Covert Communication in Relay-Assisted IoT Systems

Chan Gao, Bin Yang, Xiaohong Jiang, *Senior Member, IEEE*, Hiroshi Inamura, *Member, IEEE*, and Masaru Fukushi, *Member, IEEE*

***Abstract*—Internet of Things (IoT) systems are of paramount importance to provide ubiquitous wireless connectivity for smart cities. However, such systems are facing security challenges due to the broadcast and openness nature of wireless channels. This article studies the performance of covert communication under a scenario consisted of a source–destination pair, a passive warden, and multiple relays. We first propose two relay selection schemes, one is random selection and another is superior-link selection. Based on these two schemes, we then examine the transmission strategy design for the source and thus define the necessary condition that the source can transmit covert messages. We further derive the detection error probability of warden and covert capacity based on two relay selection schemes and also explore the covert capacity maximization through efficient numerical searches. Finally, numerical results are provided to illustrate our theoretical findings and the performance of covert communication in such systems. Remarkably, the superior-link selection scheme has 108% improved to the random selection scheme for the maximum covert capacity performance under the same transmission power at the source.**

***Index Terms*—Covert communication, covert performance, Internet of Things (IoT) systems, relay selection.**

I. Introduction

INTERNET of Things (IoT) systems are of paramount importance to provide ubiquitous wireless connectivity for smart cities, such as smart home, healthcare, automobile, industrial environments, etc., [1]–[4]. However, due to the broadcast and openness nature of wireless channels, there exist various security threats in IoT systems. The security in IoT systems is extremely important to guarantee the transmissions of highly sensitive data for widespread smart city applications [5], [6]. Conventional cryptography-based security techniques cannot provide strong security protection for IoT systems with the emergence of IoT devices with powerful computing capabilities [7]. Recently, physical layer security (PLS) has become an appealing security mechanism in IoT systems [8], wherein the randomness and noise of wireless channels are utilized to enhance the security of wireless transmissions. However, adversaries can still detect the existence of wireless transmissions among IoT devices, such that they can even launch attacks for IoT devices [9].

Different from the PLS mechanism, covert communication is a promising technique to prevent adversaries from detecting the existence of wireless transmissions among IoT devices. Thus, it can strongly protect the security of wireless transmissions in IoT systems [10], [11]. Specifically, the secure communications in IoT-based intelligent transport systems have played a vital role in smart cities, like the communications between vehicles and vehicles, between vehicles and infrastructure, and between vehicles and cloud servers [12], [13]. Due to its great potential to meet the security requirements in such systems, covert communication has received much attention from both academia and industry [14]. In smart cities, various multimedia devices are equipped with vehicles and infrastructure to satisfy the needs of intelligent transportation services and personalized multimedia applications [12], [13], whereby each user can send or receive highly sensitive information, such as the locations and personal preferences. To support various applications of such systems in smart cities, it is critical to study the performance of covert communication. However, the performance of covert communication still remains largely unknown in multiple relays-assisted IoT systems.

The existing works on the performance of covert communication mainly focus on the two scenarios of single hop or two hops with the help of a single relay (see Section II). The former scenario consists of a transmitter, a receiver, and a warden, while for the latter one, there is a relay besides the three nodes. These works show that the relay can significantly improve the covert performance in terms of detection error probability of warden and covert capacity. However, the above works only consider a simple scenario with no relay or a single relay. In practical IoT systems, there usually exist multiple IoT devices and a device can send information to another with the help of multiple relays. For instance, a large number of IoT devices

Manuscript received October 11, 2020; revised December 13, 2020; accepted January 6, 2021. Date of publication January 14, 2021; date of current version April 7, 2021. This work was supported in part by the Japan Society for the Promotion of Science (JSPS) under Grant 18H03235; in part by NSFC under Grant 61962033 and Grant 61702068; in part by the Anhui Province Project under Grant 201903a06020026; Grant 1808085MF165; and Grant gxgwfx2019060; in part by the Yunnan NSF Project under Grant 2018FH001-010; in part by the Shaanxi NSF Project under Grant NSSOF1900109; and in part by the CHZU NSF Project under Grant 2020qd16 and Grant zrjz2019011. *(Corresponding author: Bin Yang.)*

Chan Gao, Xiaohong Jiang, and Hiroshi Inamura are with the School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan (e-mail: gaochan001@163.com; jiang@fun.ac.jp; inamura@fun.ac.jp).

Bin Yang is with the School of Computer and Information Engineering, Chuzhou University, Chuzhou 239000, China, and also with the School of Electrical Engineering, Aalto University, 02150 Espoo, Finland (e-mail: yangbinchi@gmail.com).

Masaru Fukushi is with the Graduate School of Sciences and Technology for Innovation, Yamaguchi University, Yamaguchi 753-8511, Japan (e-mail: mfukushi@yamaguchi-u.ac.jp).

Digital Object Identifier 10.1109/JIOT.2021.3051694

can communicate with each other cooperatively through relays to construct a self-organized intelligent IoT system for accomplishing complex tasks in smart cities, such as traffic flow monitoring, healthcare monitoring, flood and natural disaster detection, vehicle communication, etc.

Recently, the work in [15] studied the covert communication performance in fixed multihop routing unmanned aerial vehicle (UAV) systems, where multiple relays are distributed equidistantly on the line from a transmitter to its receiver. This is also a simple multiple relay scenario that the transmitter cannot select an optimal relay to enhance the covert communication performance. As a result, a challenging issue of relay selection arises in IoT systems for improving the covert communication performance. To address this issue, this article proposes two relay selection schemes and studies the performance of covert communication in multiple relays-assisted IoT systems with these two schemes. The main contributions of this article can be summarized as follows.

1) We first propose two relay selection schemes (i.e., random selection and superior-link selection) in multiple relays-assisted IoT systems, where the source needs to transmit two types of messages with/without covert requirement, namely, legitimate and covert messages. Under the random selection scheme, the source randomly chooses a relay to help it forward the two types of messages to the destination. The transmission from the source to the relay may experience an outage once the received signal at the relay is smaller than its required threshold. For the superior-link selection scheme, the source can select an optimal relay to maximize the minimum channel gain between these two ones from the source to the relay and from the relay to the destination. The scheme can improve the poor channel gain such that guaranteeing channel gain fairness. The channel gain includes channel fading and path loss. With the scheme, the source selects a transmission mode in the following three modes according to channel quality: a) transmitting legitimate and covert messages; b) transmitting legitimate messages; and c) keeping silent, where the transmission will not experience an outage.
2) Under the random selection scheme, we first examine the transmission strategy design for the source and determine the detection error probability at the warden according to the probabilities of the false alarm and missed detection. For the false alarm, the warden judges that the source is transmitting covert messages, while it is not transmitting actually. The missed detection represents that the warden judges that the source is not transmitting a covert message, while it is transmitting actually. We then optimize the transmit power of the source to maximize the covert capacity which satisfies the constraint of covert requirement through efficient numerical searches.
3) Under the superior-link selection scheme, we first examine the transmission strategy design for the source and thus define the necessary condition that the source can transmit covert messages. We then derive the detection error probability of the warden according to the probabilities of the false alarm and missed detection and the covert capacity. We further optimize the transmit power of the source to maximize the covert capacity with the constraint of covert requirement through efficient numerical searches.
4) Finally, numerical results are provided to illustrate the impact of system parameters on the detection error probability and covert capacity, and also to reveal our findings.

The remainder of this article is organized as follows. Section II introduces related works. The system model and performance metrics are presented in Section III. Section IV presents the random selection scheme and analyzes covert performance. Section V presents the superior-link scheme and analyzes covert performance. The numerical results are provided in Section VI. Finally, we conclude this article in Section VII.

II. Related Works

Available works on the study of covert communication mainly focus on the single-hop and two-hop relay wireless systems.

