

Cooperative Jamming and Relay Selection for Covert Communications in Wireless Relay Systems

Chan Gao, Bin Yang, Dong Zheng, Xiaohong Jiang, Tarik Taleb

Abstract—This paper investigates the covert communications via cooperative jamming and relay selection in a wireless relay system, where a source intends to transmit a message to its destination with the help of a selected relay, and a warden attempts to detect the existence of wireless transmissions from both the source and relay, while friendly jammers send jamming signals to prevent warden from detecting the transmission process. To this end, we first propose two relay selection schemes, namely random relay selection (RRS) and max-min relay selection (MMRS), as well as their corresponding cooperative jamming (CJ) schemes for ensuring covertness in the system. We then provide theoretical modeling for the covert rate performance under each relay selection scheme and its CJ scheme and further explore the optimal transmit power controls of both the source and relay for covert rate maximization. Finally, extensive simulation/numerical results are presented to validate our theoretical models and also to illustrate the covert rate performance of the relay system under cooperative jamming and relay selection.

Index Terms—Wireless relay systems, covert communications, relay selection, cooperative jamming, covert rate.

I. INTRODUCTION

WIRELESS communication technologies have fundamentally transformed our daily life in the past decade, and are expected to create a fully-connected digital world in the coming sixth-generation (6G) era, where enabling the Internet of everything will promote unprecedented transmissions of sensitive personal data over wireless channels [2]. Due to the broadcasting and open characteristics of wireless channels, wireless systems are highly vulnerable to security threats both in civil and military applications. To cope with such threats, it is desired to explore a promising security method providing

This work was supported by the National Natural Science Foundation of China under Grant No. 62372076, 62372370 and 62072371, the Youth Innovation Team of Shaanxi Universities, and the Natural Science Project of Anhui/Chuzhou University under Grant No. 2020qd16, KJ2021ZD0128, 2022XJZD12, 2023AH051593 and KJ2021B01. (Corresponding author: Bin Yang)

C. Gao is with the National Engineering Research Center for Secured Wireless, School of Cybersecurity, Xi'an University of Posts and Telecommunications, Xi'an 710121, China. E-mail: gaochan001@163.com.

B. Yang is with the School of Computer and Information Engineering, Chuzhou University, China. E-mail: yangbinchi@gmail.com.

D. Zheng is with the National Engineering Research Center for Secured Wireless, School of Cybersecurity, Xi'an University of Posts and Telecommunications, Xi'an 710121, China. E-mail: zhengdong@xupt.edu.cn.

X. Jiang is with the School of Systems Information Science, Future University Hakodate, Japan. E-mail: 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. E-mail: tarik.taleb@oulu.fi.

An earlier version of part work in this paper was appeared in the author's thesis [1].

strong protection for numerous security-sensitive applications in 5G/6G wireless systems.

The available security methods mainly utilize encryption technologies implemented at upper-layer protocol. Such methods usually require high computational power because of their complexity [3]. However, there exist many Internet-of-Things (IoT) devices with limited power. As a complementary to the encryption technologies, physical layer security (PLS) is emerging as a promising class of technologies, which are to exploit the interference and noise of wireless channels to ensure the secrecy of communications. Specially, covert communications are a promising PLS technology aiming to hide the process of wireless transmission from being detected by a warden.

A. Related Works

The available works on the studies of covert communications mainly focus on one-hop and two-hop wireless relay systems where a transmitter attempts to covertly transmit information to a receiver with/without the help of a relay. For the one-hop wireless systems, these works explore the fundamental covert performances in terms of covert rate and detection error probability under various scenarios such as different channel models [4], [8]–[11], channel uncertainty [12], noise uncertainty [13], channel inversion power control [14], delay constraints [15], jamming signals [16]–[23], and unmanned aerial vehicle (UAV) scenarios [24]. The covert performances are further investigated in the two-top wireless relay systems [26]–[30], where one/multiple wardens try to detect the presence of wireless communications from a transmitter to a relay and from the relay to a destination.

Regarding the one-hop wireless systems, the works focus on covert communications with/without the aid of jamming signals. Without the jamming signals, the authors in [5]–[7] prove that when the number of channel uses n goes to infinity, $O(\sqrt{n})$ bits of message can be transmitted covertly to a legitimate receiver. Following these works, the same results are proved to be achievable under various channel models such as discrete memoryless channels [8], [9], multiple-access channels [10] and state-dependent channels [11]. In addition, channel uncertainty [12] and noise uncertainty [13] are used to enhance covert performances. Later, the work in [14] adopts channel inversion power control to achieve covert communications. The work in [15] further explores the impact of delay constraints on covert communications. The authors in [25] examines delay-intolerant covert communications in additive white Gaussian noise (AWGN) channels with a finite

block length and enhances the covert rate by using uniformly distributed random transmit power. Then, they study the optimality of Gaussian signalling for covert communications with an upper bound [4], and further explores the jointly optimizes the flying location and wireless communication transmit power for a UAV conducting covert operations in [24].

For the one-hop wireless systems with the jamming signals, the works in [16], [17] explore that a friendly node sends artificial noise to confuse the detection of a warden. For the scenario of multiple interferers, the work in [18] investigates the impact of the density and the transmit power of the interferers on the covert performance, where the locations of the interferers follow the Poisson point process. The work in [19] further optimizes the covert rate through the jamming signals from the interferers in the scenario consisting of a source equipped with multiple antennas, a destination, randomly distributed wardens, and interferers. The work in [20] indicates that the covert communications are achievable via artificial noise from a friendly unmanned aerial vehicle. In a device-to-device (D2D) underlaid cellular system, the covert communications are proved to be achievable with the aid of artificial noise from a base station (BS) [21]. Recently, each friendly jamming node can be selected to independently transmit jamming signals to defeat the warden based on an uncoordinated jammer selection scheme [22]. The authors in [23] use the inherent uncertainty of backscatter transmissions to achieve active and passive covert communications.

Note that two-hop wireless relay systems are different from one-hop wireless systems due to the extended wireless range with the help of relay. However, it also poses a new challenge on covert communications. In such systems, warden can detect the two hop transmission processes. The existing works in two-hop wireless relay systems mainly focus on the scenario including only one relay without jamming signals. The work in [26] studied the covert performances in terms of the detection error probability and covert rate under the AWGN channels. The channel uncertainty is used to degrade the detection of warden in [27]. The authors in [28] investigate the achievable performance of covert communication in a greedy relay-aided wireless system, where the relay also attempts to covertly send its own messages to a destination when it forwards the messages from a source. In the work [29], they explore the performance of covert communication and associated costs for a self-sustained relay, where the source provides energy to the relay for forwarding its information and the relay's covert transmission is forbidden. The authors in [30] study the covert communication and secure transmission in the scenario with multiple untrusted relays, where the destination and the source can inject jamming signals for achieving covert communications. Recently, the reconfigurable intelligent surface (RIS) is emerging as a promising technology that has the ability to prevent a warden from detecting the transmission process and improve energy efficiency [36]. In work [37], UAV-IRS is acted as a similar relay, and transmit power of the transmitter and the phase shift of IRS are jointly optimized to maximize the covert rate. Although RIS has some similarities with relay, their impact on the system performance has fundamental differences. The main limitation of RIS is that the reflected

channel from source to RIS (S-R) and from RIS to destination (R-D) is worse than the direct channel between the source and destination, since the reflected channel is the product of the S-R channel and the R-D channel. The relay technology can overcome this limitation of RIS but at the cost of additional energy consumption at the relay.

B. Motivation and Contributions

It is notable that cooperative jamming and relay selection are two critical schemes for improving covert performances in the above works. Using the cooperative jamming scheme, the available works mainly utilize the jamming signals to confuse the detection of the warden, while ignoring the serious interference of the jamming signals on the legitimate receiver which may lead to the degradation of system performances. Hence, one fundamental issue is to design a cooperative jamming scheme such that the jamming signals can interfere with an illegal warden and reduce the interference to the legal receiver as much as possible. On the other hand, the relay selection is of great importance for the improvement of covert performances. Particularly, the work in [33] demonstrates the potential of cooperative jamming and relay selection in enhancing covert performance in a two-hop wireless relay system. However, the work considers a simple scenario with one jammer and the second hop covert communication. Meanwhile, it also ignores the impact of the first hop channel status on the relay selection. In reality, it is essential to guarantee the covertness of two-hop transmissions for achieving user's privacy protection. As a result, two challenging issues arise in wireless relay systems. One challenging issue is how to enhance the covert performance of two-hop transmissions by a joint design for cooperative jamming and relay selection. The difficulty in the joint design is how to select multiple jammers to interfere with the warden as much as possible while minimizing the negative effect of the jamming signals on the legal receivers. Another challenging issue is how to develop a theoretical model of covert rate performance. This is because it is difficult to derive some basic results, e.g., the complex probability density function of the sum of multiple random variables on channel gains, the complex detection error probability at the warden, the complex optimal detection threshold, and the complex transmission outage probability. It is notable that the essential difference between the theoretical model and that of [33] is that the former is more complex due to the fact that multiple jammers introduce multiple random variables on channel gains, while there is only one jammer in [33].

