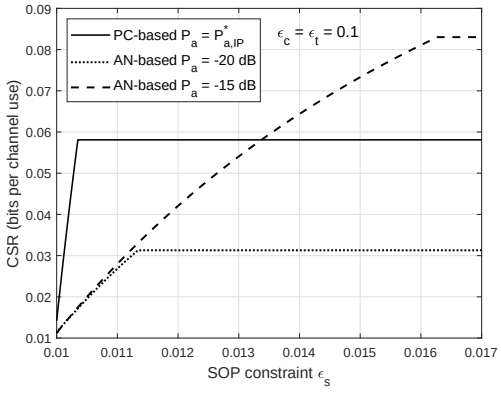


(a) Independence relationship scenario.

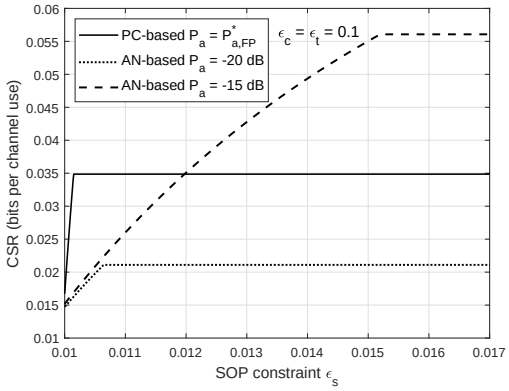


(b) Friend relationship scenario.

Fig. 9. Comparisons of the CSR performances in the PC-based and AN-based transmission schemes (R_{cs} vs. ϵ_c).



(a) Independence relationship scenario.



(b) Friend relationship scenario.

Fig. 10. Comparisons of the CSR performances in the PC-based and AN-based transmission schemes (R_{cs} vs. ϵ_s).

power is not a big concern in the wireless data collection process of IoT, transmitters may prefer to adopt the AN-based transmission scheme to achieve a better CSR performance, especially when a less strict constraint is imposed on the covertness, secrecy and transmission performances. On the other hand, when the transmit power is constrained (e.g., in IoT and sensor networks), the PC-based scheme is more preferable for transmitters.

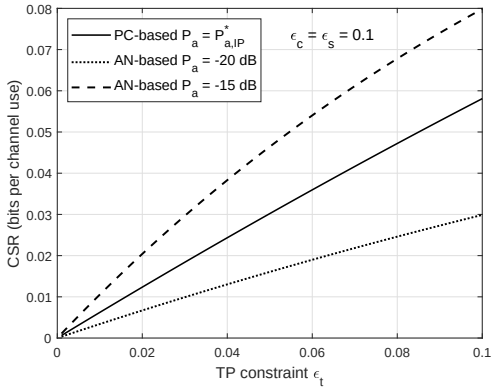
D. Performance Comparisons with Existing Schemes

We also compare the secure communication performance between this work in the Independence-AN scenario with the work in [63] with only covertness guarantee and the work in [64] with only secrecy guarantee, and show in Fig. 12 the corresponding results of CSR/covert rate/secrecy rate vs. Alice's transmit power P_a. Here, we set the COP constraint, SOP constraint and TP constraint as $\epsilon_c = \epsilon_s = \epsilon_t = 0.1$ and set the noise power at Bob $\sigma_b^2 = 0$ dB. We can observe from Fig. 12 that the CSR obtained from this work is always smaller than the covert rate given in [63] and the secrecy rate given in [64]. This is intuitive because the CSR concerned in this work is subjected to the stricter constraints of both covertness and secrecy guarantees, while the covert rate in [63] concerns with only the covertness guarantee and the secrecy rate in [64] concerns with only the secrecy guarantee.

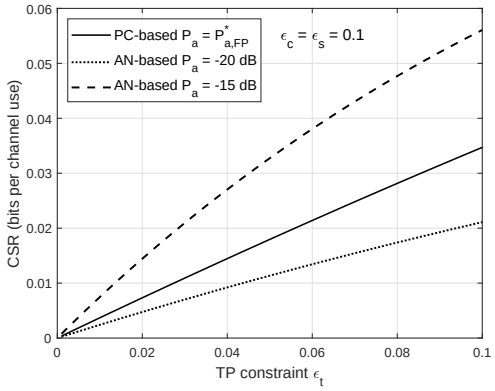
VI. Conclusion

This paper explores a new secure wireless communication scenario for the data collection in the Internet of Things (IoT), where the physical layer security technology is applied to ensure both the covertness and secrecy of the communication. We define a novel metric of covert secrecy rate (CSR) to depict the security performance of the new scenario, and also provide solid theoretical analysis on CSR under two transmission schemes (i.e., artificial noise (AN)-based one and power control (PC)-based one) and two detector-eavesdropper relationships (i.e., independence and friend). The results in this paper indicate that in general the CSR performance of the data collection in the IoT can be improved when the constraints on covertness, secrecy and transmission performance become less strict. In particular, the PC-based transmission scheme outperforms the AN-based transmission scheme in terms of the CSR performance for collecting data in the IoT when strict constraints are applied to the covertness, secrecy and transmission performance. On the other hand, when these constraints become less strict, the AN-based scheme may achieve better CSR performance than the PC-based one by properly adjusting the message transmit power. We expect that this work can shed light on the future studies of both covertness and secrecy guarantees in wireless communication.