A. Covert Communication Under Single-Hop Scenario

In the single-hop scenario, Bash *et al.* [16]–[18] proved that $\mathcal{O}\sqrt{n}$ bits of information can be transmitted to a legitimate receiver reliably and covertly in n channel uses as $n \to \infty$. Then, the works were extended to different channel models, such as the binary symmetric channel [19], the discrete memoryless channel (DMC) [20], [21], the multiple-access channels [22], the state-dependent channel [23], the memoryless broadcast channel [24], and the uncertain channel [25].

Based on these pioneering works on covert communication, much research effort is dedicated to the study of covert communication in various scenarios [26]–[33]. The work in [26] explored the impact of imperfect knowledge of the channel gain and noise power on the average detection error probability at the eavesdropper and the covert throughput under the Rayleigh fading channel. The work in [27] proved that covert communication could be achievable by adopting channel inversion power control with Rayleigh fading channels. Shahzad *et al.* [28] utilized the artificial noise from a full-duplex receiver to confuse a warden and derived a closed-form expression for the optimal detection performance of the warden.

The work in [29] considered a Poisson field of interferers in a covert communication scenario and proved that the density and the transmit power of the interferers have no effect on the covert throughput as long as the system stays in the interference-limited regime, for both the nonfading and the fading channels. Zheng *et al.* [30] studied the throughput performance of the covert communication under a stochastic geometry framework in a system where multiantenna-aided covert communications coexist with randomly located wardens and interferers. Shahzad *et al.* [31] took into account the effect of delay constraints in covert communication. The covert

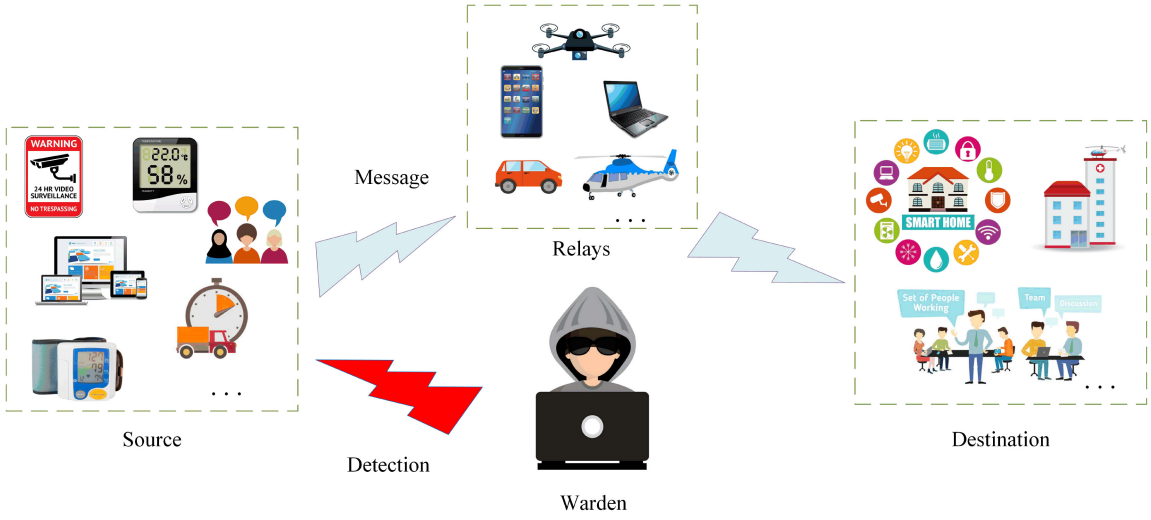


Fig. 1. Covert communication scenario for smart cities.

communication could be realized from a sequential change-point detection (SCPD) perspective in [32]. The work of [33] proposed two covert schemes based on the number of antennas at a base station which transmitted artificial noise to confuse adversaries in a D2D underlying cellular system. The work in [10] derived covert transmit bits in a dense IoT system with lower frequency additive white Gaussian noise (AWGN) channels and demonstrated that covert communication was achievable by utilizing the reflection or diffuse scattering from a rough surface in a terahertz band IoT system.

B. Covert Communication Under Two-Hop Scenario

Regarding a two-hop scenario with a single relay, Wu *et al.* [34], [35] studied the covert communication performance in terms of detection error probability and source's limited rate under AWGN channels. The work in [36] proved that channel uncertainty introducing confusions can degrade the performance of Willie's detection. Hu *et al.* [37] studied the impact of a greedy relay on covert communication performance. The work in [38] examined the possibility, performance limits, and associated costs for a self-sustained relay to transmit its own covert information to a destination.

III. System Model and Performance Metrics

A. System Model

As shown in Fig. 1, we consider a two-hop relay IoT system consisting of a source (Alice), multiple relays, a destination (Bob), and a warden (Willie). With the two-hop relay routing, Alice first transmits the legitimate message to the relay, and the relay then forwards the messages to Bob. In particular, Alice opportunistically transmits covert messages to the relay on top of transmitting legitimate messages. Willie tries to detect whether Alice is transmitting covert messages or not. Alice employs power P_a to transmit its messages. Once the transmit power P_a exceeds its maximum power constraint $P_{\max}$, Willie can detect that Alice is transmitting covert messages.

We assume that the time is evenly divided into equal-sized time slots, and the independent quasistatic Rayleigh fading is used to model wireless channels in our study, where each channel keeps unchanged in a time slot, but randomly and independently from the current time slot to the next one. The channel coefficients are modeled as complex Gaussian random variables with zero mean and unit variance. There are in total three channels in the system, i.e., the channel from Alice to the relay, the one from the relay to Bob, and the one from Alice to Willie, whose channels coefficients are denoted as h_{ar}, h_{rb}, and h_{wa}, respectively. The $|h_k|^2$ is the channel gain, where $k \in \{ar, rb, wa\}$. We assume that Alice knows $|h_{ar}|^2$, relay knows both $|h_{ar}|^2$ and $|h_{rb}|^2$, and Willie knows $|h_{wa}|^2$. In addition, the channel noise is AWGN with variance σ^2. We assume that the system bandwidth is W MHZ. Without loss of generality, we assume $W = 1$ throughout this article.

B. Performance Metrics

To decide whether Alice is transmitting covert messages to the relay or not, Willie conducts two hypotheses, i.e., null hypothesis H_0 and alternative hypothesis H_1. The former represents that Alice does not transmit covert messages while the latter represents that Alice transmits. Then, we define two performance metrics as follows.

Detection Error Probability: It is the probability that Willie makes a wrong decision on whether or not Alice is transmitting covert messages, which is expressed as

$$\zeta = \mathbb{P}_{\text{FA}} + \mathbb{P}_{\text{MD}} \tag{1}$$

where ζ denotes the detection error probability, $\mathbb{P}_{\text{FA}}$ denotes the probability of false alarm that Willie trusts H_1, while H_0 is true, $\mathbb{P}_{\text{MD}}$ denotes the probability of missed detection that Willie trusts H_0, while H_1 is true.

Covert Capacity: It is defined as the maximum rate at which messages from Alice are transmitted covertly to Bob with high detection error probability at Willie. In our study, we consider that Willie only detects the message transmission of Alice, and the relay can employ high transmit power to forward the messages to Bob. Therefore, the covert capacity is equal to that from Alice to the relay.

IV. Covert Communication Under Random Selection Scheme

This section first proposes the transmission strategies of Alice and then derives the detection error probability at Willie, and covert capacity under the random selection scheme.

A. Alice's Transmission Strategies

We propose two transmission strategies without/with covert messages under the random selection scheme. With the selection scheme, Alice randomly chooses one R_s from all relays. The selection scheme does not consider the quality of channel from Alice to the relay, which may result in transmission outage once if the received signal strength at the relay is smaller than its required threshold.