To address these two challenging issues, this paper explores a joint design for cooperative jamming and relay selection in a two-hop wireless relay system. To the best of my knowledge, this is the first work to focus on a general scenario with multiple jammers-assisted two-hop covert communications. Such a joint design can improve the covert rate performance of two-hop transmissions through reducing the negative effect of multiple jamming signals on the relay and legal receiver and selecting the best relay with carefully considering two hop channel statuses. We also develop the theoretical models to characterize the covert rate performance in such a system.

TABLE I
MAIN NOTATIONS

Variable	Definition	Variable	Definition
A	Source node	P_T	Covert message transmit power of nodes A and C
B	Destination node	P_J	Jamming transmit power of node J_j
W	Warden node	P_{max}	Maximum transmit power constraint of nodes A , C and jammer
C	Selected message relay	H_0	The node isn't sending covert message
J_j	Selected jamming relay	H_1	The node is sending covert message
RRS	Random relay selection	\mathbb{P}_{FA}	Probability of false alarm
MMRS	Max-min relay selection	\mathbb{P}_{MD}	Probability of missed detection
CJ	Cooperative jamming	α	Interference threshold
SIR	Signal-to-Interference Ratio	λ	Detection threshold
$ h_{ij} ^2$	Channel gain between nodes i and j	ζ	Total detection error probability
σ_i^2	Noise variance of node i	ζ^*	The minimum value of total detection error probability
n	Number of relays	θ	Decoding threshold
l	Number of jamming relays	R_i	The i -th relay
m	Number of channel uses	P_{to}	Transmission outage probability under RRS scheme
$\ln(\cdot)$	Logarithmic function	P_{sto}	Transmission outage probability under MMRS scheme
$\exp(\cdot)$	Exponential function	R_{ij}	Covert rate between nodes i and j under RRS scheme
$\Gamma(\cdot)$	Gamma distribution	R_{ij}^*	Covert rate between nodes i and j under MMRS scheme
$P(\cdot)$	Probability operator	R_{ij}^*	Maximum covert rate between nodes i and j under RRS scheme
$f(\cdot)$	Probability-density-function (PDF)	R_{ij}^*	Maximum covert rate between nodes i and j under MMRS scheme
$\mathbb{E}[\cdot]$	Expectation operator	ε_c	Covertness requirement

The main contributions of this paper can be summarized as follows.

- We consider a wireless relay system consisting of one source Alice, a number of potential relays, one destination Bob, and one warden. In such a scenario, we propose two relay selection schemes, namely random relay selection (RRS) and max-min relay selection (MMRS), as well as their corresponding cooperative jamming schemes for ensuring covertness.
- By applying a joint jamming and RRS scheme, we first examine the transmission strategy design for the source and determine the detection error probability at the warden. We then derive the expressions for three performance metrics (i.e., transmission outage probability, detection error probability of the warden, and covert rate), and also explore the covert rate maximization through efficient numerical searches under the given covertness and outage requirements.
- We further apply a joint jamming and MMRS scheme. Under this scheme, we first examine the transmission strategy design for the source. We then derive the detection error probability of the warden, and optimize the transmit power of the source to maximize the covert rate with a constraint of covertness requirement through efficient numerical searches.
- Finally, extensive simulation and numerical results are presented to validate our theoretical models and also to illustrate the covert rate performance of the relay system under joint jamming and relay selection.

We organize the rest of the paper as follows. Section II introduces related works. The system model and performance metrics are presented in Section III. Section IV explores the covert rate performance under the joint jamming and RRS scheme. Section V explores the covert rate performance under the joint jamming and MMRS scheme. We provide the numerical results in Section VI. This paper is concluded in Section VII. The main notations of this thesis are summarized in Table I.

II. SYSTEM MODELS

A. Network Model

As shown in Fig.1, we consider a wireless relay system composed of one source Alice (A), n potential relays, one destination Bob (B), and one warden Willie (W). Alice aims to covertly transmit a message to Bob with the aid of a relay Carol (C) selected from these relays, while Willie attempts to detect whether Alice sends a message or not. The potential relays can also be selected as friendly jammers broadcasting jamming signals to confuse the detection of Willie. Alice and Carol employ the same covert transmit power P_T to send a message and all friendly Jammers have a transmit power P_J , which is no more than a maximum power constraint P_{max} . We assume that each of Alice, Carol, Jammers, and Bob is equipped with a single antenna.

B. Channel Model

Rayleigh fading happens because of the multipath reception, and thus it is most applicable when there is no a strong line-of-sight path from a transmitter to its receiver [34]. Our concerned wireless relay system is deployed in an urban area with obstacles (e.g., buildings). Thus, we use a quasi-static Rayleigh fading to model wireless channels in a time-slotted relay system. With the fading, all channel coefficients keep unchanged within one time slot and change independently from one time slot to another.

The channel fading coefficients between Alice and Carol, Alice and Willie, Carol and Bob, Carol and Willie, any friendly Jammer (J_i) and Willie, J_i and Carol, and J_i and Bob are denoted as h_{AC} , h_{AW} , h_{CB} , h_{CW} , h_{J_iW} , h_{J_iC} , and h_{J_iB} , respectively, which follow a complex Gaussian distribution with zero mean and unit variance. The $|h_{ij}|^2$ is the corresponding channel gain, where $ij \in \{AC, AW, CB, CW, J_iC, J_iW, J_iB\}$. We assume that the channel gain includes the antenna gain of the transmit/receive antennas as well as the distance between any two nodes [38].

We use AWGN with variance σ^2 to model the channel noise. We assume that Carol works in half-duplex mode and hence

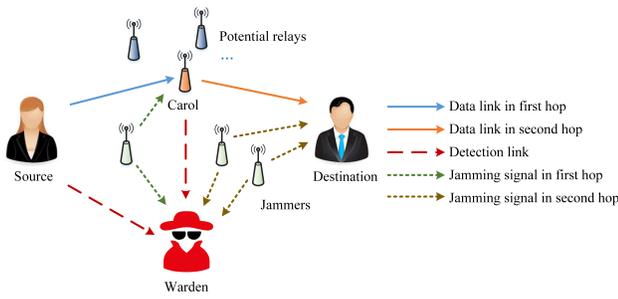


Fig. 1. Covert communication scenario.

the transmission from Alice to Carol and that from Carol to Bob occur in different time slots. Without loss of generality, we assume that the total system bandwidth is 1 MHz.

C. Relay Selection Schemes

We consider two relay selection schemes (i.e., RRS and MMRS) in our study.

RRS: Under such a scheme, Alice randomly chooses one from all potential relays, which will help him to forward the message to Bob.

MMRS: Under this scheme, a potential relay can be selected as the relay Carol if the following condition holds: the maximum value of the minimum channel gain between $|h_{AC}|^2$ and $|h_{CB}|^2$ equals the maximum one of all minimum channel gains. Here, each minimum channel gain corresponds to the minimum one between $|h_{Ai}|^2$ and $|h_{iB}|^2$ for any potential relay i .

D. Cooperative Jamming Scheme

Under each relay selection scheme, the corresponding cooperative jamming (CJ) scheme is further proposed for enhancing covertness performance. The mechanism and process architecture is shown in Fig.2. Based on this scheme, the jammers selected from the potential relays (except the relay Carol) can send artificial noise to confuse the warden's detection, and also reduce interference on Carol and the destination Bob as much as possible. Specifically, for the first hop transmission, any potential relay J_i can be selected as a jammer only if the interference of the jammer on Carol is less than a given threshold. This means that the channel gain from J_i to Carol C is smaller than a threshold α , i.e., $|h_{J_iC}|^2 < \alpha$. As for the second hop transmission, J_i can be selected as a jammer only if the interference of the jammer on Bob is less than a given threshold. This means that the channel gain from J_i to Bob B is smaller than a threshold α , i.e., $|h_{J_iB}|^2 < \alpha$.

E. Performance Metrics

Willie attempts to decide whether Alice sends a message or not. To this end, it performs two hypotheses, namely, null hypothesis H_0 and alternative hypothesis H_1 . Under H_0 , the transmitter does not transmit a message, while it transmits under H_1 . Then, we give the following definitions of two performance metrics.

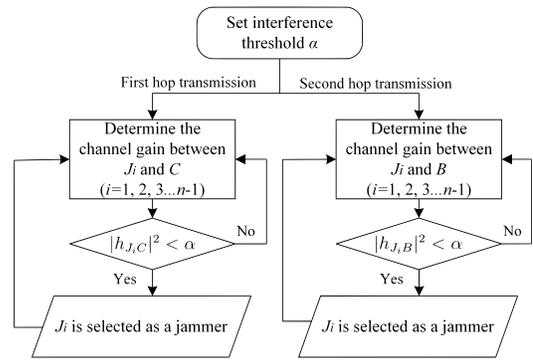


Fig. 2. Mechanism and process architecture of cooperative jamming scheme.