Most related works including ours mainly focus on artificial



(a) Independence relationship scenario.



(b) Friend relationship scenario.

Fig. 11. Comparisons of the CSR performances in the PC-based and AN-based transmission schemes (R_{cs} vs. ϵ_t).

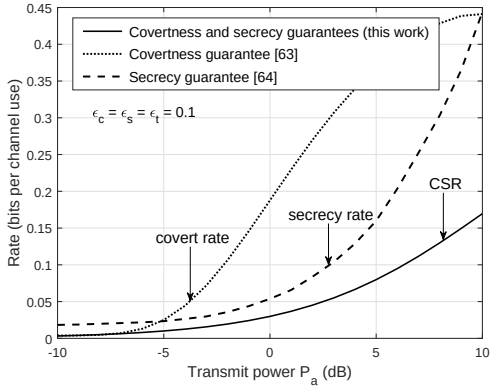


Fig. 12. Comparisons of the secure communication performance between this work and the related works in [63], [64].

noise and cooperative jamming technologies to resist both detection and eavesdropping attacks in single-hop wireless communication, while some PLS technology (e.g., beamforming and resource allocation) can benefit covertness and secrecy guarantees in large complex networks. Thus, a possible future research is to consider other PLS technology for covertness and secrecy guarantees in multi-antenna/multi-hop wireless communication. In addition, notice that this paper considers a simple scenario (i.e., one sender, one receiver, one detector and one eavesdropper), so another interesting future work is to explore the interplay between detection and eavesdropping attacks in more general secure wireless communication scenario with multiple users (or eavesdroppers).

Appendix A
Proof of Theorem 3

The proof follows the same idea as the Theorem 1, and thus the optimization problem in (5) is required to be solved. We first derive the optimal transmit power P_a. We can see that p_{tx}^{FP} as given by (8) monotonically increases as P_a increases. Substituting the optimal threshold θ_{FP}^* in (45) into COP in (43), and then taking the derivative of the optimal p_{co}^{FP} regarding P_a, we have

$$\frac{\partial p_{co}^{\mathrm{FP}}}{\partial P_a} = \frac{\upsilon^2}{P_a^3} \exp\left(-\frac{\upsilon}{P_a}\right), \tag{56}$$

which implies that p_{co}^{FP} is an increasing function of P_a. Thus, under the covertness constraint in (5b), the optimal P_a can be derived as $P_{a,\mathrm{FP}}^*$ in (48). Next, we derive the optimal target secrecy rate R_s. Taking the derivative of SOP in (41) in terms of R_s gives

$$\frac{\partial p_{so}^{\mathrm{FP}}}{\partial R_s} = \frac{2(\sigma_w^2+\sigma_e^2)^2}{(2^{R_s}\sigma_b^2+\sigma_w^2+\sigma_e^2)^3}, \tag{57}$$

which indicates that p_{so}^{FP} monotonically increases as R_s increases. We can also see that as R_s increases, p_{tx}^{FP} in (8) monotonically decreases. Thus, according to the SOP constraint in (5c), TP constraint in (5d) and the feasible region of objective function in (5a), the optimal R_s can be obtained as $R_{s,\mathrm{FP}}^* = R_{s,\mathrm{FP}}^0$ when $R_{s,\mathrm{FP}}^0 \leq \min\{R_{s,\mathrm{FP}}^{\mathrm{SOP}}, R_{s,\mathrm{FP}}^{\mathrm{TP}}\}$, otherwise $R_{s,\mathrm{FP}}^* = \min\{R_{s,\mathrm{FP}}^{\mathrm{SOP}}, R_{s,\mathrm{FP}}^{\mathrm{TP}}\}$. The $R_{s,\mathrm{FP}}^{\mathrm{TP}}$ and $R_{s,\mathrm{FP}}^0$ are the same as those given in (18) and (19), respectively, and $R_{s,\mathrm{FP}}^{\mathrm{SOP}}$ is derived in (47).