1) Alice's Transmission Without Covert Message: We consider that Alice only transmits legitimate messages with power P_{ar} subject to maximum power constraint $P_{\max}$. Then, the received signal at R_s is given by

$$y_r = \sqrt{P_{ar}} h_{ar} x_b + n_r \tag{2}$$

where x_b denotes the signal transmitted by Alice, and $n_r \sim \mathcal{CN}(0, \sigma_r^2)$ represents the received noise at R_s.

Accordingly, the signal-to-noise ratio (SNR) at R_s is determined as

$$\gamma_r = \frac{P_{ar}|h_{ar}|^2}{\sigma_r^2}. \tag{3}$$

2) Alice's Transmission With Covert Message: When Alice sends a covert message on top of transmitting legitimate messages, the received signal at R_s is determined as

$$y_r = \sqrt{P_{ar}} h_{ar} x_b + \sqrt{P_{ac}} h_{ar} x_c + n_r \tag{4}$$

where P_{ar} and P_{ac} represent the transmit power of transmitting legitimate messages x_b and covert messages x_c, respectively.

To ensure that the legitimate messages from Alice can be received, the relay R_s first decodes x_b and regards x_c as interference. Then, the signal-to-interference-plus-noise ratio (SINR) at R_s is determined as

$$\gamma_r = \frac{P_{ar}|h_{ar}|^2}{P_{ac}|h_{ar}|^2 + \sigma_r^2}. \tag{5}$$

B. Detection Error Probability

To determine the detection error probability at Willie, we first introduce the hypothesis test of Willie to make a decision on whether Alice is transmitting or not.

1) Hypothesis Test: We consider that Willie only detects whether Alice sends covert messages. Thus, the received signal y_w at Willie under the random selection scheme is given by

$$y_w = \begin{cases} \sqrt{P_{ar}} h_{\text{aw}} x_b + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P_{ar}} h_{\text{aw}} x_b + \sqrt{P_{ac}} h_{\text{aw}} x_c + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{6}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise at Willie.

To minimize the detection error probability at Willie, the optimal decision rule can be expressed as [39]

$$\frac{V}{n} \underset{D_0}{\overset{D_1}{\gtrless}} \lambda \tag{7}$$

where D_0 and D_1 denote that Willie makes a decision in favor of H_0 and H_1, respectively, λ is a detection threshold, and $V = \sum_{i=1}^{n} |y_w^i|^2$ is the received power at Willie in a time slot. Here, y_w^i is the received signal at Willie in the ith channel use, and n is the number of channel uses.

According to Lebesgue's dominated convergence theorem, V can be determined as

$$V = \begin{cases} P_{ar}|h_{\text{aw}}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is true} \\ P_{ar}|h_{\text{aw}}|^2 + P_{ac}|h_{\text{aw}}|^2 + \sigma_w^2, & \text{if } H_1 \text{ is true.} \end{cases} \tag{8}$$

2) Detection Error Probability at Willie: It can be determined as

$$\zeta = \mathbb{P}_{\text{FA}} + \mathbb{P}_{\text{MD}} \tag{9}$$

where

$$\begin{aligned} \mathbb{P}_{\text{FA}} &= P\Big(P_{ar}|h_{\text{aw}}|^2 + \sigma_w^2 \geq \lambda\Big) \\ &= P\left(|h_{\text{aw}}|^2 \geq \frac{\lambda - \sigma_w^2}{P_{ar}}\right) \\ &= \begin{cases} \exp\Big(\frac{\sigma_w^2 - \lambda}{P_{ar}}\Big), & \text{if } \lambda \geq \sigma_w^2 \\ 1, & \text{otherwise} \end{cases} \end{aligned} \tag{10}$$

and

$$\begin{aligned} \mathbb{P}_{\text{MD}} &= P\Big(P_{ar}|h_{\text{aw}}|^2 + P_{ac}|h_{\text{aw}}|^2 + \sigma_w^2 < \lambda\Big) \\ &= P\left(|h_{\text{aw}}|^2 < \frac{\lambda - \sigma_w^2}{P_{ar} + P_{ac}}\right) \\ &= \begin{cases} 1 - \exp\Big(\frac{\sigma_w^2 - \lambda}{P_{ar} + P_{ac}}\Big), & \text{if } \lambda > \sigma_w^2 \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{11}$$

To achieve covert communication, it should guarantee that $\zeta \geq 1 - \varepsilon$ for any $\varepsilon > 0$, when n tends to infinity [17].

Now, we optimize λ to maximize the detection error probability ζ. To this end, we rewrite (30) as

$$\zeta = \begin{cases} 1 - \exp\Big(\frac{\sigma_w^2 - \lambda}{P_{ar} + P_{ac}}\Big) + \exp\Big(\frac{\sigma_w^2 - \lambda}{P_{ar}}\Big), & \text{if } \lambda > \sigma_w^2 \\ 1, & \text{otherwise.} \end{cases} \tag{12}$$

Under the case of $\lambda \leq \sigma_w^2$, $\zeta = 1$. This means that Willie cannot detect the transmission from Alice to the relay absolutely. Thus, we only consider the case of $\lambda > \sigma_w^2$. Take the derivation of (12) with respect to λ and let the result equal to zero, we have

$$\frac{\partial \zeta}{\partial \lambda} = \frac{1}{P_{ar} + P_{ac}} \exp\left(\frac{\sigma_w^2 - \lambda}{P_{ar} + P_{ac}}\right) - \frac{1}{P_{ar}} \exp\left(\frac{\sigma_w^2 - \lambda}{P_{ar}}\right) = 0. \tag{13}$$

Then, we have

$$\lambda^* = \frac{(P_{ar} + P_{ac}) P_{ar}}{P_{ac}} \ln\left(\frac{P_{ar} + P_{ac}}{P_{ar}}\right) + \sigma_w^2. \tag{14}$$

Substituting (14) into (13), we can obtain that $(\partial\zeta)/(\partial\lambda) > 0$, if $\lambda > \lambda^*$ and $(\partial\zeta)/(\partial\lambda) < 0$, if $\lambda < \lambda^*$. Thus, Willie can know the optimal threshold $\lambda^\dagger = \lambda^*$ to achieve the minimum value of ζ, i.e., $\zeta^\dagger = \zeta(\lambda^\dagger)$.

C. Covert Capacity

To derive the covert capacity, we first determine the probability that transmission from Alice to the relay does not occur outage.

1) Probability Without Outage: A signal received at the relay can be successfully decoded if and only if the channel capacity C_{ar} from Alice to the relay is greater than the required threshold R_{ab} at the relay, and we say that no outage happens if $C_{ar} \geq R_{ab}$. When H_1 is true, the probability without outage $\delta_r(H_1)$ at the relay is determined as

$$\begin{aligned}\delta_r(H_1) &= P\big[\log_2(1+\gamma_r) \geq R_{ab}\big] \\ &= P\left(|h_{ar}|^2 \geq \frac{\Delta c \sigma_r^2}{P_{ar} - \Delta c P_{ac}}\right) \\ &= \exp\left(-\frac{\Delta c \sigma_r^2}{P_{ar} - \Delta c P_{ac}}\right) \end{aligned} \tag{15}$$

where $\Delta c = 2^{R_{ab}} - 1$. We know that $P_{ar} - \Delta c P_{ac} > 0$ in (15). Since $P_{ar} + P_{ac} \leq P_{\max}$, $P_{ac} \leq P_{\max}/(1+\Delta c)$. Notice that the increasing of P_{ac} leads to the decreasing of P_{ar} such that the outage may happen.

