Energy Harvesting Jammer-Aided Covert Communications in Wireless Multi-Relay IoT Systems

Hao Lv, Bin Yang, Xiuwen Sun, Chan Gao, Bao Gui, Tarik Taleb

Abstract—This paper investigates covert communications in a multi-relay Internet of Things (IoT) system with multiple energy harvesting jammers, where a transmitter (Alice) attempts to covertly transmit confidential messages to its destination (Bob) through relay forwarding, while a warden (Willie) detects the existence of Alice's transmission. Specifically, we employ a harvesting-then-jamming protocol with which the jammers first harvest energy from Alice and then send jamming signals to interfere with Willie's detection. We propose a relay and jammer selection strategy, namely quality of service (QoS)-aware selection, and use the random selection strategy as a comparison strategy. Under these two selection strategies, we derive the optimal detection threshold and minimum detection error probability at Willie, respectively. We then model the covert throughput performance and obtain the maximum covert throughput by jointly optimizing covert transmit power and jamming transmit power. Extensive numerical results are provided to illustrate the impacts of system parameters on covert throughput performance.

Keywords: Internet of Things, covert communications, energy harvesting, relay and jammer selection

I. INTRODUCTION

Wireless Internet of Things (IoT) systems play an indispensable role in everyday life and industrial applications, where a wealth of privacy information is transmitted through wireless media, such as personal health data, geographic location information, financial transaction records, etc [1-6]. However, such IoT systems encounter information leakage risk because of open wireless media and broadcast signals. Traditional cryptographic security methods usually increase computational complexity to enhance security of information transmissions, and thus cannot fully satisfy the needs of information security for a large number of energy-limited IoT devices [7-10]. As an effective supplement, covert communications are emerging as a cutting-edge lightweight security technology which utilizes the random characteristics of wireless channel to conceal the wireless communication process [11-14]. To support various security-sensitive applications, it is crucial to explore covert communications in wireless IoT systems.

The available studies on covert communications in wireless systems can be classified into two categories in terms of no relay and relay assistance. For the scenario with no-relay assistance, Hu et al. designed a chaotic pseudo-orthogonal covert communication scheme to improve system covertness [15]. Wang et al. proposed a transmission time selection strategy and a power control strategy to enhance covert performance by utilizing channel state information and transmit power control, respectively [16]. Lu et al. studied short packet covert communications and exploited transmission time uncertainty to achieve a tradeoff between effective throughput and communication covertness [17]. Che et al. proposed a covert transmission scheme based on random sub-channel selection to enhance system covertness in a multi-channel system [18]. Xiong et al. employed a cognitive jammer to improve covert throughput performance, in which the jammer sensed whether Alice transmits messages and then sends jamming signals to confuse Willie's detection when Alice conducts transmission [19]. Lv et al. utilized an intelligent reflecting surface to achieve covert downlink and uplink transmissions in a non-orthogonal multiple access (NOMA) system [20]. Shmuel et al. adopted a jammer equipped with multiple antennas to assist covert communications between a legitimate user pair, in which the jammer sends artificial noise to create uncertainty at the detector [21]. Tao et al. utilized an energy harvesting jammer to achieve covert communications in an uplink non-orthogonal multiple access system [22]. Forouzesh et al. further explored joint secure and covert communications in a single-input multiple-output system, where an untrusted user intercepted the transmission content of a legitimate user pair, while a detector detected the transmission existence of another legitimate user pair [23].

For the scenario with relay assistance, Hu et al. examined covert communications in a greedy relay system where the relay also opportunistically sent its own message besides forwarding source's message [24]. Su et al. proposed a relay selection strategy to select a relay with the highest chain gain from the relay to the destination and indicated the covert throughput

This work was supported in part by the National Natural Science Foundation of China under Grants 62372076,62102001; in part by the Anhui Talent Project under Grant DTR2023051; and in part by the European Union's HE Research and Innovation Program HORIZON-JUSNS-2023 through the 6G-Path Project under Grant 101139172. The research work presented in this article was conducted in part at ICTFICIAL Oy, Finland. (Corresponding authors: Bin Yang; Xiuwen Sun.)

Hao Lv is with the School of Computer Science and Technology of Anhui University, Hefei 230000, China and the School of Computer and Information Engineering, Chuzhou University, Chuzhou 239000, China (e-mail: lvhao8806@gmail.com)

Bin Yang and Bao Gui are with the School of Computer and Information Engineering, Chuzhou University, Chuzhou 239000, China (e-mail: yangbinchi@gmail.com; gui_bao1@163.com).

Xiuwen Sun is with the School of Computer Science and Technology of Anhui University, Hefei 230000, China (e-mail: mr.xiuwen@gmail.com)

Chan 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).

Tarik Taleb is with the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, Bochum 44801, Germany (e-mail: tarik.taleb@rub.de).

Table 1 All symbols and their explanations in the paper

Symbol	Definition	Symbol	Definition
Alice	Transmitter node	P_{ar}	Power of Alice transmitting public messages
Bob	Receiver node	P_{max}	The maximum transmit power of Alice
Willie	Warden node	P_{ac}	Power of Alice transmitting covert messages
RS	The selected relay	P_j	Power of EHJs transmitting interfering signals
EHJ	Erengy harvesting jammer	σ_i^2	Noise variance at node i
$\|h_{ij}\|^2$	Channel gain from i to j	P_{ar}^*	Power of Alice not transmitting covert messages under the QoS-aware selection strategy
E	The harvested energy by the energy harvesting jammer	$P_{ar}^\#$	Power of Alice transmitting covert messages under the QoS-aware selection strategy
μ	Energy conversion efficiency	τ	Detection threshold of Willie
ϖ	Time-switching factor	R	Singal threshold
T	A time slot	τ_{opt}	The optimal detection threshold
P_a	Power of Alice transmitting public messages during the first phase	$\mathrm{C_{ar}}$	Channel rate from Alice to Relay
ϕ	Detection error probability	ϕ_{opt}	The optimal detection error probability
$\mathbb{P}_{FA}$	False alarm probability	κ	Covert throughput
$\mathbb{P}_{MD}$	Missed probability	ϱ	The channel rate when Alice transmits covert message to RS
H_1	Alice sends covert message	P_{ac}^{opt}	The optimal covert message transmission power
H_0	Alice doesn't send covert messages	P_j^{opt}	The optimal interference power
$\mathrm{SINR_r}$	Signal-to-interference-plus-noise ratio at RS	κ_{opt}	The optimal covert throughput
ε	The covert requirement		

improvement of the relay-to-destination pair [25]. Jiang et al. considered a UAV-aided relay system and explored the covert throughput maximization by jointly optimizing time slots, transmit power, and trajectory of UAV [26]. Wang et al. jointly employed UAV and intelligent reflecting surface (IRS) installed on UAV to further enhance covert throughput performance [27]. Gao et al. investigated covert throughput maximization in a multi-relay system, where a relay can be selected through a random way and rate-optimal way, respectively [28]. Forouzesh et al. further explored joint covert and secure communications in an untrusted relay system in the presence of multiple detectors [29].

It is notable that cooperative jamming and relaying are two promising methods to improve system covert performance. The cooperative jamming method utilizes artificial noise emitted by the jammer to confuse the detector's judgment on wireless transmission. As for the cooperative relaying method, it can decrease the transmit power of a transmitter via the relay's forwarding and thus enhances the covertness of wireless transmission. On the other hand, it can also achieve information transmission between a transmitter-receiver pair without direct link in a deep fading environment. However, wireless devices (e.g., sensors) often have limited energy resources and selfish behaviors in practical wireless systems, especially in wireless IoT systems. Thus, these devices are not willing to serve as jammers to consume their own energy. To tackle the challenge, energy harvesting is an attractive technology to harvest energy from the environment for the wireless devices. Based on the above observations, this paper investigates covert communications in an IoT system by combining cooperative jamming and relaying. In particular, multiple potential jammers can harvest energy from a transmitter, and then a selected jammer assists the transmitter's covert information transmissions.

The combination of relay and jamming can incur two new challenges. One is how to select a jammer, which can interfere with Willie's judgment on covert transmission as much as possible and reduce the negative effect of the interference on the legal relay. Another is that the jammer's interference leads to more complex on the modelling of detection error probability and covert throughput in comparison with separate relay's scenario. The main contribution of this paper is summarized as follows.

(1) We consider a wireless multi-relay IoT system with a transmitter (Alice), a receiver (Bob), multiple potential relays (Relays), multiple energy harvesting jammers (EHJs) and a detector (Willie). We employ a harvesting-then-jamming protocol consisting of two phases. In the first energy harvesting phase, Alice sends public information to a selected relay which forwards it to the receiver, and EHJs harvest energy from Alice. In the second jamming phase, Alice sends public and covert information simultaneously, and a selected EHJ sends artificial noise (AN) to interfere with Willie's detection of covert information transmissions.