Detection error probability: It is defined as the probability ζ that Willie misjudges whether Alice sends a message or not, which equals the sum of the probability of false alarm \mathbb{P}_{FA} and that of missed detection \mathbb{P}_{MD} . Here, the false alarm means that Willie approves H_1 , but H_0 is true actually. The missed detection means that Willie approves H_0 , but H_1 is true actually.

Covert rate: It is defined as the achievable rate at which Alice can covertly send messages to Bob while maintaining high detection error probability at Willie.

III. COVERT RATE UNDER A JOINT CJ AND RRS SCHEME

A. Detection At Willie

At a time slot, Willie attempts to judge whether Alice transmits a message or not according to the two hypotheses introduced in Section II-E. Based on the hypotheses, the received signal y_W at Willie from Alice/Carol under the joint CJ and RRS scheme is given by

$$y_W = \begin{cases} \sum_{J_i} \sqrt{P_J} h_{J_iW} x_j + n_W, & \text{if } H_0 \text{ is true} \\ \sqrt{P_T} h_{kW} x_k + \sum_{J_i} \sqrt{P_J} h_{J_iW} x_j + n_W, & \text{if } H_1 \text{ is true} \end{cases} \quad (1)$$

where x_j is the signal transmitted by jammers J_i , x_k is the signal transmitted by Alice/Carol, $k \in \{A, C\}$, and n_W is the AWGN at Willie with variance σ_W^2 , i.e., $n_W \sim \mathcal{CN}(0, \sigma_W^2)$.

According to the Neyman-Pearson criterion, Willie uses the following optimal decision to minimize his detection error probability [28]:

$$Y \underset{D_0}{\overset{D_1}{\gtrless}} \lambda, \quad (2)$$

where D_0 and D_1 denote that Willie decides to approve H_0 and H_1 , respectively, λ is a detection threshold, and $Y = \frac{1}{m} \sum_{i=1}^m |y_W^i|^2$ is the average received power at Willie in the time slot. Here, y_W^i is the received signal at Willie in i th channel use, and m is the number of channel uses. Considering an infinite number of channel uses in our study, we have

$$Y = \begin{cases} \sum_{J_i} P_J |h_{J_i W}|^2 + \sigma_W^2, & \text{if } H_0 \text{ is true} \\ P_T |h_{k W}|^2 + \sum_{J_i} P_J |h_{J_i W}|^2 + \sigma_W^2. & \text{if } H_1 \text{ is true} \end{cases} \quad (3)$$

B. Optimal Detection Threshold and Minimum Detection Error Probability

To determine the optimal detection threshold and minimum detection error probability, we first derive the detection error probability at Willie given in the following Theorem.

Theorem 3.1: Under the CJ and RRS schemes, the detection error probability ζ at Willie can be determined as

$$\zeta = \begin{cases} 1 + \frac{\Gamma(l)}{(l-1)!} - \left(\frac{P_T}{P_T - P_J}\right)^l \exp\left(\frac{\sigma_W^2 - \lambda}{P_T}\right), & \text{if } \lambda \geq \sigma_W^2 \\ 1, & \text{otherwise} \end{cases} \quad (4)$$

where l denotes the number of friendly jammers and gamma function $\Gamma(l)$ is given by

$$\Gamma(l) = \int_0^\infty x^{(l-1)} e^{-x} dx. \quad (5)$$

where $x \sim \Gamma(l, a)$, $a = (\lambda - \sigma_W^2)/P_J$.

Proof 3.1: Based on the definition of detection error probability, we have

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}. \quad (6)$$

We first determine \mathbb{P}_{FA} . We use l to denote the number of friendly jammers, and then we have

$$\begin{aligned} \mathbb{P}_{FA} &= P\left(\sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 \geq \lambda\right) \\ &= P\left(\sum_{i=0}^l |h_{J_i W}|^2 \geq \frac{\lambda - \sigma_W^2}{P_J}\right) \\ &= \int_{\left(\frac{\lambda - \sigma_W^2}{P_J}\right)}^\infty f_{\sum_{i=0}^l |h_{J_i W}|^2}(x) dx. \end{aligned} \quad (7)$$

Since the probability density function (PDF) of the random variable $|h_{J_i W}|^2$ is given by

$$f_{|h_{J_i W}|^2}(x) = e^{-x}, \text{ if } 0 < x < \infty \quad (8)$$

using the convolution theorem, the PDF of $\sum_{i=0}^l |h_{J_i W}|^2$ can be determined as

$$f_{\sum_{i=0}^l |h_{J_i W}|^2}(x) = \frac{1}{(l-1)!} x^{(l-1)} e^{-x}, \text{ if } 0 < x < \infty \quad (9)$$

Thus, we obtain

$$\mathbb{P}_{FA} = \begin{cases} \frac{\Gamma(l)}{(l-1)!}, & \text{if } \lambda \geq \sigma_W^2 \\ 1, & \text{otherwise} \end{cases} \quad (10)$$

We proceed to determine \mathbb{P}_{MD} . We use Z to denote the event that there are l potential relays serving as friendly jammers. By applying the law of total probability, we have

$$\begin{aligned} \mathbb{P}_{MD} &= P(P_T |h_{k W}|^2 + \sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 < \lambda) \\ &= \sum_{l=0}^{n-1} P(P_T |h_{k W}|^2 + \sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 < \lambda | Z) P(Z) \\ &= \mathbb{E}_{|h_{k W}|^2} \left[1 - \exp\left(\frac{\sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 - \lambda}{P_T}\right) \right] \\ &= 1 - \mathbb{E}_{|h_{k W}|^2} \exp\left(\frac{\sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 - \lambda}{P_T}\right) \\ &= 1 - \exp\left(\frac{\sigma_W^2 - \lambda}{P_T}\right) \prod_{i=0}^l \mathbb{E}_{|h_{J_i W}|^2} \exp\left(\frac{P_J |h_{J_i W}|^2}{P_T}\right) \\ &= 1 - \exp\left(\frac{\sigma_W^2 - \lambda}{P_T}\right) \\ &\quad \cdot \prod_{i=0}^l \int_0^\infty \exp\left(\frac{P_J |h_{J_i W}|^2}{P_T}\right) f_{|h_{J_i W}|^2}(x) dx, \end{aligned} \quad (11)$$

where $\mathbb{E}(\cdot)$ denotes the expectation function and the conditional expectation function is used to derive \mathbb{P}_{MD} .

Substituting $f_{|h_{J_i W}|^2}(x)$ into (11), we obtain

$$\mathbb{P}_{MD} = \begin{cases} 1 - \left(\frac{P_T}{P_T - P_J}\right)^l \exp\left(\frac{\sigma_W^2 - \lambda}{P_T}\right), & \text{if } \lambda > \sigma_W^2 \\ 0, & \text{otherwise} \end{cases} \quad (12)$$

Substituting (10) and (12) into (6), (4) follows.

When $\lambda \leq \sigma_W^2$, $\zeta = 1$. This means that Willie cannot detect the transmission from Alice to Carol and the one from Carol to Bob.

Thus, we only consider the case of $\lambda > \sigma_W^2$. Taking the derivation of (4) with respect to λ , we have

$$\begin{aligned} \frac{\partial \zeta}{\partial \lambda} &= -\frac{(\lambda - \sigma_W^2)^{(l-1)} \exp\left(\frac{\sigma_W^2 - \lambda}{P_J}\right)}{P_J^2 (l-1)!} \\ &\quad + \frac{1}{P_T} \left(\frac{P_T}{P_T - P_J}\right)^l \exp\left(\frac{\sigma_W^2 - \lambda}{P_T}\right), \end{aligned} \quad (13)$$

and then we determine the second-order derivative of (4) with respect to λ as

$$\begin{aligned} \frac{\partial^2 \zeta}{\partial \lambda^2} &= -\frac{(\lambda - \sigma_W^2)^{(l-1)} \exp\left(\frac{\sigma_W^2 - \lambda}{P_J}\right)}{(\lambda - \sigma_W^2) P_J^2 (l-1)!} \\ &\quad + \frac{(\lambda - \sigma_W^2)^{(l-1)} \exp\left(\frac{\sigma_W^2 - \lambda}{P_J}\right)}{P_J^3 (l-1)!} - \frac{\left(\frac{P_T}{P_T - P_J}\right)^l \exp\left(\frac{\sigma_W^2 - \lambda}{P_T}\right)}{P_T^2}. \end{aligned} \quad (14)$$

To reduce the negative effect of P_J on legal receivers, we consider P_T is much larger than P_J , and thus $\lambda - \sigma_W^2$ should be larger than P_J . Then, we have $\frac{\partial^2 \zeta}{\partial \lambda^2} > 0$. Thus, the detection error probability ζ is convex.

Then, by solving the $\frac{\partial \zeta}{\partial \lambda} = 0$, the optimal threshold λ^* can be determined as

$$\lambda^* = \exp\left(\frac{1}{l-1}(\phi + \rho + \varsigma) + \sigma_W^2\right), \quad (15)$$

where $\phi = \ln\left(\frac{P_T}{P_T - P_J}\right)$, $\varsigma = \ln\left(\frac{P_J^2 \Gamma(l)}{P_T}\right)$, and $\rho = (1 - l)\text{LambertW}\left(\frac{(P_J - P_T)\left(\frac{P_T}{P_J - P_T}\right)^l P_J^2 \Gamma(l)}{P_J P_T (l-1)}\right)^{\frac{1}{l-1}}$.