2) Covert Capacity: Based on the probability $\delta_r(H_1)$ and channel capacity C_e from Alice to the relay for covert messages transmission, the covert capacity C can be determined as

$$\begin{aligned} C &= C_e \delta_r(H_1) \\ &= \log_2\left(1 + \frac{P_{ac}|h_{ar}|^2}{P_{ar}|h_{ar}|^2 + \sigma_r^2}\right) \exp\left(-\frac{\Delta c \sigma_r^2}{P_{ar} - \Delta c P_{ac}}\right). \end{aligned} \tag{16}$$

3) Covert Capacity Maximization: The objective of covert capacity maximization is to maximize the covert capacity C while maintaining a high detection error probability at Willie. It can be formulated as the following optimization problem:

$$P_{ac}^{\dagger} = \arg\max_{P_{ac}} \ C \tag{17a}$$

$$\text{s.t.} \quad \zeta^{\dagger} \geq 1 - \varepsilon \tag{17b}$$

$$0 < P_{ac} \leq P_{\max}/(1+\Delta c) \tag{17c}$$

where $P_{ac}^{\dagger}$ denotes the optimal covert transmit power, constraint (17b) represents that the minimum detection error probability is greater than some value, ε denotes the covertness requirement, and constraint (17c) denotes the range of covert transmit power.

Note that (17) is a 1-D optimization problem, which can be easily solved by numerical search. By substituting $P_{ac}^{\dagger}$ into (16), we then obtain the maximum capacity denoted as C^*.

V. Covert Communication Under Superior-Link Selection Scheme

This section first proposes the superior-link selection scheme, transmission strategies of Alice, then derives detection error probability at Willie, and covert capacity under the superior-link selection scheme.

A. Superior-Link Selection Scheme

To enhance the covert capacity performance, we propose a superior-link selection scheme to find a best relay without an outage. With the selection scheme, the selected relay should be the maximum value of $\min\{|h_{ar_k}|^2, |h_{r_k b}|^2\}$ for all relays, where $|h_{ar_k}|^2$ and $|h_{r_k b}|^2$ represent the channel gain from Alice to the kth relay, and the one from the kth relay to Bob, respectively. To ensure that Alice transmits covert messages to the selected relay denoted as R_s without occurring outage, the channel gain $|h_{ar_s}|^2$ from Alice to the R_s needs to be greater than some threshold δ. Then, we have

$$\mathbb{P}(J) = P\Big(\big|h_{ar_s}\big|^2 \geq \delta\Big) \tag{18}$$

where J and $\mathbb{P}(J)$ denote the event that the R_s is selected, and corresponding probability, respectively, and $|h_{ar_s}|^2$ follows exponential distribution with unit mean.

We now determine the probability $\mathbb{P}(J)$. For each relay R_k where $k = 1, 2, \ldots, n$, let $M_k = \min\{|h_{ar_k}|^2, |h_{r_k b}|^2\}$, and D_k denote the event that Alice selects the relay. We then have

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

where M_k is an exponential random variable with mean 1/2. Based on the law of total probability and [40, Lemma 1], we have

$$\begin{aligned} P\Big(\big|h_{ar_s}\big|^2 < x\Big) &= \sum_{k=1}^{n} P\Big(\big|h_{ar_k}\big|^2 < D_k\Big) \\ &= \sum_{k=1}^{n} P\left\{\big|h_{ar_k}\big|^2 < x, \bigcap_{l=1, l\neq k}^{n} (M_l \leq M_k)\right\} \\ &= \sum_{k=1}^{n} \int_0^{\infty} P\left\{\big|h_{ar_k}\big|^2 < x, \bigcap_{l=1, l\neq k}^{n} (M_l \leq t), M_k = t\right\} dt \\ &= \int_0^{\infty} n P\Big(\big|h_{ar_k}\big|^2 < x, M_k = t\Big)\Big(1 - e^{-2t}\Big)^{n-1} dt \end{aligned} \tag{19}$$

where

$$\begin{aligned} &P\Big(\big|h_{ar_k}\big|^2 < x, M_k = t\Big) \\ &\quad = \begin{cases} e^{-t}\big(2e^{-t} - e^{-x}\big), & \text{if } 0 \leq t \leq x \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{20}$$

Then, we further obtain that

$$\begin{aligned} &P\Big(\big|h_{ar_b}\big|^2 < x\Big) \\ &\quad = \int_0^x n e^{-t}\big(2e^{-t} - e^{-x}\big)\Big(1 - e^{-2t}\Big)^{n-1} dt \\ &\quad = \Big(1 - e^{-2x}\Big)^n - n e^{-x} \int_0^x e^{-t}\Big(1 - e^{-2t}\Big)^{n-1} dt \\ &\quad = \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{k e^{-x} + (k-1) e^{-2kx}}{2k-1}. \end{aligned} \tag{21}$$

Thus, we have $\mathbb{P}(J) = 1 - P(|h_{ar_s}|^2 \leq \delta)$.

B. Alice's Transmission Strategy

We consider two transmission strategies of Alice.

1) Alice's Transmission Without Covert Message: When Alice transmits legitimate messages, the received signal at the relay is given by

$$y_r = \sqrt{P_{ar}^0} h_{ar} x_b + n_r \tag{22}$$

where P_{ar}^0 denotes the power used to transmit legitimate messages at Alice.

Then, the SNR γ_r at the relay is given by

$$\gamma_r = \frac{P_{ar}^0 |h_{ar}|^2}{\sigma_r^2}. \tag{23}$$

We know that when the required signal threshold of the relay $R_{ab} \leq C_{ar}$, the outage will not happen. Here, C_{ar} denotes that the channel capacity from Alice to the relay, which is determined as $C_{ar} = \log_2(1 + \gamma_r)$. Thus, we obtain $|h_{ar}|^2 \geq \Delta c \sigma_r^2 / P_{ar}$, where $\Delta c = 2^{R_{ar}} - 1$. Then, we have

$$P_{ar}^0 = \begin{cases} \frac{\Delta c \sigma_r^2}{|h_{ar}|^2}, & \text{if } |h_{ar}|^2 \geq \frac{\Delta c \sigma_r^2}{P_{\max}} \\ 0, & \text{if } |h_{ar}|^2 < \frac{\Delta c \sigma_r^2}{P_{\max}}. \end{cases} \tag{24}$$

2) Alice's Transmission With Covert Message: When Alice transmits legitimate and covert messages, the received signal at the relay is given by

$$y_r = \sqrt{P_{ar}^1} h_{ar} x_b + \sqrt{P_{ac}} h_{ar} x_c + n_r \tag{25}$$

where P_{ar}^1 denotes the power used to transmit legitimate messages at Alice. In general, $P_{ac} < P_{ar}^1$ for the purpose of covert communication. The relay first decodes the legitimate messages and thus regards the covert messages as interference. Thus, the SINR at the relay is given by

$$\gamma_r = \frac{P_{ar}^1 |h_{ar}|^2}{P_{ac} |h_{ar}|^2 + \sigma_r^2}. \tag{26}$$

Notice that when the selected relay should not lead to the outage, $R_{ab} \leq C_{ar}$. Thus, we have $|h_{ar}|^2 \geq \Delta c \sigma_r^2 / (P_{\max} - (1 + \Delta c) P_{ac})$. Then, we have

$$P_{ar}^1 = \begin{cases} \frac{\Delta c (P_{ac} |h_{ar}|^2 + \sigma_r^2)}{|h_{ar}|^2}, & \text{if } |h_{ar}|^2 \geq \frac{\Delta c \sigma_r^2}{P_{\max} - (1+\Delta c) P_{ac}} \\ \frac{\Delta c \sigma_r^2}{|h_{ar}|^2}, & \text{if } \frac{\Delta c \sigma_r^2}{P_{\max}} \leq |h_{ar}|^2 < \frac{\Delta c \sigma_r^2}{P_{\max} - (1+\Delta c) P_{ac}} \\ 0, & \text{if } |h_{ar}|^2 < \frac{\Delta c \sigma_r^2}{P_{\max}} \end{cases} \tag{27}$$

where the first case represents that Alice keeps silent, the second one represents that Alice only sends legitimate messages, and the third one represents that Alice sends legitimate and covert messages simultaneously. With the maximum power constraint, we can obtain $P_{ac} \leq (P_{\max} - \Delta c \sigma_r^2 / |h_{ar}|^2) / (1 + \Delta c)$.