Appendix B
Proof of Theorem 4

This proof follows the same idea as the Theorem 2 and therefore requires solving the optimization problem in (6). The analysis of the optimal R_s is similar to that in Theorem 3 and thus omitted here. The difference is to derive the optimal power allocation parameter ρ instead of optimal transmit power P_a. We can obviously see that the objective function in (6a) increases as ρ increases, which implies that the upper bound on ρ is the optimal value. Substituting $\theta = \theta_{\mathrm{FA}}^*$ as in (54) into (53), the optimal p_{co}^{FA} can be given by

$$p_{co}^{\mathrm{FA}} = \left[\rho(2-\rho) - 2(1-\rho)\ln(1-\rho)\right](1-\rho)^{\frac{2(1-\rho)}{\rho}}. \tag{58}$$

Next, taking the derivative of the COP in (58) regarding ρ, we have

$$\frac{\partial p_{co}^{\mathrm{FA}}}{\partial \rho} = \left(\frac{2\ln(1-\rho)}{\rho}\right)^2 (1-\rho)^{\frac{2-\rho}{\rho}}, \tag{59}$$

which demonstrates that p_{co}^{FA} is an increasing function of ρ. In addition, we can see from (26) and (51) that, as ρ increases, p_{tx}^{FA} increases, while p_{so}^{FA} decreases. According to the constraints (6d) and (6c), the lower bounds $\rho_{\mathrm{FA}}^{\mathrm{TP}}$ and

$\rho_{\mathrm{FA}}^{\mathrm{SOP}}$ can be obtained, respectively. Therefore, the covertness constraint (6b) gives an upper bound of ρ which is the optimal power allocation parameter as

$$\rho_{\mathrm{FA}}^{*} = \underset{0\leq\rho\leq 1}{\arg} \; p_{co}^{\mathrm{FA}}(\rho) = \epsilon_c, \tag{60}$$

when the conditions must hold as $\rho_{\mathrm{FA}}^{*} \geq \max\left\{\rho_{\mathrm{FA}}^{\mathrm{TP}}, \rho_{\mathrm{FA}}^{\mathrm{SOP}}\right\}$.

ACKNOWLEDGMENT

This work was supported in part by the Japan Society for the Promotion of Science (JSPS) under Grant No.23H03386, in part by the Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shaanxi (Grant No. QCYRCXM-2022-144), in part by the National Natural Science Foundation of China (Grant No. 62220106004, No. 62202354 and No. 61972308).

REFERENCES

[1] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[2] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[3] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communications without channel state information at receiver in IoT systems," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11 103–11 114, 2020.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[9] 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, 2017.

[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, 2014.

[11] C. Wu, S. Yan, X. Zhou, R. Chen, and J. Sun, "Intelligent reflecting surface (IRS)-aided covert communication with warden's statistical CSI," *IEEE Wireless Communications Letters*, 2021.

[12] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Robust power allocation in covert communication: Imperfect CDI," *IEEE Transactions on Vehicular Technology*, 2021.

[13] 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.

[14] M. Zheng, A. Hamilton, and C. Ling, "Covert communications with a full-duplex receiver in non-coherent rayleigh fading," *IEEE Transactions on Communications*, vol. 69, no. 3, pp. 1882–1895, 2021.

[15] X. Chen, W. Sun, C. Xing, N. Zhao, Y. Chen, F. R. Yu, and A. Nallanathan, "Multi-antenna covert communication via full-duplex jamming against a warden with uncertain locations," *IEEE Transactions on Wireless Communications*, 2021.

[16] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3463–3473, 2020.

[17] K. Shahzad and X. Zhou, "Covert wireless communications under quasi-static fading with channel uncertainty," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1104–1116, 2020.

[18] 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.

[19] R. Ma, W. Yang, L. Tao, X. Lu, Z. Xiang, and J. Liu, "Covert communications with randomly distributed wardens in the finite blocklength regime," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 533–544, 2021.

[20] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12 432–12 436, 2019.

[21] T. Zheng, H. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1974–1987, 2019.

[22] D. Kibloff, S. M. Perlaza, and L. Wang, "Embedding covert information on a given broadcast code," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2019, pp. 2169–2173.

[23] M. Tahmasbi and M. R. Bloch, "Covert secret key generation with an active warden," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1026–1039, 2019.

[24] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet of Things Journal*, 2021.

[25] Y. Su, H. Sun, Z. Zhang, Z. Lian, Z. Xie, and Y. Wang, "Covert communication with relay selection," *IEEE Wireless Communications Letters*, 2020.

[26] L. Sun, T. Xu, S. Yan, J. Hu, X. Yu, and F. Shu, "On resource allocation in covert wireless communication with channel estimation," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6456–6469, 2020.

[27] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Secure millimeter-wave ad hoc communications using physical layer security," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021.