By substituting λ^* into (4), we obtain the minimum detection error probability $\zeta^* = \zeta(\lambda^*)$.

C. Covert Rate Modeling

To model the fundamental covert rate performance, we first determine the transmission outage probability from Alice to Bob. The transmission outage means that the received signal strength at the receiver Carol/Bob is smaller than its required threshold θ so that the receiver cannot successfully recover the original message.

We derive the transmission outage probability in the following Theorem.

Theorem 3.2: We use P_{to} to denote the transmission outage probability. Then, we have

$$P_{to} = 1 - \exp\left(-\frac{\theta(\sigma_C^2 + \sigma_B^2)}{P_T}\right) \left[\frac{1 - e^{(-\alpha(1+K))}}{(1+K)(1-e^{-\alpha})}\right]^{2n-2}, \quad (16)$$

where $K = \theta P_J / P_T$.

Proof 3.2: In our concerned two-hop wireless network, if the transmission is not an outage, each of the two transmissions from Alice to Carol and from Carol to Bob cannot be an outage. Thus, the transmission outage probability P_{to} is given by

$$\begin{aligned} P_{to} &= P(\text{SIR}_{AC} < \theta \cup \text{SIR}_{CB} < \theta) \\ &= 1 - P(\text{SIR}_{AC} \geq \theta \cap \text{SIR}_{CB} \geq \theta), \end{aligned} \quad (17)$$

where the signal-to-noise SIR_{AC} at C is expressed as

$$\text{SIR}_{AC} = \frac{P_T |h_{AC}|^2}{\sum_{J_i} P_J |h_{J_i C}|^2 + \sigma_C^2}, \quad (18)$$

and the signal-to-noise SIR_{CB} at B is expressed as

$$\text{SIR}_{CB} = \frac{P_T |h_{CB}|^2}{\sum_{J_i} P_J |h_{J_i B}|^2 + \sigma_B^2}. \quad (19)$$

Here, σ_C^2 and σ_B^2 represent the noise power.

Since the two events $\text{SIR}_{AC} < \theta$ and $\text{SIR}_{CB} < \theta$ are independent of each other, we rewrite (17) as

$$P_{to} = 1 - P(\text{SIR}_{AC} \geq \theta)P(\text{SIR}_{CB} \geq \theta). \quad (20)$$

To solve (20), we need to determine the cumulative distribution function of $|h_{J_i C}|^2$. According to the conditional probability formula, if variable $x < \alpha$, we have

$$\begin{aligned} F_{|h_{J_i C}|^2}(x) &= P(|h_{J_i C}|^2 < x | |h_{J_i C}|^2 < \alpha) \\ &= \frac{P(|h_{J_i C}|^2 < x, |h_{J_i C}|^2 < \alpha)}{P(|h_{J_i C}|^2 < \alpha)} \\ &= \frac{P(|h_{J_i C}|^2 < x)}{P(|h_{J_i C}|^2 < \alpha)} \\ &= \frac{1 - e^{-x}}{1 - e^{-\alpha}}. \end{aligned} \quad (21)$$

By taking the derivative of the cumulative distribution function, we obtain the PDF of $|h_{J_i C}|^2$ as

$$f_{|h_{J_i C}|^2}(x) = \begin{cases} \frac{e^{-x}}{1 - e^{-\alpha}}, & \text{if } 0 \leq x \leq \alpha \\ 0, & \text{if } x > \alpha \end{cases} \quad (22)$$

Then, we have

$$\begin{aligned} P(\text{SIR}_{AC} \geq \theta) &= P\left[|h_{AC}|^2 \geq \frac{\theta(\sum_{i=0, J_i \neq C}^{n-1} P_J |h_{J_i C}|^2 + \sigma_C^2)}{P_T}\right] \\ &= \mathbb{E}\left[\exp\left(-\frac{\theta(\sum_{i=0, J_i \neq C}^{n-1} P_J |h_{J_i C}|^2 + \sigma_C^2)}{P_T}\right)\right] \\ &= \exp\left(-\frac{\theta \sigma_C^2}{P_T}\right) \prod_{i=0, J_i \neq C}^{n-1} \mathbb{E}\left[\exp\left(-\frac{\theta P_J |h_{J_i C}|^2}{P_T}\right)\right] \\ &= \exp\left(-\frac{\theta \sigma_C^2}{P_T}\right) \left[\frac{1 - e^{(-\alpha(1+K))}}{(1+K)(1-e^{-\alpha})}\right]^{n-1}, \end{aligned} \quad (23)$$

where $K = \theta P_J / P_T$.

Similarly, we have

$$P(\text{SIR}_{CB} \geq \theta) = \exp\left(-\frac{\theta \sigma_B^2}{P_T}\right) \left[\frac{1 - e^{(-\alpha(1+K))}}{(1+K)(1-e^{-\alpha})}\right]^{n-1}. \quad (24)$$

Substituting (23) and (24) into (20), we obtain (16).

Based on the P_{to} , we obtain the covert rate R_{AB} from Alice to Bob as follows.

$$R_{AB} = (1 - P_{to}) \min\{R_{AC}, R_{CB}\}, \quad (25)$$

where the achievable covert rate R_{AC} from Alice to Carol is expressed as $R_{AC} = \log_2(1 + \text{SIR}_{AC})$, and the achievable rate R_{CB} from Carol to Bob is expressed as $R_{CB} = \log_2(1 + \text{SIR}_{CB})$.

D. Covert Rate Maximization

Our goal is to maximize the covert rate R_{AB} while maintaining a high detection error probability at Willie. It can be formulated as the following optimization problem.

$$\text{Maximize } R_{AB} \quad (26a)$$

$$\text{s.t. } \zeta^*(P_T) \geq 1 - \varepsilon_c, \quad (26b)$$

$$P_T \leq P_{max}, \quad (26c)$$

$$\varepsilon_c \in (0, 1), \quad (26d)$$

where ε_c represents the covert requirement, (26b) represents the covert constraint, and (26c) represents the range of the transmit power P_T . The objective function of the optimization problem is an increasing function with respect to the covert transmit power, so the covert rate can be maximized by finding the optimal covert transmit power that satisfies the constraints. It is difficult to solve for the extreme value of ζ by substituting λ^* back into (4) because of the expression (15) includes Lambert-W and gamma functions. Therefore, the closed-form expression for the optimal covert transmit power is unavailable with the optimization conditions such that we cannot find an analytical solution of the optimization problem. To this end, we employ an iterative algorithm based on the stochastic gradient descent (SGD) method as shown in Algorithm 1. Note that the ζ^* and the corresponding optimal covert transmit power within the maximum power constraint are calculated in each iteration based on the results of previous loop, and then we can get the maximum covert rate.

IV. COVERT RATE UNDER A JOINT CJ AND MMRS SCHEME

A. Detection At Willie

Based on the two hypotheses introduced in the Section III-E, at a time slot, the received signal y_W at Willie from Alice/Carol under the joint CJ and MMRS scheme is given by

$$y_W = \begin{cases} \sum_{J_i} \sqrt{P_J} h_{J_i W} x_j + n_W, & \text{if } H_0 \text{ is true} \\ \sqrt{P_T} h_{k W} x_k + \sum_{J_i} \sqrt{P_J} h_{J_i W} x_j + n_W, & \text{if } H_1 \text{ is true} \end{cases} \quad (27)$$

where x_j is the signal transmitted by a jammer i , x_k is the signal transmitted by Alice/Carol, $k \in \{A, C\}$, P_T is the transmit power of Alice/Carol, and n_W is the AWGN at Willie with variance σ_W^2 , i.e., $n_W \sim \mathcal{CN}(0, \sigma_W^2)$.

Based on (2) and (27), the average received power Y at Willie can be determined as

$$Y = \begin{cases} \sum_{J_i} P_J |h_{J_i W}|^2 + \sigma_W^2, & \text{if } H_0 \text{ is true} \\ \frac{\theta(\sum_{J_i} P_J |h_{J_i C}|^2 + \sigma_C^2) |h_{A,W}|^2}{|h_{AC}|^2} + \sum_{J_i} P_J |h_{J_i W}|^2 + \sigma_W^2. & \text{if } H_1 \text{ is true} \end{cases} \quad (28)$$

B. Optimal Detection Threshold and Minimum Detection Error Probability

To determine the optimal detection threshold and minimum detection error probability, we first derive the detection error probability at Willie given in the following Theorem.

Theorem 4.1: Under the CJ and MMRS schemes, the detection error probability ζ at Willie can be determined as

$$\zeta = \begin{cases} 1 + \frac{\Gamma(l)}{(l-1)!} \\ - \left(\frac{1}{1-\varphi} \right)^l \exp \left[\frac{\varphi(\sigma_W^2 - \lambda)}{P_J} \right], & \text{if } \lambda \geq \sigma_W^2 \\ 1, & \text{otherwise} \end{cases} \quad (29)$$

where l is the number of friendly jammers and $\varphi = (P_J |h_{AC}|^2) / \theta(\sum_{i=0}^l P_J |h_{J_i C}|^2 + \sigma_C^2)$.