C. Detection Error Probability

To determine the detection error probability at Willie, we first introduce the hypothesis test of Willie to make a decision on whether Alice is transmitting or not.

1) Hypothesis Test: We consider that Willie only detects whether Alice sends covert messages. Thus, the received signal y_w at Willie under the superior-link selection scheme is given by

$$y_w = \begin{cases} \sqrt{P_{ar}^0} h_{\text{aw}} x_b + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P_{ar}^1} h_{\text{aw}} x_b + \sqrt{P_{ar}} h_{\text{aw}} x_c + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{28}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise at Willie.

According to (7), the received power V at Willie can be determined as

$$V = \begin{cases} P_{ar}^0 |h_{\text{aw}}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is true} \\ P_{ar}^1 |h_{\text{aw}}|^2 + P_{ac} |h_{\text{aw}}|^2 + \sigma_w^2, & \text{if } H_1 \text{ is true.} \end{cases} \tag{29}$$

2) Detection Error Probability at Willie: It can be determined as

$$\zeta = \mathbb{P}_{\text{FA}} + \mathbb{P}_{\text{MD}}. \tag{30}$$

We need to calculate $\mathbb{P}_{\text{FA}}$ and $\mathbb{P}_{\text{MD}}$. Based on (27)–(29), we have

$$\begin{aligned} \mathbb{P}_{\text{FA}} &= P\left\{ \frac{\Delta c \sigma_r^2}{|h_{ar}|^2} |h_{\text{aw}}|^2 + \sigma_w^2 \geq \lambda \right\} \\ &= P\left\{ |h_{\text{aw}}|^2 \geq \frac{(\lambda - \sigma_w^2) |h_{ar}|^2}{\Delta c \sigma_r^2} \right\} \\ &= \begin{cases} \exp\left[\frac{(\sigma_w^2 - \lambda) |h_{ar}|^2}{\Delta c \sigma_r^2} \right], & \text{if } \lambda \geq \sigma_w^2 \\ 1, & \text{otherwise} \end{cases} \end{aligned} \tag{31}$$

and

$$\begin{aligned} \mathbb{P}_{\text{MD}} &= P\left\{ \left[\frac{\Delta c \sigma_r^2}{|h_{ar}|^2} + (1 + \Delta c) P_{ac} \right] |h_{\text{aw}}|^2 + \sigma_w^2 < \lambda | J \right\} \\ &= \frac{P\left[|h_{\text{aw}}|^2 < \frac{\lambda - \sigma_w^2}{(1+\Delta c) P_{ac} + \frac{\Delta c \sigma_r^2}{|h_{ar}|^2}} \right]}{\mathbb{P}(J)} \\ &= \begin{cases} 1 - \exp\left[\frac{\sigma_w^2 - \lambda}{(1+\Delta c) P_{ac} + \frac{\Delta c \sigma_r^2}{|h_{ar}|^2}} \right], & \text{if } \lambda > \sigma_w^2 \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{32}$$

Now, we optimize λ to maximize the detection error probability ζ. To this end, we rewrite (30) with (31) and (32) as

$$\zeta = \begin{cases} 1 - \exp\left(\frac{\sigma_w^2 - \lambda}{\tau + \alpha} \right) + \exp\left(\frac{\sigma_w^2 - \lambda}{\alpha} \right), & \text{if } \lambda > \sigma_w^2 \\ 1, & \text{otherwise} \end{cases} \tag{33}$$

where $\alpha = (\Delta c \sigma_r^2) / (|h_{ar}|^2)$, and $\tau = (1 + \Delta c) P_{ac}$.

Similar to the random selection scheme, we only need to consider the case of $\lambda > \sigma_w^2$. Take the derivation of (33) with respect to λ and let the result equal to zero, we have

$$\frac{\partial \zeta}{\partial \lambda} = \frac{1}{\tau + \alpha} \exp\left(\frac{\sigma_w^2 - \lambda}{\tau + \alpha} \right) - \frac{1}{\alpha} \exp\left(\frac{\sigma_w^2 - \lambda}{\alpha} \right) = 0. \tag{34}$$

Then, we obtain

$$\lambda^* = \frac{(\tau + \alpha)\alpha}{\tau} \ln\left[\frac{(\tau + \alpha)}{\alpha} \right] + \sigma_w^2. \tag{35}$$

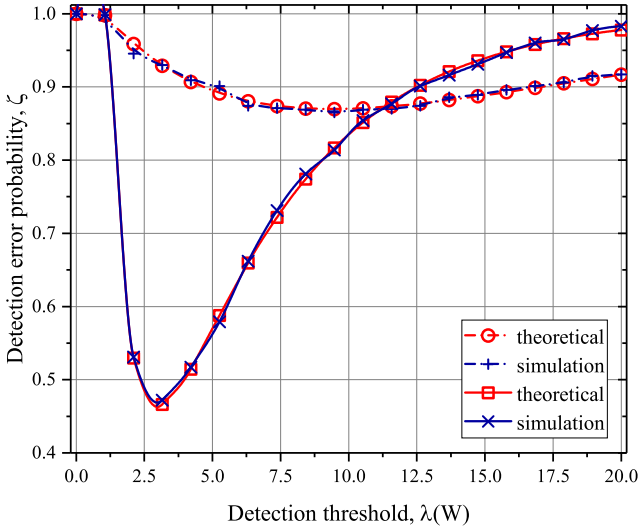


Fig. 2. Model validation.

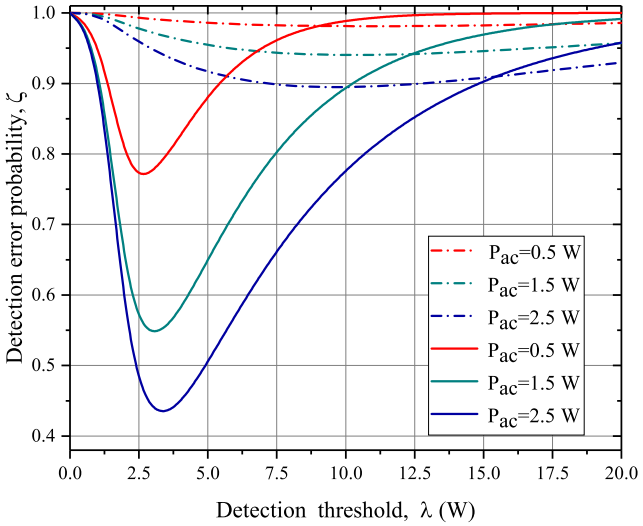


Fig. 3. Impact of detection threshold on detection error probability.

We further obtain that $(\partial\zeta)/(\partial\lambda) > 0$, if $\lambda > \lambda^*$ and $(\partial\zeta)/(\partial\lambda) < 0$, if $\lambda < \lambda^*$. Thus, Willie can know the optimal threshold $\lambda^\dagger = \lambda^*$ to achieve the minimum value of ζ, i.e., $\zeta^\dagger = \zeta(\lambda^\dagger)$.