[28] F. Sarkohaki, R. Fotohi, and V. Ashrafian, "An efficient routing protocol in mobile ad-hoc networks by using artificial immune system," *arXiv preprint arXiv:2003.00869*, 2020.

[29] 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.

[30] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, "Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1216–1220, 2020.

[31] Z. Peng, Z. Zhang, C. Pan, L. Li, and A. L. Swindlehurst, "Multiuser full-duplex two-way communications via intelligent reflecting surface," *IEEE Transactions on Signal Processing*, 2021.

[32] Z. H. Abbas, G. Abbas, M. S. Haroon, and F. Muhammad, "Analysis of interference management in heterogeneous cellular networks in the presence of wideband jammers," *IEEE Communications Letters*, vol. 24, no. 5, pp. 1138–1141, 2020.

[33] W. U. Khan, F. Jameel, M. A. Jamshed, H. Pervaiz, S. Khan, and J. Liu, "Efficient power allocation for NOMA-enabled IoT networks in 6G era," *Physical Communication*, vol. 39, p. 101043, 2020.

[34] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure beamforming for full-duplex MIMO two-way untrusted relay systems," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3775–3790, 2020.

[35] X. Huanga, A. T. Leb, and Y. J. Guoc, "Transmit beamforming for communication and self-interference cancellation in full duplex MIMO systems: A trade-off analysis," *IEEE Transactions on Wireless Communications*, 2021.

[36] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy efficient robust beamforming and cooperative jamming design for IRS-assisted MISO networks," *IEEE Transactions on Wireless Communications*, 2020.

[37] 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.

[38] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1670–1683, 2018.

[39] Y. Liu, W. Wang, H. H. Chen, L. Wang, N. Cheng, W. Meng, and X. Shen, "Secrecy rate maximization via radio resource allocation in cellular underlaying V2V communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7281–7294, 2020.

[40] Y. Wu, J. Shi, K. Ni, L. Qian, W. Zhu, Z. Shi, and L. Meng, "Secrecy-based delay-aware computation offloading via mobile edge computing for internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4201–4213, 2018.

[41] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, "Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 493–505, 2019.

[42] J. Du, C. Jiang, J. Wang, Y. Ren, and M. Debbah, "Machine learning for 6G wireless networks: Carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 122–134, 2020.

[43] X. Liao, J. Si, J. Shi, Z. Li, and H. Ding, "Generative adversarial network assisted power allocation for cooperative cognitive covert communication system," *IEEE Communications Letters*, vol. 24, no. 7, pp. 1463–1467, 2020.

[44] A. K. Kamboj, P. Jindal, and P. Verma, "Machine learning-based physical layer security: techniques, open challenges, and applications," *Wireless Networks*, vol. 27, no. 8, pp. 5351–5383, 2021.

[45] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: Architecture, security challenges and research opportunities," *Computers & Security*, vol. 104, pp. 102–211, 2021.

[46] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, pp. 101–883, 2021.

[47] L. Li, L. Liu, H. Peng, Y. Yang, and S. Cheng, "Flexible and secure data transmission system based on semitensor compressive sensing in wireless body area networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3212–3227, 2018.

[48] K.-A. Shim, "Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9211–9212, 2019.

[49] M. Forouzesh, P. Azmi, N. Mokari, and K. K. Wong, "Covert communications versus physical layer security," *arXiv preprint arXiv:1803.06608*, 2018.

[50] H.-M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 389–401, 2020.

[51] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020.

[52] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7170–7181, 2020.

[53] T. Wang, Y. Li, Y. Wu, and T. Q. Quek, "Secrecy driven federated learning via cooperative jamming: An approach of latency minimization," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 4, pp. 1687–1703, 2022.

[54] 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.

[55] W. He, J. Chen, G. Li, H. Wang, X. Chu, R. He, Y. Xu, and Y. Jiao, "Optimal transmission probabilities of information and artificial noise in covert communications," *IEEE Communications Letters*, pp. 1–1, 2022.

[56] S. Feng, X. Lu, S. Sun, and D. Niyato, "Mean-field artificial noise assistance and uplink power control in covert IoT systems," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7358–7373, 2022.

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

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

[59] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE international symposium on information theory*. IEEE, 2006, pp. 356–360.

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

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

[62] 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.

[63] M. Wang, W. Yang, X. Lu, C. Hu, B. Liu, and X. Lv, "Channel inversion power control aided covert communications in uplink NOMA systems," *IEEE Wireless Communications Letters*, vol. 11, no. 4, pp. 871–875, 2022.

[64] H. Guo, Z. Yang, Y. Zou, B. Lyu, Y. Jiang, and L. Hanzo, "Joint reconfigurable intelligent surface location and passive beamforming optimization for maximizing the secrecy-rate," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2098–2110, 2023.