Proof 4.1: Based on the definition of detection error probability, we have

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}. \quad (30)$$

Similar to the derivation process of \mathbb{P}_{FA} under the RRS scheme, \mathbb{P}_{FA} under the MMRS scheme can be determined as

$$\mathbb{P}_{FA} = \begin{cases} \frac{\Gamma(l)}{(l-1)!}, & \text{if } \lambda \geq \sigma_W^2, \\ 1. & \text{otherwise} \end{cases} \quad (31)$$

We use Z to denote the event that there are l potential relays serving as friendly jammers. Applying the law of total probability, \mathbb{P}_{MD} is determined as

$$\begin{aligned} \mathbb{P}_{MD} &= P(P_T |h_{AW}|^2 + \sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 < \lambda) \\ &= \sum_{l=0}^{n-1} P(P_T |h_{AW}|^2 + \sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 < \lambda | Z) P(Z) \\ &= \sum_{l=0}^{n-1} P \left(\frac{\theta(\sum_{i=0}^l P_J |h_{J_i C}|^2 + \sigma_C^2)}{|h_{AC}|^2} |h_{AW}|^2 + \sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 < \lambda \right) P(Z) \\ &= \mathbb{E}_{|h_{J_i W}|^2} \left[1 - \exp \left(\frac{(\sum_{i=0}^l P_J |h_{J_i W}|^2 + \sigma_W^2 - \lambda) |h_{AC}|^2}{\theta(\sum_{i=0}^l P_J |h_{J_i C}|^2 + \sigma_C^2)} \right) \right] \\ &= 1 - \exp \left(\frac{(\sigma_C^2 - \lambda)\varphi}{P_J} \right) \prod_{i=0}^l \mathbb{E}_{|h_{J_i W}|^2} \exp \left(\sum_{i=0}^l |h_{J_i W}|^2 \varphi \right) \\ &= 1 - \exp \left(\frac{(\sigma_C^2 - \lambda)\varphi}{P_J} \right) \prod_{i=0}^l \int_0^\infty \exp(-|h_{J_i W}|^2 \varphi) f_{|h_{J_i W}|^2}(x) dx, \end{aligned} \quad (32)$$

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

The covert communication can be achieved if $\zeta \geq 1 - \varepsilon$ for any $\varepsilon > 0$. Similarly, when $\lambda \leq \sigma_W^2$, $\zeta = 1$. This means that Willie cannot detect the transmission from Alice to Carol and the one from Carol to Bob. Hence, we consider the case of $\lambda > \sigma_W^2$. Take the derivation of (29) with respect to λ , we have

$$\begin{aligned} \frac{\partial \zeta}{\partial \lambda} &= - \frac{(\lambda - \sigma_W^2)^{(l-1)} \exp \left(\frac{\sigma_W^2 - \lambda}{P_J} \right)}{P_J^2 (l-1)!} \\ &\quad + \frac{\varphi}{P_J} \left(\frac{1}{1-\varphi} \right)^l \exp \left[\frac{\varphi(\sigma_W^2 - \lambda)}{P_J} \right]. \end{aligned} \quad (33)$$

We further determine the second-order derivatives of (29) with respect to λ as

$$\begin{aligned} \frac{\partial^2 \zeta}{\partial^2 \lambda} &= -\frac{(\lambda - \sigma_W^2)^{(l-1)} \exp(\frac{\sigma_W^2 - \lambda}{P_J})}{(\lambda - \sigma_W^2) P_J^2 (l-1)!} \\ &+ \frac{(\lambda - \sigma_W^2)^{(l-1)} \exp(\frac{\sigma_W^2 - \lambda}{P_J})}{P_J^3 (l-1)!} - \frac{\varphi^2 (\frac{1}{1-\varphi})^l \exp(\frac{\varphi(\sigma_W^2 - \lambda)}{P_T})}{P_T^2}. \end{aligned} \quad (34)$$

Similar to the RRS scheme, the detection error probability ζ is convex. Then, by solving $\frac{\partial \zeta}{\partial \lambda} = 0$, the optimal threshold λ^* can be determined as

$$\lambda^* = \exp(\text{RootOF}(\delta - \xi + \gamma) + \sigma_W^2), \quad (35)$$

where $\xi = \ln\left(\frac{\Gamma(l) P_J^3 \varphi^2}{P_T^2 (\exp(Q) + P_J - P_T l)}\right) P_T P_J$, $\gamma = \varphi \exp(Q) P_J - 2 P_J P_T Q - P_T \exp(Q)$, $\delta = -\ln\left(-\frac{1}{\varphi-1}\right) l P_T P_J + P_T P_J Q l$, $\text{RootOF}(\text{expr})$ represents all the roots of expr , and Q denotes the complex constant in the solution. Then, we can obtain the optimal threshold λ^* by solving the minimum value of ζ , i.e., $\zeta^* = \zeta(\lambda^*)$.

C. Covert Rate Modeling

Similarly, to model the fundamental covert rate performance, we first determine the transmission outage probability from Alice to Bob. We derive the transmission outage probability under this relay selection scheme in the following Theorem.

Theorem 4.2: We use P_{sto} to denote the transmission outage probability. Then, we have

$$\begin{aligned} P_{sto} &= P(\min\{\text{SIR}_{AC}, \text{SIR}_{CB}\} < \theta) \\ &= U k \exp\left(\frac{-\theta \sigma_C^2}{P_T}\right) \left[\frac{1 - e^{-(1+z)\alpha}}{(1 - e^{-\alpha})(1+z)}\right]^l \\ &+ U(k-1) \exp\left(\frac{-2k\theta \sigma_C^2}{P_T}\right) \left[\frac{1 - e^{-(2kz+1)\alpha}}{(1 - e^{-\alpha})(2kz+1)}\right]^l \end{aligned} \quad (36)$$

where $z = \theta P_J / P_T$, $U = \sum_{k=0}^n \binom{n}{k} (-1)^k \left(\frac{1}{2k-1}\right)$.

Proof 4.2: For each relay R_k where $k = 1, 2, \dots, n$, let $M_k = \min\{|h_{AR_k}|^2, |h_{R_k B}|^2\}$, and D_k denote the event that Alice select the relay. We then have this expression

$$D_k \triangleq \bigcap_{v=1, v \neq k}^n (M_v \leq M_k),$$

where M_k is an exponential random variable with mean $1/2$.

Next, if $M_k = |h_{AR_k}|^2$, then based on the previous work [31] we have

$$\begin{aligned} P(|h_{AC}|^2 < x) &= \int_0^x n e^{-t} (2e^{-t} - e^{-x}) (1 - e^{-2t})^{n-1} dt \\ &= (1 - e^{-2x})^n - n e^{-x} \int_0^x e^{-t} (1 - e^{-2t})^{n-1} dt \\ &= \sum_{k=0}^n \binom{n}{k} (-1)^k \frac{k e^{-x} + (k-1) e^{-2kx}}{2k-1}. \end{aligned} \quad (37)$$

The transmission outage probability can be expressed as

$$\begin{aligned} P_{sto} &= P(\text{SIR}_{AC} < \theta) \\ &= U k \exp\left[-\frac{\theta(P_J \sum_{i=0}^l |h_{J_i C}|^2 + \sigma_C^2)}{P_T}\right] \\ &+ U(k-1) \exp\left[-2k \frac{\theta(P_J \sum_{i=0}^l |h_{J_i C}|^2 + \sigma_C^2)}{P_T}\right] \\ &= U k \exp\left(\frac{-\theta \sigma_C^2}{P_T}\right) \prod_{i=0}^l \mathbb{E}_{|h_{J_i C}|^2} \left[\exp(-z \sum_{i=0}^l |h_{J_i C}|^2)\right] \\ &+ U(k-1) \exp\left(\frac{-2k\theta \sigma_C^2}{P_T}\right) \\ &\cdot \prod_{i=0}^l \mathbb{E}_{|h_{J_i C}|^2} \left[\exp(-2kz \sum_{i=0}^l |h_{J_i C}|^2)\right], \end{aligned} \quad (38)$$

(36) can be obtained.

We obtain the covert rate R'_{AB} from Alice to Bob under the MMRS scheme as follows.

$$R'_{AB} = (1 - P_{sto}) \min\{R_{AC}, R_{CB}\}, \quad (39)$$

where the achievable covert rate R_{AC} from Alice to Carol is expressed as $R_{AC} = \log_2(1 + \text{SIR}_{AC})$, and the achievable rate R_{CB} from Carol to Bob is expressed as $R_{CB} = \log_2(1 + \text{SIR}_{CB})$.

Although it is first determined that the link meets the transmit condition before sending the covert messages, then the covert transmission itself will not occur outage, but the setting of α affects the probability of the link satisfying the requirement in a time slot. We should ensure that within a certain period of time, more time slots are sent for covert messages. Hence, we should promise that covert transmission probability must be greater than a threshold to make Alice have more opportunities to send covert messages.