D. Covert Capacity

1) Covert Capacity: Based on the channel capacity C_e from Alice to the relay for covert messages transmission, the covert capacity C can be determined as

$$C = C_e = \log_2\left\{1 + \frac{P_{ac}|h_{ar}|^2}{\Delta c\left(P_{ac}|h_{ar}|^2 + \sigma_r^2\right) + \sigma_r^2}\right\}. \quad (36)$$

2) Covert Capacity Maximization: The covert capacity maximization aims to maximize the covert capacity C while keeping a high detection error probability at Willie. We can formulate covert capacity maximization as the following optimization problem:

$$P_{ac}^\dagger = \arg\max_{P_{ac}} C \quad (37a)$$

$$\text{s.t.} \quad \zeta^\dagger \geq 1 - \varepsilon \quad (37b)$$

$$0 < P_{ac} \leq \frac{P_{\max} - \Delta c\sigma_r^2/|h_{ar}|^2}{(1 + \Delta c)} \quad (37c)$$

where $P_{ac}^\dagger$ denotes the optimal covert transmit power, constraint (37b) represents that the minimum detection error probability is greater than some value, ε denotes the covertness requirement, and constraint (37c) denotes the range of covert transmit power.

Unitizing numerical search, we can easily solve the 1-D optimization problem in (37). By substituting $P_{ac}^\dagger$ into (36), we then obtain the maximum capacity denoted as C^*.

VI. Numerical Results

In this section, extensive numerical results are provided to illustrate the impact of various system parameters on the detection error probability at Willie and covert capacity performance, and also to reveal our findings under these two relay selection schemes. Some parameters used in this article are set as $R_{ab} = 1$ Mb/s/Hz, $\sigma_w^2 = \sigma_r^2 = 0$ dB, and $P_{\max} = 10$ W, unless otherwise specified. In the following figures, the dashed lines and solid ones are used to show the results under the random selection scheme and the superior-link selection scheme, respectively.

A. Model Validation

To validate our proposed theoretical results, we compare the theoretical results with the simulation ones under the two relay selection schemes with the setting of covert transmit power $P_{ac} = 2$ W. We summarize in Fig. 2 how the detection error probability ζ varies with the detection error threshold λ. We can see from Fig. 2 that for each relay selection scheme, the theoretical ζ matches well with the simulation one. This demonstrates that our theoretical results can well capture the performance of covert communication under these two relay selection schemes.

B. Performance Analysis Under Two Schemes

We first explore the impact of detection threshold λ on the detection error probability ζ under these two relay selection schemes. We summarize in Fig. 3 how ζ varies with λ under the two schemes with the setting of covert transmit power $P_{ac} = \{0.5, 1.5, 2.5\}$ W. We can see from Fig. 3 that for each setting of P_{ac}, 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 P_{FM} and missed detection probability P_{MD}. P_{FM} is a decreasing function of λ while P_{MD} is an increasing function. As λ is relatively small, the former one dominates ζ, leading to the decreasing of ζ with λ. On the other hand, as λ further increases, the latter one dominates ζ, leading to the increasing of ζ. As shown in Fig. 3, there exists a minimum ζ, at which Willie has the strongest detection ability to detect the transmission from Alice to the relay. Notice that the decreasing of P_{ac} not only increases ζ but also decreases covert capacity.

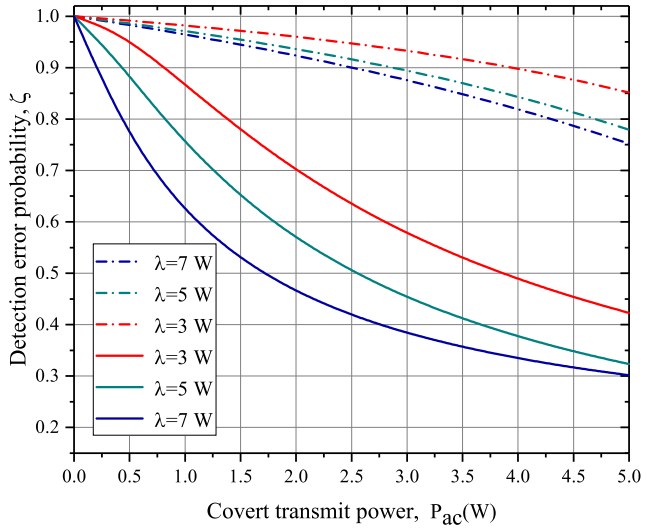


Fig. 4. Impact of covert transmit power on detection error probability.

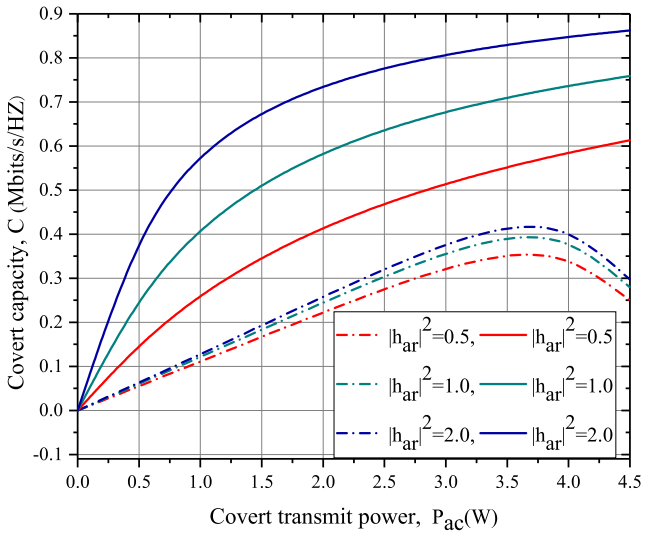


Fig. 5. Impact of covert transmit power on covert capacity.

Thus, P_{ac} needs to be carefully set so as to satisfy different application requirements with the detection error probability and covert capacity.

A careful observation of Fig. 3 indicates that for each fixed λ, ζ under the random selection scheme is greater than that under the superior-link selection scheme. It is due to the following reasons. In comparison with the random selection scheme, the channel quality from Alice to the relay is better under the superior-link selection scheme, such that Alice under the former needs to a higher power to send its legitimate message. This will extremely confuse Willie under the former. Thus, the detection error probability ζ at Willie under the former is greater than that of the latter.

To investigate the impact of covert transmit power P_{ac} on the detection error probability ζ, we summarize in Fig. 4 how ζ varies with the increasing of P_{ac} under these two relay selection schemes with the setting of $\lambda = \{3, 5, 7\}$ W. It can be observed from Fig. 4 that as P_{ac} increases, ζ decreases under both the schemes. This is because the increasing of P_{ac} leads to the increasing of probability that the transmission from Alice to the relay is detected by Willie and, thus, the detection error probability ζ decreases with P_{ac}. We can also see from Fig. 4 that for each fixed P_{ac}, ζ under the random selection scheme is greater than that under the superior-link selection scheme. This can be explained as follows. The channel quality from Alice to the relay under the former is worse than that under the latter one. To reduce the outage probability under the former, Alice needs to increase the power to transmit its legitimate message which confuses Willie. Thus, ζ under the former one is more than the latter.

We now proceed to explore how the covert transmit power P_{ac} affects the covert capacity C under these two relay selection schemes. We summarize in Fig. 5 how C varies with P_{ac} for a setting of channel gain $|h_{ar}|^2 = \{0.5, 1.0, 2.0\}$. We observe from Fig. 5 that as P_{ac} increases, C first increases and then decreases under the random selection scheme, while C always increases under the superior-link selection scheme. This can be explained as follows. The transmit power of Alice consists of covert transmit power P_{ac} and the power P_{ar} used to transmit the legitimate message, and is subject to the constraint of a maximum transmit power $P_{\max}$. Under the former, we know that C is related to outage probability and covert transmit power. As P_{ac} is relatively small, the latter power is high. Although P_{ac} increases, the relative high P_{ar} corresponds to a small outage probability. Thus, the positive effect of P_{ac} dominates the negative effect of outage probability, leading to the increasing of covert capacity C. As P_{ac} further increases, P_{ar} becomes relatively small, which leads to a high outage probability, such that the negative effect of outage probability dominates the positive effect of P_{ac}, leading to the decreasing of C. Notice that under the superior-link selection scheme, the covert capacity C is related to the only covert transmit power P_{ac}. Thus, the covert capacity C increases with P_{ac}. More careful observation from Fig. 5 indicates that for each fixed P_{ac}, the C under the random selection scheme is lower than that under the superior-link selection scheme. This is because there does not exist a negative effect of outage probability on the covert capacity under the superior-link selection scheme, leading to a bigger C.