(2) We propose a strategy to select an EHJ and a relay, namely quality of service (QoS)-aware selection, and use the random selection strategy as a comparison strategy. Under the random selection strategy, we randomly select an EHJ and a relay. Under the QoS-aware selection strategy, the selected EHJ can significantly negatively affect Willie's detection and reduce the negative effect on a selected relay as much as possible. The selected relay under such a

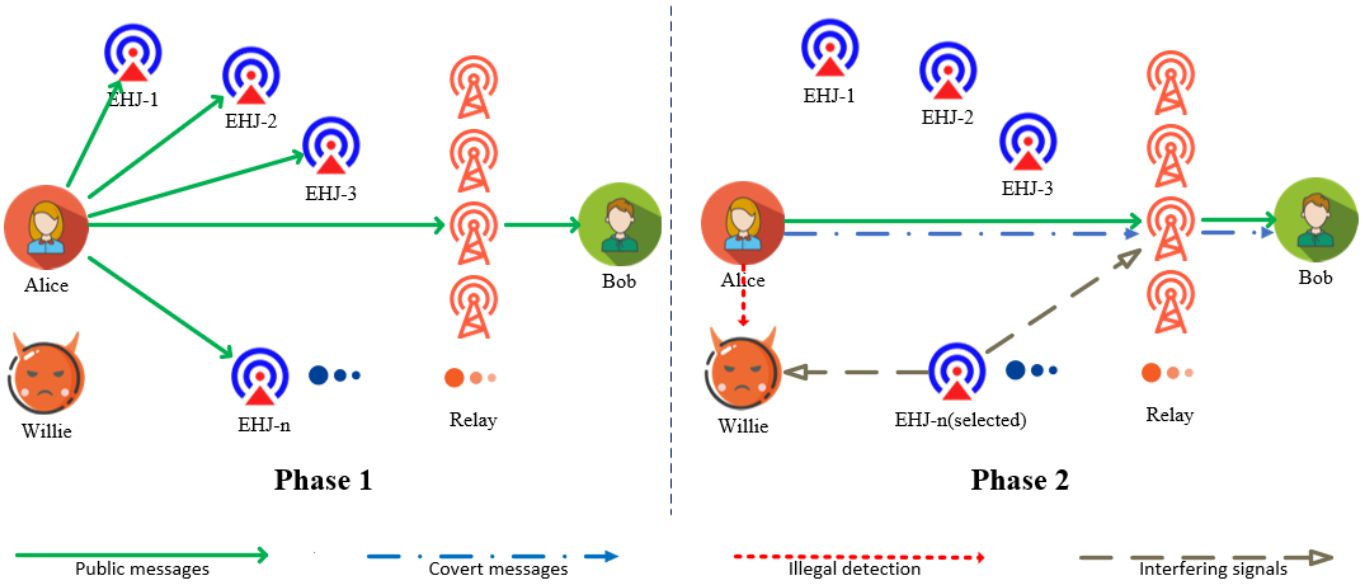


Fig. 1 System model

strategy is optimal with carefully considering channel gains from Alice to each potential relay and from each potential relay to Bob.

(3) Under these two selection strategies, we derive the optimal detection threshold and minimum detection error probability at Willie, respectively. We then model the covert throughput performance and obtain the maximum covert throughput by jointly optimizing covert transmit power and jamming transmit power.

(4) We present numerical results to indicate that the effect of system parameters on the covert throughput performance and also to make performance comparisons under these two strategies.

The remainder of this paper is organized as follows. Section II presents the system model. The two EHJ and relay selection strategies are proposed in section III. Detection performance is discussed in section IV. Section V provides covert throughput model and optimization. Numerical results are presented in section VI. Section VII concludes this paper. All symbols and their explanations in the paper are outlined in Table 1.

II. System Model

As shown in Figure 1, the considered wireless multi-relay IoT system consists of a transmitter Alice, a receiver Bob, a warden Willie, multiple potential relays and multiple energy harvesting jammers (EHJs). The IoT system employs a harvesting-then-jamming protocol. In this protocol, Alice first sends public information to a selected relay (RS), forwarding it to Bob, and EHJs harvest energy from Alice. Alice then sends public and covert information simultaneously, and a selected EHJ sends AN to prevent Willie from detecting covert information transmissions. It is note that Alice is directly connected to a power supply and thus can provide enough energy for these energy-limited EHJs.

A. Channel Model

We adopt an independent quasi-static Rayleigh fading model as the channel model used in this scenario, where each channel remains unchanged within the same time slot and changes independently in different time slots. We model the channel coefficients as complex Gaussian random variables with zero mean and unit variance. There are a total of six channels in the system, namely the channel from Alice to RS, the one from Alice to EHJ, the one from Alice to Willie, the one from RS to Bob, the one from EHJ to RS, and the channel from EHJ to Willie. Their channel coefficients are represented as h_{ar}, h_{aj}, h_{aw}, h_{rb}, h_{jr} and h_{jw}, respectively. $|h_x|^2$ is the channel gain, where $x \in \{ar, aj, aw, rb, jr, jw\}$, and the path loss of the signals is included in the channel gain. We assume that Alice knows $|h_{ar}|^2$ and $|h_{aj}|^2$, RS knows $|h_{ar}|^2$ and $|h_{rb}|^2$, each EHJ knows $|h_{jr}|^2$ and $|h_{jw}|^2$, and Willie knows $|h_{aw}|^2$ and $|h_{jw}|^2$. We assume that the noise is AWGN with variance σ^2, and the system bandwidth is W MHz. Without loss of generality, we assume W=1 in this paper.

B. Harvesting-then-Jamming Protocol

We employ a harvesting-then-jamming protocol as the transmission model. Under this model, time is evenly divided into time slots of size T, and each time slot is further divided into two sub time slots for the energy harvesting with time switching. The energy harvesting phase occurs in the first sub time slot, and the jamming phase occurs in the second sub time slot, which are summarized as follows.

1)Energy harvesting phase: In this phase, Alice sends a public message, and RS receives the message and forwards it to Bob. All EHJs can harvest the energy from Alice's emitted message during this phase. The duration of this phase is ϖT, where ϖ is the time-switching factor, and the harvested energy by the energy harvesting jammer in this phase can be expressed as

$$E = \mu \varpi T P_a |h_{aj}|^2, \quad (1)$$

where μ is the energy conversion efficiency.

2)Jamming phase: In this phase, Alice may send covert messages while sending public messages. A selected EHJ utilizes the harvested energy to send jamming signals to confuse Willie's detection. The transmit power P_j of EHJ satisfies

$$P_j \le \frac{E}{(1-\varpi)T} = \frac{\mu\varpi P_a |h_{aj}|^2}{(1-\varpi)}. \quad (2)$$

It is observed from formula (2) that the range of P_j can be flexibly controlled by setting the value of time-switching factor ϖ.

C. Performance Metrics

In the jamming phase, Alice has two possible states. One state is that Alice sends covert messages to Bob (i.e., H_1) and another is that it does not do covert transmissions (i.e., H_0). Then, we define two performance metrics used in this paper.

1)Detection error probability: It refers to the probability that Willie mistakenly determines whether Alice sends a covert message. Its expression is given by the following equation:

$$\phi = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \quad (3)$$

where ϕ represents the detection error probability of Willie, $\mathbb{P}_{FA}$ is the false alarm probability, indicating that Willie believes that Alice sent a covert message (H_1), but actually Alice did not send one (H_0); $\mathbb{P}_{MD}$ is the missed probability, indicating that Willie thinks that Alice did not send a covert message (H_0), but actually sent (H_1).

2)Covert throughput: It refers to the maximum achievable rate at which Alice can send covert messages to RS satisfying covert requirement constraint.

III. Relay and Energy Harvesting Jammer Selection Strategy

In this section, we introduce two strategies for relay and energy harvesting jammer selection, namely random selection and QoS-aware selection.

A. Random Selection Strategy

The random selection strategy aims to randomly select an EHJ and a relay. Such a strategy can reduce system's computational complexity and communication overhead, and usually can also achieve a moderate system performance.