D. Covert Rate Maximization

The objective of covert rate maximization is to maximize the covert rate R'_{AB} while maintaining an arbitrary high detection error probability at Willie. It can be formulated as the following optimization problem.

$$\text{Maximize } R'_{AB} \quad (40a)$$

$$\text{s.t. } \zeta^*(P_T) \geq 1 - \varepsilon_c, \quad (40b)$$

$$P_T \leq P_{max}, \quad (40c)$$

$$\varepsilon_c \in (0, 1), \quad (40d)$$

where ε_c is the covertness requirement. (40b) represents covert constraint, and (40c) represents transmit power constraint for source and relay. We also use an iterative algorithm based on SGD method illustrated in Algorithm 1 to solve the optimization problem in (40).

V. NUMERICAL RESULTS

This section first validates our theoretical models and then explores the impact of system parameters on covert rate performance.

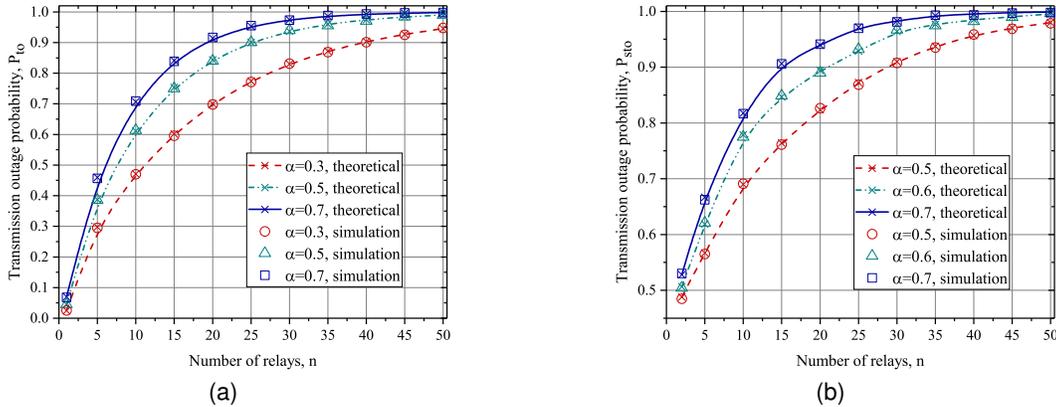


Fig. 3. Transmission outage probability validation.(a)Transmission outage probability validation under RRS. (b)Transmission outage probability validation under MMRS.

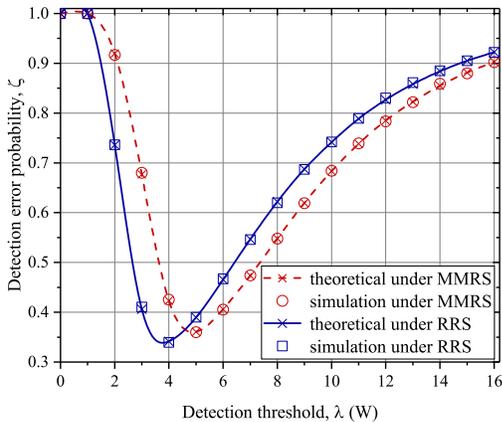


Fig. 4. Detection error probability validation.

A. Model Validation

To ensure the efficiency of our theoretical covert rate models in (25) and (39), we only need to validate the transmission outage probabilities under the RSS and MMRS schemes.

Towards this end, we compare the simulation results with the theoretical ones under these two schemes. Specifically, the simulated transmission outage probability is calculated as the average value of 10^5 independent simulations. Here, the simulated probability equals the ratio of the number of transmission outages to the total number of transmissions. For the scenario with the setting of the number of relay $n = 50$, the threshold of the cooperative jamming $\alpha = \{0.3, 0.5, 0.7\}$, transmission power of Alice and Carol $P_T = 5$ W, outage threshold $\theta = 1$, jamming power $P_J = 1$ W and noise $\sigma_C^2 = \sigma_B^2 = -5$ dB. We can see from Fig.3 that for each α , the theoretical transmission outage probability almost matches with the simulation one under these two schemes, indicating that our theoretical model can well capture the covert rate performance under each scheme. Another observation indicates that as the number of relays increases, the transmission outage probability increases. Based on the cooperative jamming scheme introduced in Section III-D, we know that as the number of relays or α increases will result in more relays satisfying the conditions

of this scheme to act as cooperative jamming relays and then transmitting jamming signals, which increases the noise on the legitimate receiver as well. This will lead to the decrease of the SIRs at the relay Carol and the destination Bob, which further leads to the increase of transmission outage probability.

To achieve maximum covert rate based on the optimization problems of (26) and (40), we now validate the theoretical detection error probability ζ under the two relay selection schemes via the comparison between theoretical results and simulation ones, where each simulated value is calculated as the average value of 10^5 independent simulations. For the scenario of $n = 10$, $P_T = 5$ W, $\alpha = 0.3$, $\theta = 1$, $P_J = 1$ W, $|h_{A,C}|^2 = |h_{C,B}|^2$ and $\sigma_W^2 = -5$ dB, We can observe from Fig. 4 that the theoretical ζ almost matches the simulation one under each scheme. This demonstrates that our theoretical results can well predict the simulation results under these two relay selection schemes.

We can also observe from Fig.4 that as λ increases, ζ first decreases and then increases under both the schemes. This can be explained as follows. We know that ζ is the sum of false alarm probability \mathbb{P}_{FA} and missed detection probability \mathbb{P}_{MD} . Based on our theoretical analysis of these two probabilities, we know that \mathbb{P}_{FA} is a decreasing function of λ while \mathbb{P}_{MD} is an increasing function. As λ is relatively small, the former one dominates ζ , which leads to the decrease of ζ with λ . On the other hand, as λ further increases, the latter one dominates ζ , which leads to the increase of ζ .

There exists a minimum ζ corresponding to the maximum transmission power limit of P_T , which means that Willie has the strongest detection ability to detect the transmission of two hops.

B. Theoretical Analysis of Covert Performance

We first explore the impact of P_T on the covert rate under these two relay selection schemes. We summarize the numerical results in Fig.5 with the setting of $\alpha = \{0.3, 0.5, 0.7\}$ and $\sigma_C^2 = \sigma_B^2 = -5$ dB. It can be observed from Fig.5 that as P_T increases, the covert rates increase under both the schemes. This is because the increase of P_T leads to the increase of the SIR at the receivers Carol and Bob. A careful

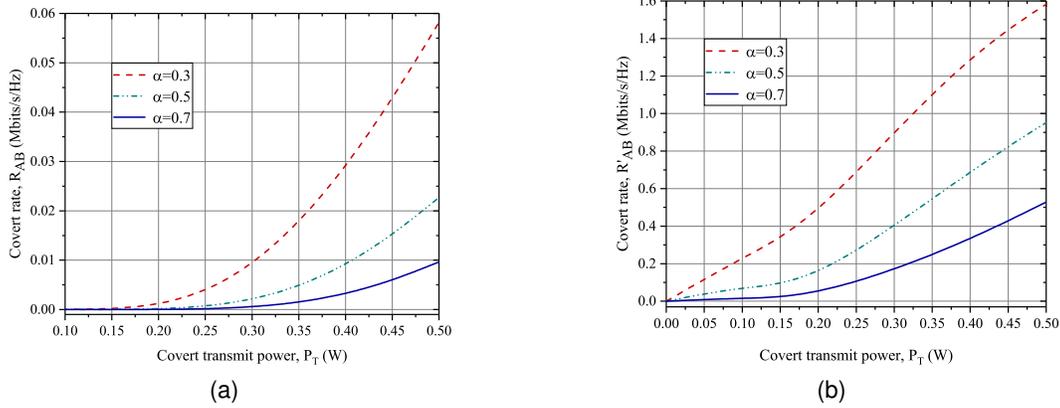


Fig. 5. The impact of P_T on covert rate. (a) R_{AB} vs. P_T . (b) R'_{AB} vs. P_T .

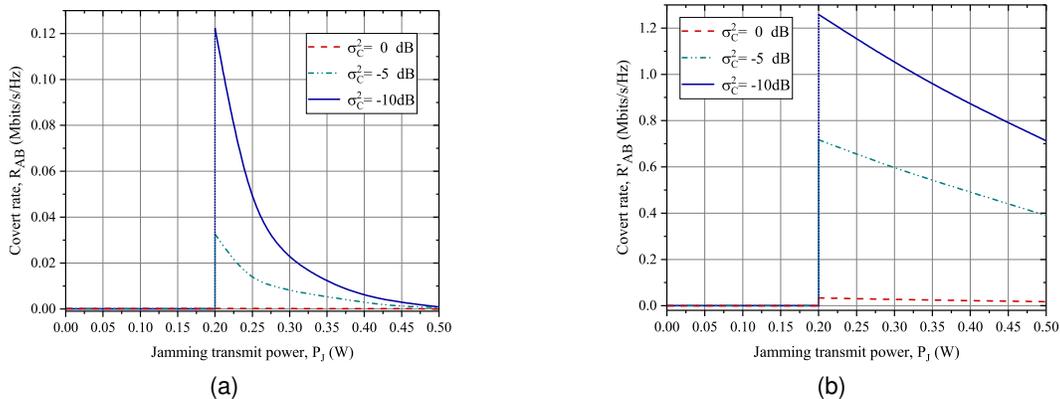


Fig. 6. The impact of P_J on covert rate. (a) R_{AB} vs. P_J . (b) R'_{AB} vs. P_J .