We further observe from Fig. 5 that for each fixed P_{ac}, the covert capacity C increases with the increasing of channel gain $|h_{ar}|^2$ under each selection scheme. This is because a large $|h_{ar}|^2$ leads to a strong received signal at the relay under each scheme, and also low outage probability under the random selection scheme, which results in a large covert capacity C.

It is notable that although the multiple relays selection solutions have been extensively investigated in wireless networks, this article is the first work to propose two relay selection schemes to explore the covert communication in multiple relays-assisted IoT systems. We further treat the random selection scheme as a benchmark for other works. Regarding a given application with a fixed covert transmit power 3.5 W and the constraint of minimum covert capacity 0.5 Mb/s/HZ, the covert capacity under the random selection scheme is less than the one required for the given application as shown in Fig. 5.

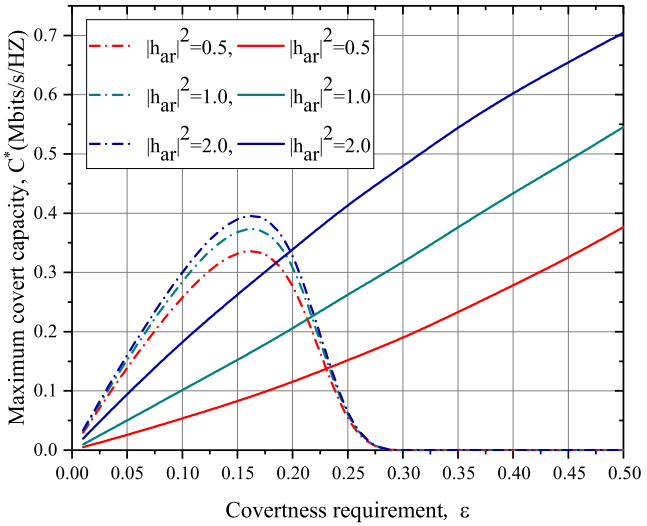


Fig. 6. Impact of covertness requirement on maximum covert capacity.

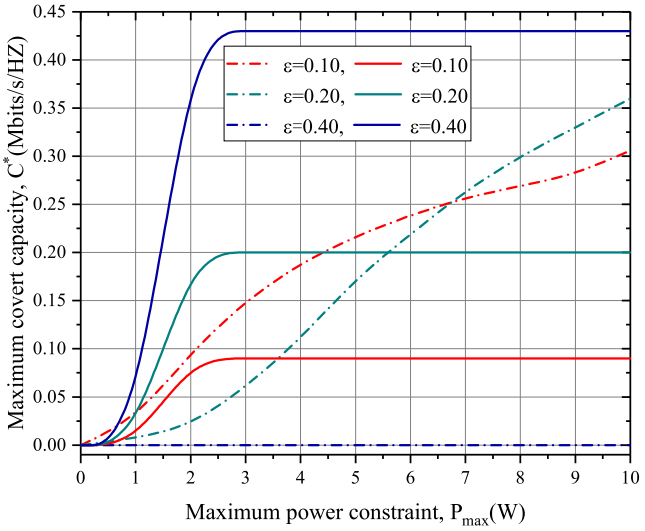


Fig. 7. Impact of maximum power constraint on maximum covert capacity.

On the other hand, the covert capacity under the superior-link selection scheme is sufficient to support the application.

C. Performance Optimization Under Two Schemes

We now explore the impact of covertness requirement ε and maximum power constraint $P_{\max}$ on the maximum covert capacity C^* under the two relay selection schemes. Fig. 6 illustrates that the impact of covertness requirement ε on the maximum covert capacity C^* under the two relay selection schemes with the setting of $|h_{ar}|^2 = \{0.5, 1.0, 2.0\}$. We can see from Fig. 6 that as ε increases, the C^* first increases and then decreases under the random selection scheme while it always increases under the superior-link selection scheme. This phenomenon can be explained as follows. The optimal covert transmit power $P_{ac}^{\dagger}$ increases as the detection error probability $\zeta^{\dagger}$ decreases while $\zeta^{\dagger}$ decreases as ε increases. Thus, the increase of ε is equivalent to that of the optimal covert transmit power. Similar to the analysis of Fig. 5, as the optimal covert transmit power is relatively small, the power P_{ar} is always high, leading to a small outage probability. Thus, the positive effect of optimal covert transmit power dominates the negative effect of outage probability, resulting in an increase of maximum covert capacity C^*. As the optimal covert transmit power further increases up to a large value, P_{ar} becomes relative small, which leads to a high outage probability, so the negative effect of outage probability dominates the positive effect of optimal covert transmit, leading to the decreasing of C^*. Notice that under the superior-link selection scheme, the maximum covert capacity C^* is related to the only covert transmit power P_{ac}. Thus, the maximum covert capacity C^* always increases as the optimal covert transmit power increases.

An observation of Fig. 6 indicates that for each fixed $|h_{ar}|^2$, as ε increases beyond a threshold, the maximum covert capacity C^* under the superior-link selection scheme is always larger than that under the random selection scheme. This can be explained as follows. We know that Willie treats the power P_{ar} as background noise. Due to the effect of the worse link with low link quality under the random selection scheme, Alice employs higher power to transmit its legitimate message. Thus, the background noise under the random selection scheme is stronger than that under the superior-link selection scheme for each fixed ε, such that the detection error probability under the former is higher than that under the latter. To achieve the same detection error probability under both schemes, the optimal covert transmits power $P_{ac}^{\dagger}$ needs to be increased under the former aiming to reduce the detection error probability, which leads to an increase of maximum covert capacity C^*. However, as ε becomes larger, the outage probability has a significant effect on C^* under the former scheme, thus the maximum covert capacity under the former is then smaller than that under the latter scheme.

Another careful observation of Fig. 6 indicates that when ε is relatively small, the maximum covert capacity under the random selection scheme is higher than the one under the superior-link selection scheme. However, under the random selection scheme, Alice needs to use higher transmit power to reduce the negative outage effect on the covert capacity is compared with the superior-link selection scheme. Thus, the former scheme is not suitable for the covert communication of the devices with limited transmit power.

Finally, we examine how the maximum power constraint $P_{\max}$ affects the maximum covert capacity C^* under two relay selection schemes. Given a setting of covertness requirement $\varepsilon = \{0.1, 0.2, 0.4\}$, we summarize in Fig. 7 how C^* varies with $P_{\max}$. We can see from Fig. 7 that as $P_{\max}$ increases, C^* always increases under the random selection scheme for each fixed $\varepsilon \in \{0.1, 0.2\}$. Particularly, $C^* = 0$ when $\varepsilon = 0.4$ under such a scheme. On the other hand, C^* first increases and then remains unchanged under the superior-link selection scheme. The reasons behind the phenomenon can be explained as follows. For each fixed $\varepsilon \in \{0.1, 0.2\}$ under the random selection scheme, the power P_{ar} increases with the increasing of $P_{\max}$, which can reduce the negative effect of outage probability on C^*. Meanwhile, the covert transmit power also needs to increase to keep an unchanged value of ε, leading to the increasing of C^*. When $\varepsilon = 0.4$, we have a large optimal

covert transmit power and a small P_{ar}, leading to an occurring of outage and $C^* = 0$. Regarding the superior-link selection scheme without an outage, according to (37), we can determine an optimal covert transmit power. As $P_{\max}$ is relatively small, the covert transmit power is less than the optimal value. Thus, the covert transmit power increases with the increase of $P_{\max}$, which leads to the increasing of maximum covert capacity C^*. Once if $P_{\max}$ increases more than some threshold, the covert transmit power achieves the optimal value and keeps unchanged, which leads to a constant C^*.