1)Transmission with Alice not sending a covert message under the random selection strategy: We consider the scenario where Alice transmits a public message with a power of P_{ar} under the random selection strategy, where $P_{ar} \le P_{max}$. Here, P_{max} represents the maximum transmit power of Alice. At this time, the signal received at RS is given by

$$y_r = \sqrt{P_{ar}} h_{ar} x_p[i] + \sqrt{P_j} h_{jr} x_j[i] + n_r[i], \quad (4)$$

where x_p represents the signal transmitted by Alice, x_j is the interference signal, i is the channel usage index, and $n_r \sim \mathcal{CN}(0, \sigma_r^2)$ represents the noise received at RS.

Therefore, the signal-to-interference-plus-noise ratio at RS ($SINR_r$) can be expressed as

$$\mathrm{SINR_r} = \frac{P_{ar}|h_{ar}|^2}{P_j|h_{jr}|^2 + \sigma_r^2}. \quad (5)$$

2)Transmission with Alice sending a covert message under the random selection strategy: Alice transmits a covert message with a power of P_{ac} on top of transmitting a public message. Here, $P_{ar} + P_{ac} \le P_{max}$. Then, the signal received at RS expressed as

$$y_r = \sqrt{P_{ar}} h_{ar} x_p[i] + \sqrt{P_{ac}} h_{ar} x_c[i] + \sqrt{P_j} h_{jr} x_j[i] + n_r[i], \quad (6)$$

where x_c represents the covert message.

Since we prioritize the transmission of public messages, RS will first decode the public message upon receiving message from Alice. In this case, the covert message is treated as noise. Therefore, the $SINR_r$ is presented as

$$\mathrm{SINR_r} = \frac{P_{ar}|h_{ar}|^2}{P_{ac}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2} \quad (7)$$

B. QoS-aware Selection Strategy

The basic idea of the QoS-aware Selection Strategy algorithm in Algorithm 1 is summarized as follows. We first determine an optimal relay. It corresponds to the relay that its channel gain is the maximum one of the minimum channel gains (i.e., min ($|h_{ar_k}|^2$, $|h_{r_k b}|^2$)) for all potential relays. We then determine an optimal jammer. It corresponds to the jammer which can interfere with Willie as much as possible while reducing the negative affection on the optimal relay. The optimal jammer is selected by finding the maximum value of $|h_{j_{zw}}|^2/|h_{j_z r_k}|^2$ for all potential jammers, where $|h_{j_{zw}}|^2$ represents the channel gain between each jammer and Willie, and $|h_{j_z r_k}|^2$ represents the channel gain between the jammer and the optimal relay.

1)Transmission with Alice not sending a covert message under the QoS-aware selection strategy: When Alice transmits only a public message, the signal received at RS is given by

$$y_r = \sqrt{P_{ar}^*} h_{ar} x_p[i] + \sqrt{P_j} h_{jr} x_j[i] + n_r[i], \quad (8)$$

where P_{ar}^* refers to the power that Alice to send public message.

The $SINR_r$ can be expressed as

$$\mathrm{SINR_r} = \frac{P_{ar}^*|h_{ar}|^2}{P_j|h_{jr}|^2 + \sigma_r^2}, \quad (9)$$

Under the QoS-aware selection strategy, we adopt a non-interruptive approach to ensure the continuity and stability of the communication link. For the system, interruption does not occur when the channel rate C_{ar} from Alice to RS is no less than the signal threshold R required at RS, i.e., $R \le C_{ar}$, where $C_{ar} = \log_2(1 + \mathrm{SINR_r})$. Then, we get $|h_{ar}|^2 \ge \eta\,(P_j|h_{jr}|^2 + \sigma_r^2)/P_{ar}^*$, where $\eta = 2^R - 1$. Since $P_{ar}^* \le P_{max}$, we set the value of P_{ar}^* as

$$P_{ar}^* = \begin{cases} \frac{\eta(P_j|h_{jr}|^2 + \sigma_r^2)}{|h_{ar}|^2}, & \text{if} |h_{ar}|^2 \ge \frac{\eta\left(P_j|h_{jr}|^2 + \sigma_r^2\right)}{P_{max}} \\ 0, & \text{else.} \end{cases} \quad (10)$$

Algorithm 1: Quality of Service (QoS)-aware selection

Input: Relay number k, EHJ number z, Channel gain from Alice to the k-th relay $|h_{ar_k}|^2$, Channel gain from the k-th relay to Bob $|h_{r_kb}|^2$, Channel gain from the z-th EHJ to the k-th relay $|h_{j_zr_k}|^2$, Channel gain from the z-th EHJ to Willie $|h_{j_zw}|^2$

Output: Optimal relay number k*, Optimal EHJ number z*.

1: Initialization: Set k = 1, z = 1, k* = 1, z* = 1, M = min ($|h_{ar_k}|^2, |h_{r_kb}|^2$).
2: **for** k = 2, 3... **do**
  if min ($|h_{ar_k}|^2, |h_{r_kb}|^2$) > M **then**
    Update optimal channel gain M = min ($|h_{ar_k}|^2, |h_{r_kb}|^2$).
    Update optimal relay number k* = k.
  end if
end for
3: Set J = $|h_{j_zw}|^2/|h_{j_zr_{k*}}|^2$;
4: **for** z = 2, 3... **do**
  if $|h_{j_zw}|^2/|h_{j_zr_{k*}}|^2$ > J **then**
    J = $|h_{j_zw}|^2/|h_{j_zr_{k*}}|^2$;
    Update optimal EHJ z* = z.
  end if
end for

2)Transmission with Alice sending a covert message under the QoS-aware selection strategy: When Alice transmits a covert message on top of sending a public message, the signal received at RS is given by

$$y_r = \sqrt{P_{ar}^{\#}}h_{ar}x_p[i] + \sqrt{P_{ac}}h_{ar}x_c[i] + \sqrt{\mathrm{P_j}}\mathrm{h_{jr}x_j[i]} + n_r[i], \quad (11)$$

where $P_{ar}^{\#}$ is the power of Alice sending a public message. Because the priority of public message transmission task is high, we first regard the transmission of covert message as interference, so $\mathrm{SINR_r}$ is given by

$$\mathrm{SINR_r} = \frac{P_{ar}^{\#}|h_{ar}|^2}{P_{ac}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2}. \quad (12)$$

We also set the value of $\mathrm{P_{ar}^{\#}}$ in a non-interrupt way, according to $R \le C_{ar}$, then we can get $|h_{ar}|^2 \ge \eta(|h_{jr}|^2 + \sigma_r^2)/(P_{ar}^{\#} - \eta P_{ac})$ .Since $P_{ar}^{\#} + P_{ac} \le P_{max}$, we get $|h_{ar}|^2 \ge \eta(|h_{jr}|^2 + \sigma_r^2)/(P_{max} - (1+\eta)P_{ac})$. Thus

$$P_{ar}^{\#} = \begin{cases} \frac{\eta(P_{ac}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2)}{|h_{ar}|^2}, & \text{if} |h_{ar}|^2 \ge \frac{\eta\left(P_j|h_{jr}|^2 + \sigma_r^2\right)}{(P_{max} - (1+\eta)P_{ac})}, \\ \frac{\eta(P_j|h_{jr}|^2 + \sigma_r^2)}{|h_{ar}|^2}, & \text{if } \frac{\eta(P_j|h_{jr}|^2 + \sigma_r^2)}{P_{max}} \le |h_{ar}|^2 < \frac{\eta\left(P_j|h_{jr}|^2 + \sigma_r^2\right)}{(P_{max} - (1+\eta)P_{ac})}, \\ 0, & \text{else.} \end{cases} \quad (13)$$

Since the channel gain threshold for transmitting covert message is $|h_{ar}|^2 \ge \eta(|h_{jr}|^2 + \sigma_r^2)/(P_{max} - (1+\eta)P_{ac})$, we can obtain the range of values for P_{ac} under the QoS-aware selection strategy as $P_{ac} \in (0, (P_{max} - \eta(P_j|h_{jr}|^2 + \sigma_r^2)/|h_{ar}|^2)/(1+\eta)]$.

IV. Detection Error Probability

The detection error probability represents Willie's probability of making incorrect judgments about covert message transmission behavior. Generally, the higher the probability of detecting errors, the more secure the communication is. In this section, we will calculate detection error probability defined as the sum of the false alarm probability and miss detection probability under each selection strategy. Addition-ally, optimal detection thresholds will be provided.

A. Detection Error Probability Under Random Selection Strategy

We employ Willie's hypothesis testing to determine whether Alice is transmitting a covert message.