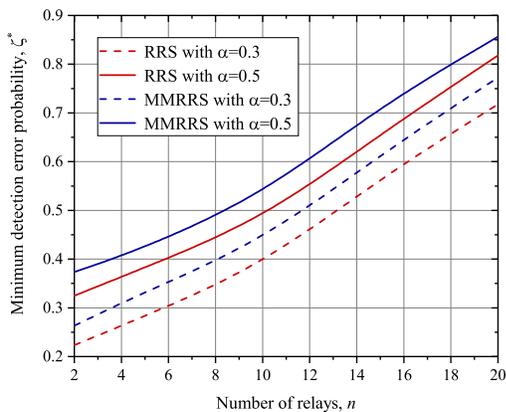


Fig. 7. The impact of n on minimum detection error probability.

observation from Fig.5 indicates that for each fixed P_T , as α further increases, the covert rate will decrease. The reason for this phenomenon is that the number of relays satisfying the selection conditions of the jammer increases, which increases the total jamming power, leading to a decrease in the SIRs at the receiver. We can also observe that for each fixed P_T , the covert rate R_{AB} under the RRS scheme in Fig.5 (a) is lower than that R'_{AB} under the MMRS scheme in Fig.5 (b).

This is due to the following reason. The channel quality of the two-hop transmissions under the RRS scheme is usually lower than that under the MMRS scheme, which means that the transmission outage probability under the former is also usually higher than that under the latter.

To investigate the impact of jamming transmit power P_J on the covert rates under the two schemes, we summarize in Fig.6 how the covert rates vary with P_J with the setting of $n = 10$, $\alpha = 0.3$ and $\sigma_C^2 = \sigma_B^2 = \{0, -5, -10\}$ dB. We can see from Fig.6 that as P_J increases, the covert rate first increases and then decreases under each scheme. This is because increasing P_J has a two-fold effect on the covert rate. It can confuse the detection of Willie, which leads to an increase in the covert rate. Meanwhile, it can also interfere with the source-relay-destination links, which leads to a decrease in the covert rate. As P_J is relatively small, the former dominates the covert rate, and thus the covert rate increases with the increase of P_J . As P_J becomes larger, the latter dominates the covert rate, and thus the covert rate decreases as P_J further increases. Therefore, we can set a proper P_J to improve the covert rate performance under each scheme.

C. Performance Optimization and Comparison

By optimizing the covert transmit power P_T , we explore the impact of number of relays n on the minimum detection

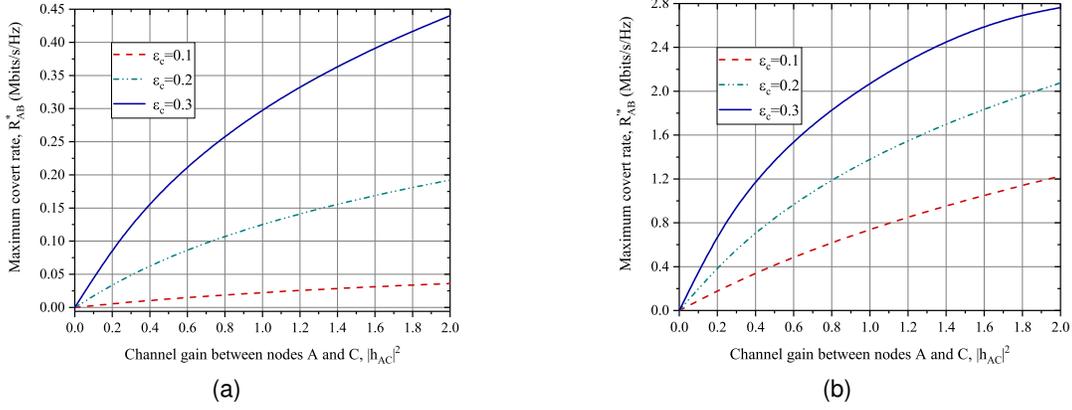


Fig. 8. The impact of $|h_{AC}|^2$ on maximum covert rate. (a) R_{AB}^* vs. $|h_{AC}|^2$. (b) R_{AB}^* vs. $|h_{AC}|^2$.

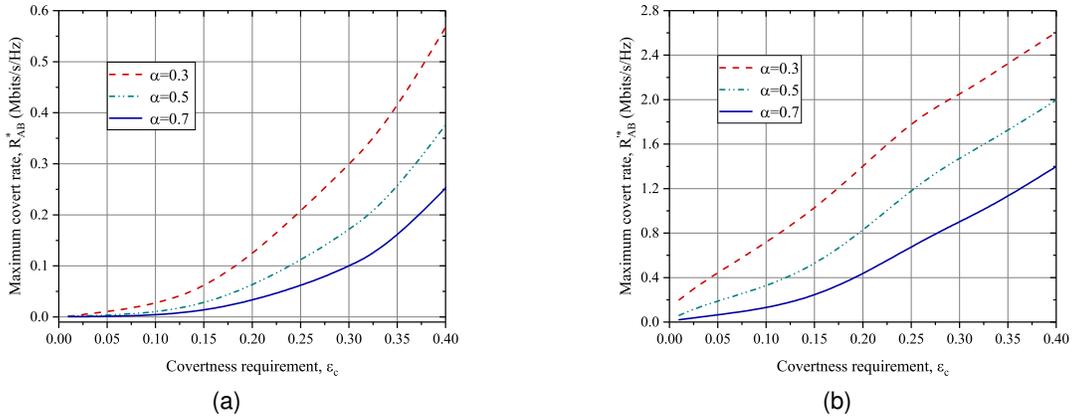


Fig. 9. The impact of ϵ_c on maximum covert rate. (a) R_{AB}^* vs. ϵ_c . (b) R_{AB}^* vs. ϵ_c .

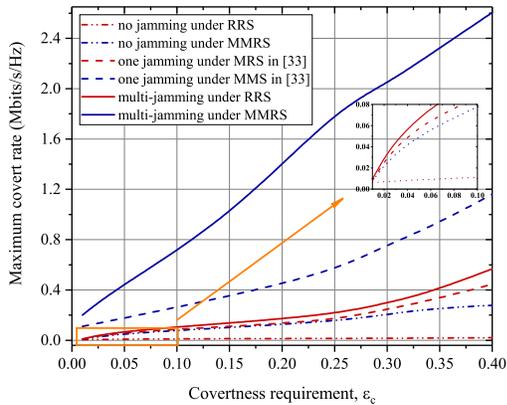


Fig. 10. Maximum covert rate comparison.

error probability under the two relay selection schemes as shown in Fig.7, for the setting of $n \in [2, 20]$, $\alpha = \{0.3, 0.5\}$, and $\sigma_W^2 = -5$ dB. We can observe from the Fig.7 that as the number of relays increases, the minimum detection error probability at warden increases under both scenarios, and this phenomenon also occurs to α as well. This implies that increasing the number of jammers can enhance the covertness performance of such system.

To further explore the impact of channel gain on the maximum covert rates under the two schemes, we summarize in Fig.8 how the maximum covert rates vary with channel gain between nodes Alice and Carol $|h_{AC}|^2$ with the setting of $n = 10$, $\alpha = 0.3$, $\epsilon_c = \{0.1, 0.2, 0.3\}$ and $\sigma_C^2 = \sigma_B^2 = \{-5, -10\}$ dB. We can see that a larger channel gain leads to an increase of maximum covert rates. This is because a larger channel gain implies a more reliable transmission link and thus a smaller probability of transmission outage.

To investigate the impact of ϵ_c on the maximum covert rates under the two relay selection schemes as shown in Fig.9. For the setting of $n = 10$, $\alpha = \{0.3, 0.5, 0.7\}$, and $\sigma_C^2 = \sigma_B^2 = -5$ dB, we can observe from Fig.9 that as ϵ_c increases, the maximum covert rates increase under both the two schemes. This is because the increase of ϵ_c is equivalent to the increase of the probability with which the two-hop transmissions are detected by Willie. This means that P_T can increase, which leads to the increase of the maximum covert rates.

Finally, we conduct the performance comparison between the two relay selection schemes with multi-jamming signals, no jamming signals, and those with one jamming signal [33] as shown in Fig.10 for the setting of $n = 10$, $\alpha = 0.3$. It can be seen from Fig.10 that the maximum covert rate under each scheme with jamming signals is larger than that

with no jamming signal. This can be explained as follows. With jamming signals, the covertness requirement constraint is easier to be satisfied than that with no jamming signal. Thus, the covert transmit power with jamming signals is larger than that with no jamming signal, which leads to a larger maximum covert rate with jamming signals than with no jamming signal. We can also observe that the schemes with multi-jamming nodes can enhance the maximum covert rate compared to the schemes with one jamming node (i.e., MRS, MMS) proposed in [33]. The reason behind the phenomena is similar to the above one. Fig. 10 also illustrates that for each fixed setting of covertness requirement ε_c , the maximum covert rate under MMRS is larger than that under RRS.