We further observe from Fig. 7 that a relatively small transmit power could lead to a big maximum covert capacity under the superior-link selection scheme, while if the maximum covert capacity achieves a big value under the random selection scheme, it needs a higher transmit power.

VII. Conclusion

This article investigated the performance of covert communication in multiple relays-assisted IoT systems. To this end, we proposed two relay selection schemes, i.e., random selection and superior-link selection. We then derived the expressions for the detection error probability and covert capacity under each selection scheme. Moreover, we also derived the maximum detection error probability by optimizing the detection threshold. We further optimized the covert transmit power to maximize the covert capacity performance with the covert requirement. Extensive numerical results were presented to illustrate the impact of critical system parameters on detection error probability and covert capacity. We found that with the same transmit power at the source, the covert capacity under the superior-link selection scheme is always higher than that under the random selection scheme. An interesting research direction is to select some neighboring nodes of the adversaries as jammers to ensure the covert communications.

References

[1] N. H. Motlagh, M. Bagaa, and T. Taleb, "Energy and delay aware task assignment mechanism for UAV-based IoT platform," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6523–6536, Aug. 2019.

[2] B. Yang, T. Taleb, Y. Shen, X. Jiang, and W. Yang, "Performance, fairness and tradeoff in UAV swarm underlaid mmwave cellular networks with directional antennas," *IEEE Trans. Wireless Commun.*, early access, Dec. 11, 2020. [Online]. Available: https://doi.org/10.1109/TWC.2020.3041800

[3] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[4] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[5] C. Benzaid and T. Taleb, "ZSM security: Threat surface and best practices," *IEEE Netw.*, vol. 34, no. 3, pp. 124–133, May/Jun. 2020.

[6] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 899–922, Jan. 2019.

[7] 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 Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[8] B. Yang, T. Taleb, Z. Wu, and L. Ma, "Spectrum sharing for secrecy performance enhancement in D2D-enabled UAV networks," *IEEE Netw.*, vol. 34, no. 6, pp. 156–163, Nov./Dec. 2020.

[9] A. Yang, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu, "Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2521–2530, Apr. 2020.

[10] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: From AWGN channel to THz band," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3378–3388, Apr. 2020.

[11] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: Hiding information in interference," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 46–52, Dec. 2018.

[12] Y. Zhang, Y. Li, R. Wang, M. S. Hossain, and H. Lu, "Multi-aspect aware session-based recommendation for intelligent transportation services," *IEEE Trans. Intell. Transp. Syst.*, early access, May 14, 2020. [Online]. Available: https://doi.org/10.1109/TITS.2020.2990214

[13] H. Lu, Y. Zhang, Y. Li, C. Jiang, and H. Abbas, "User-oriented virtual mobile network resource management for vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, early access, May 20, 2020. [Online]. Available: https://doi.org/10.1109/TITS.2020.2991766

[14] 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.

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

[16] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[17] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 448–452.

[18] B. A. Bash, D. Goeckel, and D. Towsley, "LPD communication when the warden does not know when," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 606–610.

[19] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2945–2949.

[20] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[21] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[22] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2016, pp. 2229–2233.

[23] S.-H. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2310–2319, Sep. 2018.

[24] K. S. K. Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2787–2801, Oct. 2019.

[25] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, 2017, pp. 1–5.

[26] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 236–239, Feb. 2016.

[27] J. Hu, S. Yan, X. Zhou, S. Feng, and J. Li, "Covert wireless communications with channel inversion power control in Rayleigh fading," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12135–12149, Dsec. 2019.

[28] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[29] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a poisson field of interferers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6005–6017, Dec. 2019.

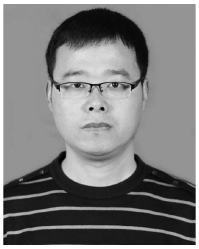
[30] T. Zheng, H. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1974–1987, Mar. 2019.

[31] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12432–12436, Dec. 2019.

[32] K. Huang, H. Wang, D. Towsley, and H. V. Poor, "LPD communication: A sequential change-point detection perspective," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2474–2490, Apr. 2020.
[33] Y. Jiang, L. Wang, and H. Chen, "Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2980–2992, Mar. 2020.
[34] H. Wu, X. Liao, Y. Dang, Y. Shen, and X. Jiang, "Limits of covert communication on two-hop AWGN channels," in *Proc. IEEE Int. Conf. Netw. Netw. Appl. (NaNA)*, 2017, pp. 42–47.
[35] H. Wu, Y. Zhang, X. Liao, Y. Shen, and X. Jiang, "On covert throughput performance of two-way relay covert wireless communications," *Wireless Netw.*, vol. 26, pp. 3275–3289, Jan. 2020.
[36] 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 Commun. Lett.*, vol. 8, no. 1, pp. 317–320, Feb. 2019.
[37] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jul. 2018.
[38] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4089–4102, Aug. 2019.
[39] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.
[40] A. Browder, *Mathematical Analysis: An Introduction*. New York, NY, USA: Springer, 2012.

Chan Gao received the B.S. and M.S. degrees from Xi'an University of Posts and Telecommunications, Xi'an, China, in 2014 and 2018, respectively. She is currently pursuing the Ph.D. degree with the School of Systems Information Science, Future University Hakodate, Hakodate, Japan.

Her research interest focuses on the covert communication in the physical layer.



Bin Yang received the Ph.D. degree in systems information science from Future University Hakodate, Hakodate, Japan, in 2015.

He is a Professor with the School of Computer and Information Engineering, Chuzhou University, Chuzhou, China, and is also a Research Fellow with the School of Electrical Engineering, Aalto University, Espoo, Finland. His research interests include unmanned aerial vehicle networks, cyber security, and Internet of Things.

Xiaohong Jiang (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees from Xidian University, Xi'an, China, in 1989, 1992, and 1999, respectively.

He was an Associate Professor with Tohoku University, Sendai, Japan, from February 2005 to March 2010. He is currently a Full Professor with Future University Hakodate, Hakodate, Japan. 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, such as IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE JOURNAL OF SELECTED AREAS ON COMMUNICATIONS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and IEEE INFOCOM. His research interests include computer communications networks, mainly wireless networks and optical networks, network security, and routers/switches design.

Hiroshi Inamura (Member, IEEE) received the B.E., M.E., and D.E. degrees from Keio University, Tokyo, Japan, in 1988, 1990, and 2010, respectively.

He has been a Professor with the School of Systems Information Science, Future University Hakodate, Hakodate, Japan, since 2016. He was an Executive Research Engineer with NTT Docomo, Inc., Tokyo. His current research interests include mobile computing, system software for smart devices, mobile/sensor network, and their security.

Prof. Inamura is a member of IPSJ, IEICE, and ACM.

Masaru Fukushi (Member, IEEE) received the B.Sc. and M.Sc. degrees from Hirosaki University, Hirosaki, Japan, in 1995 and 1997, respectively, and the Ph.D. degree in information science from the Graduate School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi, Japan, in 2002.

He was an Assistant Professor with JAIST from 2002 to 2004, and with Tohoku University, Sendai, Japan, from 2004 to 2012. He is currently an Associate Professor with the Graduate School of Sciences and Technology for Innovation, Yamaguchi University, Yamaguchi, Japan. His research interests include dependable parallel and distributed systems and Internet of Things.