1)Willie's hypothesis testing: Under Willie's null hypothesis (i.e., Alice not transmitting covert message) and alternative hypothesis (i.e., Alice transmitting covert message), the received signal at Willie is given by the following equation:

$$y_w = \begin{cases} \rho + \sqrt{P_j}h_{jw}x_j[i] + n_w[i], & H_0, \\ \rho + \sqrt{P_{ac}}h_{aw}x_c[i] + \sqrt{P_j}h_{jw}x_j[i] + n_w[i], & H_1, \end{cases} \quad (14)$$

where $\rho = \sqrt{P_{ar}}h_{aw}x_p[i]$ and $\mathrm{n_w} \sim \mathcal{CN}(0, \sigma_w^2)$ represents the noise at Willie.

Considering the Willie radiometer, we have

$$T_w \underset{D_0}{\overset{D_1}{\gtrless}} \tau, \quad (15)$$

where $T_w = \sum_{i=1}^{n} |y_w[i]|^2/n$, n is the number of usage of the channels, τ is the signal detection threshold at Willie that will be determined next, and D_0 and D_1 indicate the decision benefiting H_0 and H_1, respectively. We let $n \to \infty$ and using the strong law of large numbers [30-34], we can give T_w as

$$T_w = \begin{cases} P_{ar}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2, & H_0, \\ P_{ar}|h_{aw}|^2 + P_{ac}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2, & H_1. \end{cases} \quad (16)$$

2)Detection error probability at Willie: The detection error probability at Willie is given by (3), and then we derive $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$ as

$$\begin{aligned} \mathbb{P}_{FA} &= P(P_{ar}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2 \ge \tau) \\ &= P(|h_{aw}|^2 \ge \frac{\tau - P_j|h_{jw}|^2 - \sigma_w^2}{P_{ar}}) \\ &= \int_0^{\infty} \int_{\frac{\tau - P_j y - \sigma_w^2}{P_{ar}}}^{\infty} f_{|h_{aw}|^2}(x) f_{|h_{jw}|^2}(y)\, dx dy \\ &= \int_0^{\infty} \int_{\frac{\tau - P_j y - \sigma_w^2}{P_{ar}}}^{\infty} e^{-x} e^{-y}\, dx dy \end{aligned}$$

$$= \begin{cases} \frac{P_{ar}}{P_{ar}-P_j} e^{\frac{\sigma_w^2-\tau}{P_{ar}}}, & \text{if } \tau \geq P_j|h_{jw}|^2+\sigma_w^2, \\ 1, & \text{else}, \end{cases} \quad (17)$$

and

$$\mathbb{P}_{MD} = P(P_{ar}|h_{aw}|^2 + P_{ac}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2 < \tau)$$
$$= P(|h_{aw}|^2 < \frac{\tau - P_j|h_{jw}|^2 - \sigma_w^2}{P_{ar}+P_{ac}})$$
$$= \int_0^{\infty} \int_0^{\frac{\tau - P_j y - \sigma_w^2}{P_{ar}+P_{ac}}} f_{|h_{aw}|^2}(x) f_{|h_{jw}|^2}(y)\, dx dy$$
$$= \int_0^{\infty} \int_0^{\frac{\tau - P_j y - \sigma_w^2}{P_{ar}+P_{ac}}} e^{-x} e^{-y}\, dx dy$$
$$= \begin{cases} 1 - \frac{(P_{ar}+P_{ac})}{P_{ar}+P_{ac}-P_j} e^{\frac{\sigma_w^2-\tau}{P_{ar}+P_{ac}}}, & \text{if } \tau > P_j|h_{jw}|^2+\sigma_w^2, \\ 0, & \text{else}. \end{cases} \quad (18)$$

From the above two formulas, we can conclude that P_j needs to meet $P_j < \mathrm{P_{ar}}$. Since $P_j \leq \mu\varpi T P_a |h_{aj}|^2/(1-\varpi)$, the value range of P_j under the random selection strategy is $P_j \in [0, min\{P_{ar}, \mu\varpi T P_a|h_{aj}|^2/(1-\varpi)\})$, and the detection error probability at Willie is given by the following equation

$$\phi = \begin{cases} 1 - \frac{(P_{ar}+P_{ac})}{P_{ar}+P_{ac}-P_j} e^{\frac{\sigma_w^2-\tau}{P_{ar}+P_{ac}}} + \frac{P_{ar}}{P_{ar}-P_j} e^{\frac{\sigma_w^2-\tau}{P_{ar}}}, & \text{if } \tau > \tau_1, \\ 1, & \text{else}, \end{cases} \quad (19)$$

where $\tau_1 = P_j|h_{jw}|^2 + \sigma_w^2$.

As can be seen from the above equation, in the detection threshold of Willie $\tau \leq P_j|h_{jw}|^2 + \sigma_w^2$, the detection error probability is 1, which means that whether Alice sent covert message at this time, Willie cannot correctly judge the transmission behavior of Alice. Thus, we will not investigate this case. The covert constraint is defined as $\phi > 1-\varepsilon$, where ε is the covert requirement, this formula means that when ε take any value between 0 and 1, the total detection error probability ϕ is always greater than $1-\varepsilon$. We consider the worst-case for Willie, i.e., minimum detection error probability. To this end, we derive the optimal detection threshold for Willie. We differentiate ϕ with respect to τ and get

$$\frac{\partial \phi}{\partial \tau} = \frac{(P_{ar}+P_{ac})}{P_{ar}+P_{ac}-P_j} * \frac{1}{P_{ar}+P_{ac}} e^{\frac{\sigma_w^2-\tau}{P_{ar}+P_{ac}}} - \frac{P_{ar}}{P_{ar}-P_j} * \frac{1}{P_{ar}} e^{\frac{\sigma_w^2-\tau}{P_{ar}}} = 0. \quad (20)$$

Then we get

$$\tau_{opt} = \frac{P_{ar}(P_{ar}+P_{ac})}{P_{ac}} ln \frac{P_{ar}+P_{ac}-P_j}{P_{ar}-P_j} + \sigma_w^2. \quad (21)$$

The τ_{opt} is the extreme point of ϕ .When $\tau > \tau_{opt}$, $\partial\phi/\partial\tau > 0$, and when $\tau < \tau_{\mathrm{opt}}$, $\partial\phi/\partial\tau < 0$, so τ_{opt} is the minimum point, which is the optimal detection threshold for Willie. Taking τ_{opt} into ϕ yields the minimum detection error probability ϕ_{opt} for Willie.

B. Detection Error Probability Under QoS-aware Selection Strategy

1)Willie's hypothesis testing： Under the QoS-aware selection strategy, due to the influence of channel gain on the transmission power of Alice for transmitting public message, the received signal at Willie can be expressed as

$$y_w = \begin{cases} \mathrm{ρ}_1 + \sqrt{P_j} h_{jw} x_j[i] + n_w[i], & H_0, \\ \mathrm{ρ}_2 + \sqrt{P_{ac}} h_{aw} x_c[i] + \sqrt{P_j} h_{jw} x_j[i] + n_w[i], & H_1. \end{cases} \quad (22)$$

where $\mathrm{ρ}_1 = \sqrt{P_{ar}^*} h_{aw} x_p[i]$, $\mathrm{ρ}_2 = \sqrt{P_{ar}^{\#}} h_{aw} x_p[i]$.

Using the law of large numbers, we obtain the received power at Willie as

$$T_w = \begin{cases} P_{ar}^*|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2, & H_0, \\ P_{ar}^{\#}|h_{aw}|^2 + P_{ac}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2, & H_1. \end{cases} \quad (23)$$

2)Detection error probability at Willie: According to (3), we obtain

$$\mathbb{P}_{FA} = P\left(\frac{\eta\left(P_j|h_{jr}|^2+\sigma_r^2\right)}{|h_{ar}|^2}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2 \geq \tau\right)$$
$$= P(|h_{aw}|^2 \geq \frac{\tau - P_j|h_{jw}|^2 - \sigma_w^2}{\eta(P_j|h_{jr}|^2+\sigma_r^2)}|h_{ar}|^2)$$
$$= \int_0^{\infty} \int_{\frac{\tau - P_j|h_{jw}|^2 - \sigma_w^2}{\eta(P_j|h_{jr}|^2+\sigma_r^2)}|h_{ar}|^2}^{\infty} f_{|h_{aw}|^2}(x) f_{|h_{jw}|^2}(y)\, dx dy$$
$$= \int_0^{\infty} \int_{\frac{\tau - P_j|h_{jw}|^2 - \sigma_w^2}{\eta(P_j|h_{jr}|^2+\sigma_r^2)}|h_{ar}|^2}^{\infty} e^{-x} e^{-y}\, dx dy$$
$$= \begin{cases} \frac{\alpha}{\alpha - P_j} e^{-\frac{\gamma}{\alpha}}, & \text{if } \tau > \tau_1, \\ 1, & \text{else}, \end{cases} \quad (24)$$