VI. CONCLUSION

This paper explored the covert communications in a wireless relay system, where two joint CJ and relay selection schemes are proposed for improving covert performance. Based on each joint scheme, we developed a theoretical model to characterize the covert rate, and further maximize the covert rate by optimal transmit power control. Finally, simulation/numerical results were provided to validate our theoretical models. Specifically, increasing the covert transmit power can enhance the covert rate performance under each joint scheme.

REFERENCES

- [1] C. Gao, *Protocol Design and Performance Analysis for Covert Communications in Relay-Assisted Wireless Systems*. Doctoral Thesis. Future University Hakodate, 2021.
- [2] P. Zhang, L. Li, K. Niu, Y. Li, G. Lu, and Z. Wang, "An intelligent wireless transmission toward 6G," *Intelligent and Converged Networks*, vol. 2, no. 3, pp. 244–257, 2021.
- [3] 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, Oct. 2019.
- [4] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3542–3553, Jul. 2019.
- [5] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE journal on selected areas in communications*, vol. 31, no. 9, pp. 1921–1930, 2013.
- [6] —, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE International Symposium on Information Theory Proceedings*, pp. 448–452, July. 2012.
- [7] B. A. Bash, D. Goeckel, and D. Towsley, "LPD communication when the warden does not know when," in *Proc. IEEE International Symposium on Information Theory*, pp. 606–610, June. 2014.
- [8] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.
- [9] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.
- [10] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, pp. 2229–2233, 2016.
- [11] S. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2310–2319, 2018.
- [12] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," pp. 1–5, 2017.
- [13] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Communications Letters*, vol. 20, no. 2, pp. 236–239, 2016.
- [14] J. Hu, S. Yan, X. Zhou, S. Feng, and J. Li, "Covert wireless communications with channel inversion power control in Rayleigh fading," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, 2019.

Algorithm 1: Iterative Optimal Covert Transmit Power Algorithm

Input: Detection error probability ζ , step width ν , tolent value of SGD $\eta = 0.001$, covert requirement ε_c , $P_T \in [0, P_{max}]$, P_J , the number of jammers l , random variable $t_k \in (0, 10]$.

Output: Minimum detection error probability ζ^* , the corresponding optimal covert transmit power P_T^* and maximum covert rate R_{AB}^* .

- 1: Initialization: Set $\eta = 0.001$, $P_J = 1$, $\lambda_1 = 0.01$;
- 2: Calculate stochastic vector $g = \nabla\zeta(\lambda)$;
- 3: **for** $v = 1, 2, \dots$ **do**
 - $P_{Tv} = 0$;
 - 4: **for** $k = 1, 2, \dots$ **do**
 - Set $\nu_k = 1/k$;
 - Generate a realization random variable t_k ;
 - Set the new iterate as $\lambda_{k+1} = \lambda_k - \nu_k g(t_k)$;
 - 5: **while** $\nu_k g(t_k) \leq \eta$ **do**
 - Calculate $\zeta^* = \zeta(\lambda_{k+1})$;
 - if** $\zeta^* \geq 1 - \varepsilon_c$ **then**
 - Save λ_{k+1}, P_{Tv} ;
 - $P_T^* = P_{Tv}$;
 - Calculate maximum covert rate R_{AB}^* by substituting P_T^* back into (25) ;
 - end**
 - 6: Update covert transmit power
 - $P_{T(v+1)} = P_{Tv} + 0.1$;
 - 7: **if** $P_{T(v+1)} > P_{max}$ **then**
 - break**;
 - end**
- end**

- [15] 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. 12432–12436, 2019.
- [16] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, p. 7252–C7267, Nov. 2018.
- [17] 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.
- [18] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a Poisson field of interferers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6005–6017, 2018.
- [19] 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.
- [20] W. Liang, J. Shi, Z. Tie, and F. Yang, "Performance analysis for UAV-jammer aided covert communication," *IEEE Access*, vol. 8, pp. 111394–111400, 2020.
- [21] Y. Jiang, L. Wang, and H. Chen, "Covert communications in D2D underlying cellular networks with antenna array assisted artificial noise transmission," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2980–2992, 2020.
- [22] T. X. Zheng, Z. Yang, C. Wang, Z. Li, J. Yuan, and X. Guan, "Wireless covert communications aided by distributed cooperative jamming over slow fading channels," *IEEE Transactions on Wireless Communications*, vol. 20, no. 11, pp. 7026–7039, 2021.
- [23] W. Ma, Z. Niu, W. Wang, S. He, and T. Jiang, "Covert communication

with uninformed backscatters in hybrid active/passive wireless networks: Modeling and performance analysis," *IEEE Transactions on Communications*, vol. 70, no. 4, pp. 2622–2634, 2022.

- [24] S. Yan, S. V. Hanly, and I. B. Collings, "Optimal transmit power and flying location for UAV covert wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3321–3333, Nov. 2021.
- [25] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 129–140, Jan. 2019.
- [26] H. Wu, Y. Zhang, X. Liao, Y. Shen, and X. Jiang, "On covert throughput performance of two-way relay covert wireless communications," *Wireless Networks*, pp. 1–15, 2020.
- [27] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 317–320, 2018.
- [28] 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.
- [29] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4089–4102, 2019.
- [30] M. Forouzes, 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.
- [31] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6313–6323, 2021.
- [32] Y. Su, H. Sun, Z. Zhang, Z. Lian, Z. Xie, and Y. Wang, "Covert communication with relay Selection," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 421–425, 2021.
- [33] J. Jiang, W. Yang, and R. Ma, "Joint relay and jammer selection for covert communication," in *2021 7th International Conference on Computer and Communications (ICCC)*, pp. 131–135, 2021.
- [34] Suzuki and H, "A Statistical Model for Urban Radio Propagation," *IEEE Transactions on Communications*, vol. 25, no. 7, pp. 673–680, 1977.
- [35] M. Grant and S. Boyd. (2014). CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1. [Online]. Available: <http://cvxr.com/cvx>.
- [36] E. Shi, J. Zhang, S. Chen, J. Zheng, Y. Zhang, D. W. Kwan Ng, and B. Ai, "Wireless energy transfer in RIS-aided cell-free massive MIMO systems: Opportunities and challenges," in *IEEE Communications Magazine*, vol. 60, no. 3, pp. 26–32, 2022.
- [37] C. Wang, X. Chen, Z. Xiong, C. Xing, N. Zhao and D. Niyato, "Covert communication assisted by UAV-IRS," in *IEEE Transactions on Communications*, vol. 71, no. 1, pp. 357–369, 2023.
- [38] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu and J. Li, "Achieving covert wireless communications using a full-duplex receiver," in *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.



Chan Gao received her B.S. and M.S. degrees in Xi'an University of Posts and Telecommunications, Xi'an, China, in 2014 and 2018, and Ph.D. degree in systems information science from Future University Hakodate, Japan in 2021, respectively. She is currently an assistant professor at Xi'an University of Posts and Telecommunications and is also connected with the National Engineering Research Center for Secured Wireless, Xi'an, China. Her research interest focuses on the covert communication in physical layer.



Bin Yang received his Ph.D. degree in systems information science from Future University Hakodate, Japan in 2015. He was a research fellow with the School of Electrical Engineering, Aalto University, Finland, from Nov. 2019 to Nov. 2021. He is currently a professor with the School of Computer and Information Engineering, Chuzhou University, China. His research interests include unmanned aerial vehicle networks, cyber security and Internet of Things.



Dong Zheng received an M.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1988, and a Ph.D. degree in communication engineering from Xidian University, in 1999. He was a professor in the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a professor at Xi'an University of Posts and Telecommunications and is also connected with the National Engineering Laboratory for Wireless Security, Xi'an, China. He has published over 100 research articles including CT-RSA, IEEE Transactions on Industrial Electronics, Information Sciences. His research interests include cloud computing security, public key cryptography, and wireless network security.



Xiaohong Jiang received his B.S., M.S. and Ph.D. degrees in 1989, 1992, and 1999 respectively, all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from Feb. 2005 to Mar. 2010. Dr. Jiang's research interests include computer communications networks, mainly wireless networks and optical networks, network security, routers/switches design, etc. He has published over 300 technical papers at premium international journals and conferences, which include over 70 papers published in top IEEE journals and top IEEE conferences, like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE INFOCOM.



Tarik Taleb received the B.E. degree (with distinction) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Professor with the Center of Wireless Communications, University of Oulu, Finland. He was a Senior Researcher and a 3GPP Standards Expert with NEC Europe Ltd., Heidelberg, Germany. He was then leading the NEC Europe Labs Team, involved with research and development projects on carrier cloud platforms, an important vision of 5G systems. His current research interests include architectural enhancements to mobile core networks (particularly 3GPP), network softwarization and slicing, mobile cloud networking, network function virtualization, software defined networking, mobile multimedia streaming, and unmanned vehicular communications.