where $\alpha = \eta(P_j|h_{jr}|^2 + \sigma_r^2)/|h_{ar}|^2$, $\gamma = \tau - \sigma_w^2$,and

$$\mathbb{P}_{MD} = P(\frac{\eta(P_{ac}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2)}{|h_{ar}|^2}|h_{aw}|^2 + P_{ac}|h_{aw}|^2 + P_j|h_{jw}|^2 + \sigma_w^2 < \tau)$$
$$= P(|h_{aw}|^2 < \frac{\gamma - P_j|h_{jw}|^2}{\alpha+\beta})$$
$$= \int_0^{\infty} \int_{\frac{\tau - P_j|h_{jw}|^2 - \sigma_w^2}{\eta(P_j|h_{jr}|^2+\sigma_r^2)}|h_{ar}|^2}^{\infty} f_{|h_{aw}|^2}(x) f_{|h_{jw}|^2}(y)\, dx dy$$
$$= \int_0^{\infty} \int_0^{\frac{\gamma - P_j y}{\alpha+\beta}} e^{-x} e^{-y}\, dx dy$$
$$= \begin{cases} 1 - \frac{\alpha+\beta}{\alpha+\beta-P_j} e^{\frac{\gamma}{\alpha+\beta}}, & \text{if } \tau > \tau_1, \\ 0, & \text{else}, \end{cases} \quad (25)$$

where $\beta = (1+\eta)P_{ac}$.From the above two formulas, we know that $\alpha - P_j > 0$ .When $|h_{ar}|^2 > \eta|h_{jr}|^2$, $P_j \in [0, min\{\eta\sigma_r^2/(|h_{ar}|^2 - \eta|h_{jr}|^2, \mu\varpi TP_a|h_{aj}|^2/(1-\varpi)\})$. When $|h_{ar}|^2 < \eta|h_{jr}|^2$, $P_j \in [0,\ \mu\varpi TP_a|h_{aj}|^2/(1-\varpi)]$. Then, we can get it according to (3)

$$\phi = \begin{cases} 1 - \frac{\alpha+\beta}{\alpha+\beta-P_j} e^{\frac{\gamma}{\alpha+\beta}} + \frac{\alpha}{\alpha-P_j} e^{-\frac{\gamma}{\alpha}}, & \text{if } \tau > \tau_1, \\ 1, & \text{else.} \end{cases} \quad (26)$$

We differentiate ϕ with respect to τ and get

$$\frac{\partial\phi}{\partial\tau} = \frac{\alpha+\beta}{\alpha+\beta-P_j} * \frac{1}{\alpha+\beta} e^{\frac{\gamma}{\alpha+\beta}} - \frac{\alpha}{\alpha-P_j} * \frac{1}{\alpha} e^{-\frac{\gamma}{\alpha}} = 0. \quad (27)$$

Then, we have

$$\tau_{opt} = \frac{\alpha(\alpha+\beta)}{\beta} \ln \frac{\alpha+\beta-P_j}{\alpha-P_j} + \sigma_w^2. \quad (28)$$

We now judge whether the τ_{opt} is a minimum value. When $\tau < \tau_{opt}$,$\partial\phi/\partial\tau$ is less than 0, and when $\tau > \tau_{opt}$, $\partial\phi/\partial\tau$ is greater than 0. Thus, τ_{opt} is the optimal detection threshold of Willie. Taking τ_{opt} into ϕ yields the minimum detection error probability ϕ_{opt} for Willie.

V. Covert Throughput Modeling And Optimization

In this section, we provide the expressions for the covert throughput and maximize the covert throughput under each selection strategy.

A. Covert Throughput Modeling Under The Random Selection Strategy

Our defined covert throughput is the product of the probability of uninterrupted public information transmission and the channel rate when sending covert information. The covert throughput κ can be modeled as

$$\kappa = \varrho\varphi(H_1), \quad (29)$$

where ϱ is the channel rate when Alice transmits covert message to RS, and $\varphi(H_1)$ indicates the probability that the transmission from Alice to RS does not interrupt when H_1 is true.

1)The probability of no interruption: The transmission will not interrupt only if the channel rate from Alice to RS is greater than a given threshold R required by RS. The channel rate is given based on the Shannon formula, and therefore we have

$$\begin{aligned} \varphi(H_1) &= P(\log_2(1+\mathrm{SINR_r}) \geq \mathrm{R}) \\ &= P(1 + \frac{P_{ar}|h_{ar}|^2}{P_{ac}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2} \geq R) \\ &= P(|h_{ar}|^2 \geq \frac{\eta(P_j\mathcal{Y} + \sigma_r^2)}{P_{ar} - \eta P_{ac}}) \\ &= \int_0^\infty \int_{\frac{\eta(P_j|h_{jr}|^2+\sigma_r^2)}{P_{ar}-\eta P_{ac}}}^\infty e^{-x} e^{-\mathcal{Y}} dx d\mathcal{Y} \\ &= \frac{P_{ar} - \eta P_{ac}}{P_{ar} - \eta P_{ac} + \eta P_j} e^{-\frac{\eta\sigma_r^2}{P_{ar}-\eta P_{ac}}}. \end{aligned} \quad (30)$$

From the above formula, we know $P_{ar} - \eta P_{ac} > 0$, and because $P_{ar} + P_{ac} \leq P_{max}$, $P_{ac} \in (0, P_{max}/(1+\eta)]$.

2) Covert throughput: According to (29), we can express the covert throughput as

$$\begin{aligned} \kappa &= \varrho\varphi(H_1) \\ &= \delta \log_2\left(1 + \frac{P_{ac}|h_{ar}|^2}{P_{ar}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2}\right), \end{aligned} \quad (31)$$

where $\delta = \frac{P_{ar}-\eta P_{ac}}{P_{ar}-\eta P_{ac}+\eta P_j} e^{-\frac{\eta\sigma_r^2}{P_{ar}-\eta P_{ac}}}$.

3)Covert throughput optimization: Our objective is to maximize the covert throughput while ensuring that Willie's detection error probability meets covert requirement. It can be represented by the following optimization formula

$$\max_{P_{ac}, P_j} \quad \kappa, \quad (32a)$$

$$s.t. \ \phi_{opt} > 1 - \varepsilon, \quad (32b)$$

$$0 < P_{ac} \leq \frac{P_{max}}{1+\eta}, \quad (32c)$$

$$0 < P_j < min\left\{P_{ar}, \mu\varpi P_a|h_{aj}|^2/(1-\varpi)\right\}, \quad (32d)$$

where ϕ_{opt} is the minimum detection error probability of Willie. We use adaptive moment estimation algorithm (Adam) [35]to find the optimal values of P_{ac} and P_j that maximize the covert throughput while satisfying $\phi_{opt} > 1 - \varepsilon$. The basic idea of the Adam algorithm in Algorithm 2 is summarized as follows.

Initially, we give the initial values of P_{ac} and P_j, and set the estimates of the first and second moments to zero. In each iteration, we first compute the objective function κ based on the current values of P_{ac} and P_j. Next, numerical differentiation is used to calculate the gradients P_{ac}^{grad} and P_j^{grad} of these two parameters P_{ac} and P_j. Subsequently, we update the first and second moment estimates and apply bias correction. Finally, P_{ac} and P_j are updated based on the corrected gradients and the learning rate α. During the update process, the algorithm checks whether the parameters satisfy the predefined constraints. If the constraints are violated, the current update is skipped. After multiple iterations, the algorithm outputs the optimized parameters P_{ac} and P_j, thus finding the optimal solution that meets the specified constraints.

B. Covert Throughput Modeling Under QoS-aware Selection Strategy

1)Covert throughput: Since Alice transmits public message without interruption, the probability of uninterrupted public information transmission is 1, so the covert throughput is equal to the channel rate at which Alice transmits covert message. It is given by the following equation:

$$\begin{aligned} \kappa &= \varrho\ \varphi(H_1) \\ &= \log_2(1 + \frac{P_{ac}|h_{ar}|^2}{\eta(P_{ac}|h_{ar}|^2 + P_j|h_{jr}|^2 + \sigma_r^2) + P_j|h_{jr}|^2 + \sigma_r^2}). \end{aligned} \quad (33)$$

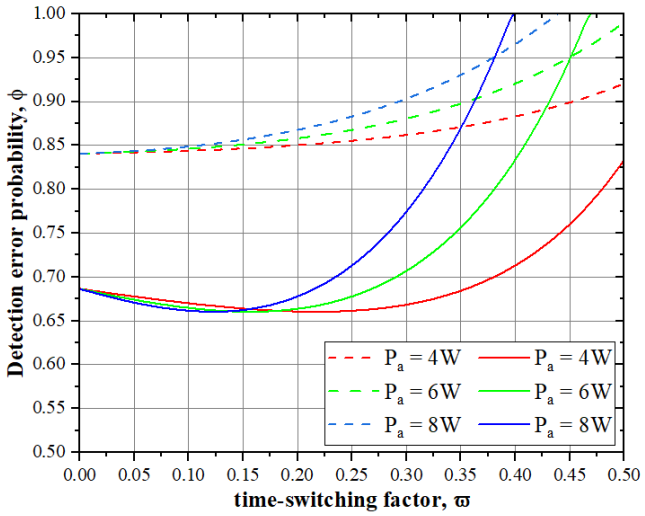


Fig. 2 Impact of time-switching factor on detection error probability

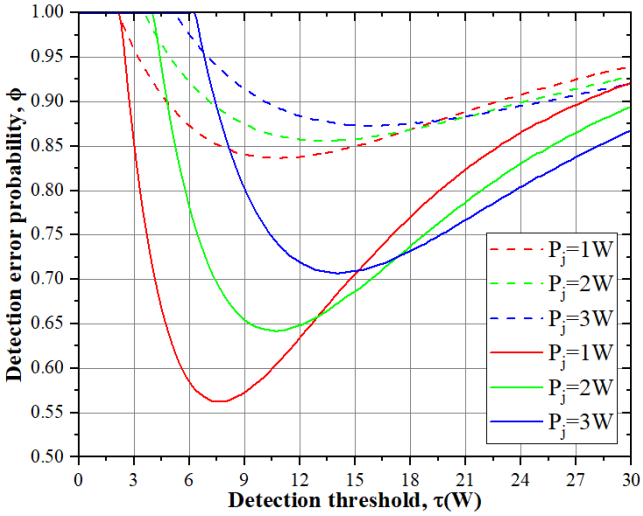


Fig. 3 Impact of detection threshold on detection error probability

2) Covert throughput optimization: By providing the optimal detection error probability for Willie, as well as the range of values for P_{ac} and P_j, we perform Adam algorithm to find the maximum covert throughput. The expression is given by the following equation:

$$\max_{P_{ac},\ P_j} \quad \kappa, \tag{34a}$$

$$s.t. \phi_{opt} > 1-\varepsilon, \tag{34b}$$

$$0 < P_{ac} \le \frac{P_{max} - \frac{\eta\left(P_j|h_{jr}|^2+\sigma_r^2\right)}{|h_{ar}|^2}}{1+\eta}, \tag{34c}$$

$$0 < P_j < \begin{cases} \varpi_1, & \text{if } |h_{ar}|^2 > \eta|h_{jr}|^2, \\ \varpi_2, & else, \end{cases} \tag{34d}$$

where $\varpi_1 = min\{\eta\sigma_r^2/(|h_{ar}|^2-\eta|h_{jr}|^2, \mu\varpi P_a|h_{aj}|^2/(1-\varpi)\}$,$\varpi_2 = \mu\varpi P_a|h_{aj}|^2/(1-\varpi)$.

VI. Numerical Results

In this section, we will present and analyze the experimental results, revealing the impacts of system parameters on covert performances in terms of detection error probability and covert throughput under each selection strategies. Unless otherwise specified, the following system parameters are set as $\mu = 0.8, \varpi = 0.5, \mathrm{R} = 1\ \mathrm{Mb/s/Hz}, \sigma_r^2 = \sigma_w^2 = 0\ \mathrm{dB}, \mathrm{P_{max}} = 16\mathrm{W}, \mathrm{P_a} = 12\mathrm{W}$.In the following figures, the dashed lines represent the results under the random selection strategy, while the solid lines represent the results under the QoS-aware selection strategy.

A. Analysis Of Detection Error Probability At Willie's Location

To explore the effect of time switching factor ϖ on the detection error probability ϕ, we summarize in Fig.2 how ϕ varies with ϖ under each selection strategy with a setting of τ=10W, P_{ac}=3W, and P_a = {4,6,8} W. We can see from the Fig. 2 that the curve shows an increasing trend under the random selection strategy. This can be explained as follows. The increase of the time-switching factor ϖ means the increase of EHJ harvesting energy time and decrease of its releasing energy time. Since we consider that EHJ releases all harvested energy at the phase 2, the interference power P_j increases according to equation (2). Thus, the detection error probability ϕ increases with the increase of P_j. Another observation from Fig. 2 is that for each fixed setting of ϖ, the higher the power P_a of the phase 1, the higher the detection error probability. This is because the higher the emission power P_a, the more energy the EHJ can harvest, and thus the more energy will be converted into the interference power P_j. However, under the QoS-aware selection strategy, the curve shows the trends of decreasing first and then increasing, which is because when the time switching factor ϖ is relatively small, the detection error probability ϕ is dominated by the missed detection probability $\mathbb{P}_{MD}$, while we can see from formula (25) that the missed detection probability $\mathbb{P}_{MD}$ decreases with the increase of the interference power P_j. With the increase of ϖ, the false alarm probability $\mathbb{P}_{FA}$ gradually becomes the dominant one, while in (24), the false alarm probability $\mathbb{P}_{FA}$ increases with the increase of the interference power P_j, so the curve gradually rises. For a fixe setting of ϖ, the increase of P_a leads to a decrease and then an increase in the detection error probability ϕ.

Then we delve into the relationship between the detection error probability ϕ at Willie and the detection threshold τ under different interference powers for the two selection strategies. As illustrated in Fig. 3, the detection error probabilities under both selection strategies initially increase and then decrease with the detection threshold. This behavior arises from the composition of the detection error probability, consisting of the false alarm probability $\mathbb{P}_{FA}$ and the missed detection probability $\mathbb{P}_{MD}$. The former is a monotonically decreasing function with respect to the detection threshold, while the latter is a monotonically increasing function. When the detection threshold is relatively small, the influence of the threshold on $\mathbb{P}_{FA}$ is greater than that on $\mathbb{P}_{MD}$, resulting in a decreasing trend in the curve. As τ further increases, the impact on $\mathbb{P}_{FA}$ diminishes relative to $\mathbb{P}_{MD}$, leading to a gradual reduction in the rate of decrease in the

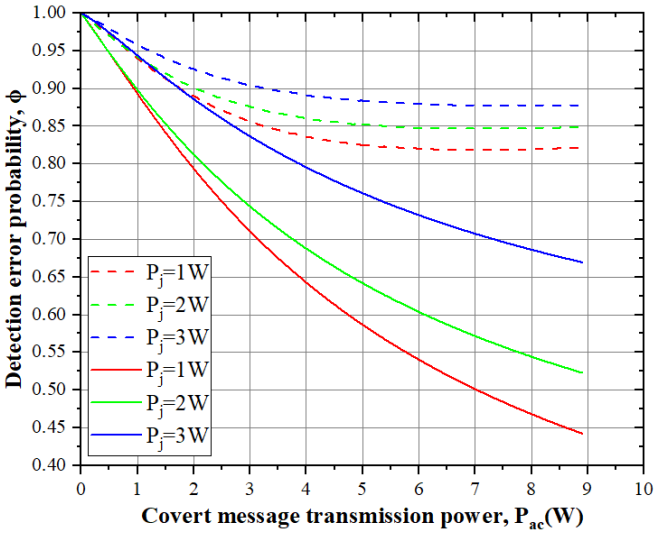


Fig. 4 Impact of cover message transmission power and interference on detection error probability

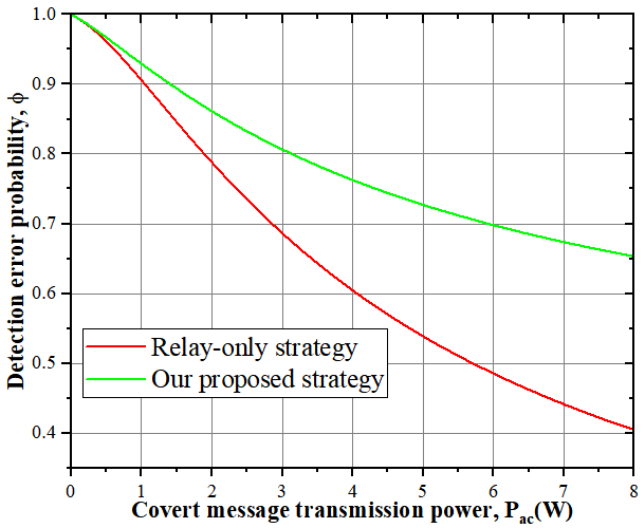


Fig. 5 Impact of cover message transmission power and jammer on detection error probability

detection error probability. Beyond the optimal detection threshold, the influence on $\mathbb{P}_{MD}$ surpasses that on $\mathbb{P}_{FA}$, causing an upward trend in the curve.

We further examine the trends of the curves under both selection strategies for $P_j = \{1, 2, 3\}$W. Regardless of the strategy, when τ is small, the detection error probability increases with the augmentation of P_j. This can be explained by the fact that a higher interference signal strength P_j released by Willie makes it more challenging to detect covert message transmission. When τ is relatively large, an increase in P_j will cause the influence of τ on $\mathbb{P}_{MD}$ to decrease relative to the impact on $\mathbb{P}_{FA}$. Consequently, this leads to a smoothing effect on the curve.

Through differentiation of the detection error probability, we ascertain that the optimal detection threshold increases with the growth of P_j. Consequently, the lowest point on the curve consistently decreases with the increase in P_j. Upon careful observation of the curves for both strategies, it is evident that the detection error probability under the random selection strategy is consistently higher than that under the QoS-aware selection strategy. This discrepancy is attributed to the non-interruptive manner in which Alice transmits public message in the QoS-aware selection strategy. In contrast, under the random selection strategy, an increase in the transmission power of public message is required to minimize interruption probability. This, in turn, results in an elevated detection error probability at Willie. Therefore, the detection error probability under the random selection strategy surpasses that under the QoS-aware selection strategy.

We present in Fig. 4 the relationship between the detection error probability at Willie and the covert transmission power at different P_j values under the two selection strategies. Obviously, for each selection strategy, with the increase of P_{ac}, the detection error probability always exhibits the decreasing trend. We can explain that when the covert message transmission power P_{ac} becomes bigger, Willie can detect the covert message transmission with higher probability (i.e., smaller detection error probability). For each fixed P_{ac}, the detection error probability always increases with the interference power P_j, due to the fact that the interference power P_j has negative effect on Willie's detection. Under the random selection strategy, we observe that as the value of P_{ac} is bigger, the value of detection error probability tends to keep unchanged. This is because to prevent interruption we need to increase the transmission power of public message on the basis of increasing P_{ac}, resulting in a almost constant detection error probability. This is also the reason that detection error probability is higher than that under the QoS-aware selection strategy.

We conduct a comparison between our proposed strategy and the relay-only strategy. We can see from Fig. 5 that the detection error probability at Willie under our proposed strategy is higher than that under the relay-only strategy. This can be explained as follows. Under our proposed strategy, the jammer injects noise to interfere with Willie, which increases the detection error probability at Willie.

In Fig. 6, we bring the optimal detection threshold under the two selection strategies into the expression of the detection error probability, aiming to explore the relationship between the optimal detection error probability and interference power between the channel gain $|h_{ar}|^2$ from Alice to RS. Throughout the whole graph, we can easily find that under each strategy, the optimal detection error probability at Willie always increases with the increase of interference power P_j, which can be explained by the optimal detection threshold formula obtained by our derivative. The increase of P_j will lead to an increase in the optimal detection threshold, and further lead to an increase in the detection error probability. Thus, the curve always exhibits an upward trend.

Under the random selection strategy, we observe that, when the value of the interference power P_j is fixed, increasing $|h_{ar}|^2$ causes a decrease in the optimal detection error probability. The reason is that for a better channel gain from Alice to RS, we do not need to have a high public message transmission power to ensure that the system transmission of public message does not interrupt, and thus an increase in $|h_{ar}|^2$ leads to a decrease in

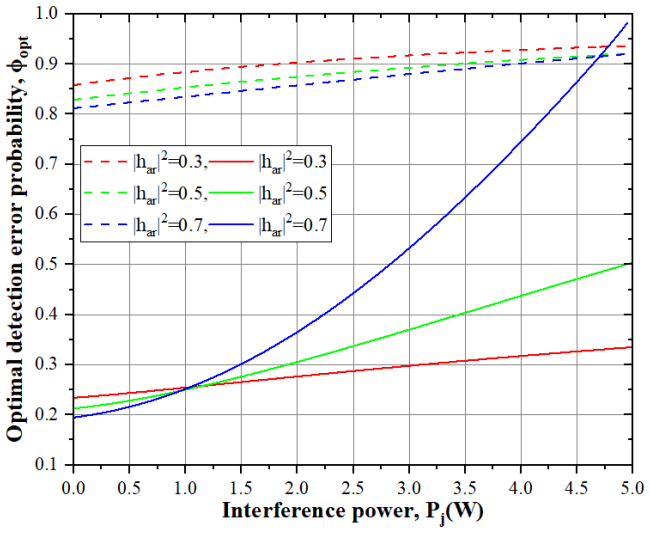


Fig. 6 Impact of interference power on optimal detection error probability

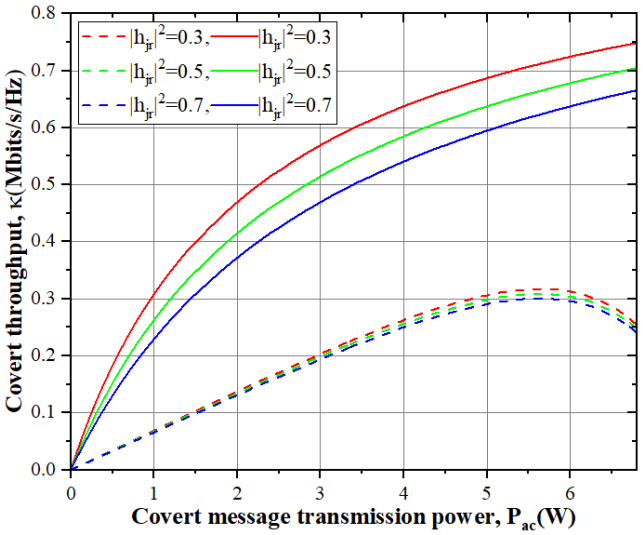


Fig. 7 impact of covert message transmission on covert throughput

P_{ar}, while the covert message transmission power P_{ac} remains unchanged. Therefore, Willie will be easier to detect the covert message transmission behavior. Under the QoS-aware selection strategy, we observe that the optimal detection threshold decreases with $|h_{ar}|^2$ at small interference power P_j, and the optimal detection threshold increases with $|h_{ar}|^2$ when P_j is large. The reason is as follows. Under the QoS-aware selection strategy, we use a non-interruptive mode to determine the public message transmission power P_{ar}. By (13), the value of P_{ar} will increase as the value of P_j increases, but decreases with the increase of $|h_{ar}|^2$. When the P_j is small, P_{ar} is more influenced by $|h_{ar}|^2$, and the $|h_{ar}|^2$ increase causes a decrease in P_{ar}, which leads to the decrease of the optimal detection error probability. However, with the increase in P_j, P_{ar} progressively larger influenced by P_j, and thus the required public message transmission power P_{ar} will become larger and larger, which leads to the optimal detection error probability with the increase of $|h_{ar}|^2$. By comparing the curves of the two strategies, we find that the optimal detection error probability under the random selection strategy is usually superior to the QoS-aware selection strategy. But for some special cases, when the value of P_j is infinitely close to the maximum value in the range of its values, it leads to a maximum optimal detection error probability.

B. Covert Throughput Analysis

We initially analyze the relationship between the covert throughput κ and covert message transmission power P_{ac} under two selection strategies when the channel gain $|h_{jr}|^2$ from EHJ to RS is set to {0.3, 0.5, 0.7}. As shown in Fig. 7, under the random selection strategy, we observe a trend where the curve first rises and then falls. This can be understood as follows: the initial ascent is due to the increase in P_{ac}, leading to an improvement in the system's signal-to-noise ratio. This implies that covert message becomes more accessible amid noise, reducing the error rate during transmission and causing the covert throughput to rise. However, when P_{ac} reaches a certain value, the limitation imposed by Alice's maximum transmission power P_{max} results in a relatively small public message transmission power P_{ar}. This significantly increases the probability of interruption in transmitting public message by Alice, negatively impacting the covert throughput and causing it to decline.

Under the QoS-aware selection strategy, the covert throughput exhibits an increasing trend without the subsequent decline observed in the random selection strategy. This is because we adopt a non-interruptive method to transmit public message, ensuring that no interruptions occur. Therefore, the covert throughput continues to rise. We also observe that under both strategies, when P_{ac} is fixed, a larger $|h_{jr}|^2$ results in a lower covert throughput. This can be easily explained: the increase in $|h_{jr}|^2$ signifies a stronger interference signal strength received by RS from EHJ, leading to increased interference noise. This makes it more challenging for RS to decode covert message. Therefore, when selecting an EHJ, a smaller $|h_{jr}|^2$ can better improve the effectiveness of covert communication.

Overall, comparing the covert throughput under the two strategies, we find that the covert throughput under the QoS-aware selection strategy is consistently higher than that under the random selection strategy. The specific reason for this is the interruption probability in the random selection strategy, leading to an overall decrease in the covert throughput.

Next, we explore the relationship between the covert throughput κ and interference power P_j when the channel gain from Alice to RS $|h_{ar}|^2$ varies under both strategies, with $|h_{ar}|^2$ ={0.3, 0.5, 0.7}. In Fig. 8, it is evident that κ decreases monotonically under both strategies. This is because an increase in interference power P_j reduces the SINR at RS, making it more challenging for RS to extract covert message from the noise. We also illustrate the impact of three different $|h_{ar}|^2$ values on κ when P_j is fixed. It is observed that, under the random selection strategy, the three different $|h_{ar}|^2$ values do not have a significant impact on the overall κ. However, under the QoS-aware selection strategy, a higher $|h_{ar}|^2$ leads to a larger κ. This is attributed to the fact that with an increase in

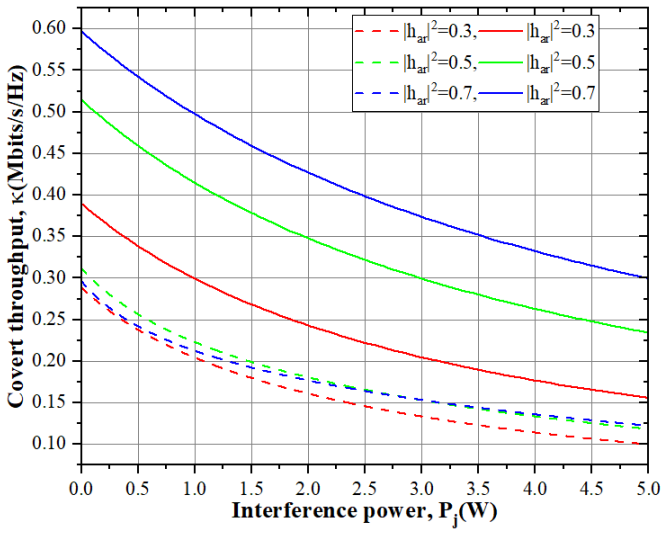


Fig. 8 impact of interference power on covert throughput

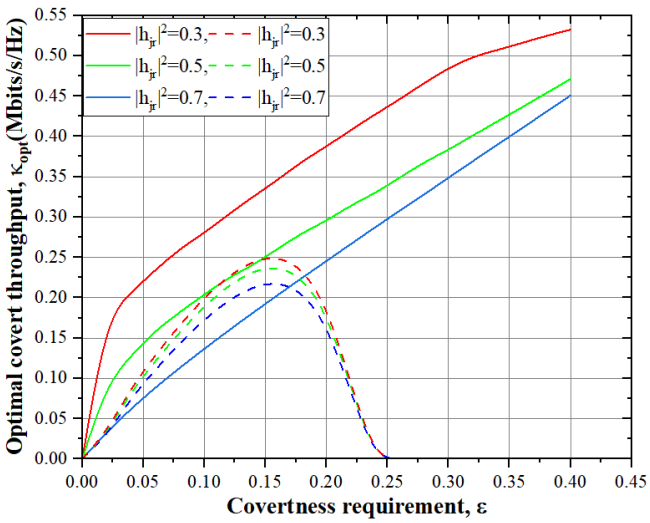


Fig. 9 impact of covert requirement on optimal covert throughput

$|h_{ar}|^2$, Alice only needs to emit a smaller public message transmission power P_{ar} to ensure interruption-free communication in the system. This results in an improved $SINR_r$, thereby enhancing κ. Therefore, when opting for the QoS-aware selection strategy, there is a preference for selecting higher-relay nodes to improve the covert communication environment.

In Fig. 9, we present the relationship between the optimal covert throughput κ_{opt} and the covert requirement ε under different $|h_{jr}|^2$ values, obtained by optimizing the values of covert message transmission power P_{ac} and interference power P_j. Under the random selection strategy, the curve exhibits an initial increase followed by a decrease. The initial increase is due to the increment in the covert requirement ε, leading to a reduction in the optimal detection error probability ϕ_{opt}. This results in a decrease in the optimal interference power P_j^{opt} and an increase in the optimal covert message transmission power P_{ac}^{opt}. While the decrease in P_j^{opt} and the increase in P_{ac}^{opt} both have positive effects on the SINR of covert message κ^T, further increments in P_{ac}^{opt} eventually make the public message transmission power P_{ar} relatively small, causing a significant increase in the interruption probability. The negative impact of the interruption probability outweighs the positive effects of increasing P_{ac}^{opt} and decreasing P_j^{opt}, leading to a subsequent decrease in the curve. Once the covert requirement ε reaches a certain level, P_{ar} becomes extremely small, resulting in an interruption, and the covert throughput κ_{opt} becomes zero.

Under the QoS-aware selection strategy, the curve exhibits an upward trend. This is due to the continuous increase in the optimal covert message transmission power P_{ac}^{opt} and the decrease in the optimal interference power P_j^{opt}, leading to an improvement in the SINR at RS and consequently an increase in the optimal covert throughput κ_{opt}. When the covert requirement ε remains constant and $|h_{jr}|^2$ increases, both-strategies show a decreasing trend in the optimal covert throughput κ_{opt}. This is because an increase in $|h_{jr}|^2$ enhances the interference from EHJ to RS, thereby negatively impacting the optimal covert throughput κ_{opt}. Additionally, when $|h_{jr}|^2 = 0.7$ and ε is relatively small, it is observed that the optimal covert throughput under the random selection strategy is greater than that under the QoS-aware selection strategy. However, in practice, under the random selection strategy, due to the influence of interruption probability, Alice typically needs to transmit public message with a relatively large power P_{ar}, which is not suitable for systems with constraints on maximum transmission power.

VII. Conclusion

This paper investigated covert communication assisted by energy harvesting jammers in a multi-relay system under two strategies for selecting relays and jammers. We derived the detection error probabilities under both strategies, and determine the optimal detection thresholds and optimal detection error probabilities. Then, we analyzed the covert throughput under both strategies and maximize the covert throughput by optimizing the transmission power of covert messages and interference power. We presented extensive numerical results to demonstrate the impacts of system parameters on covert performance under both strategies. Through experimentation, we find that the random selection strategy performs better in combating detections, while the QoS-aware selection strategy excels in achieving higher covert throughput. Thus, these two strategies can be carefully selected according to specific environmental requirements.

Algorithm 2: Adaptive Moment Estimation Algorithm

Input: Learning rate α, Exponential decay rates for the first and second moment estimates β_1 , β_2 , A small constant for numerical stability λ, Initial values for covert transmission power and interference power P_{ac}^0 , P_j^0 , Maximum number of iterations $\mathcal{L}$.

Output: P_{ac}^{opt} , P_j^{opt}

procedure κ (P_{ac}, P_j):

Check if the parameters satisfy the constraints and input P_{ac} and P_j for evaluation according to (31)(33)

return κ

end procedure

procedure ComputeGradient(P_{ac}, P_j, λ):

C = $\kappa(P_{ac}, P_j)$;

if C == -∞ then

return ∞, ∞

end if

Compute the gradient with respect to P_{ac}

P_{ac}^{grad} = ($\kappa(P_{ac} + \lambda, P_j)$ - $\kappa(P_{ac} - \lambda, P_j)$) / (2 * λ) ;

Compute the gradient with respect to P_j

P_j^{grad} = ($\kappa(P_{ac}, P_j + \lambda)$ - $\kappa(P_{ac}, P_j - \lambda)$) / (2 * λ);

return P_{ac}^{grad}, P_j^{grad}

end procedure

procedure AdamOptimization(P_{ac}^0, P_j^0, α, $\mathcal{L}$, β_1, β_2, λ):

$P_{ac} = P_{ac}^0$, $P_j = P_j^0$, $\mathcal{m}P_{ac} = 0$, $\mathcal{v}P_{ac}$= 0 ,$\mathcal{M}P_j$0, $\mathcal{V}P_j$= 0, t = 0

for iteration from 1 to $\mathcal{L}$ do:

t = t + 1;

P_{ac}^{grad}, P_j^{grad} = ComputeGradient(P_{ac}, P_j) ;

if $P_{ac}^{grad} == \infty$ or $P_j^{grad} == \infty$ then

break;

end if

Update first and second moment estimate

$\mathcal{m}P_{ac} = \beta_1 * \mathcal{m}P_{ac} + (1 - \beta_1) * P_{ac}^{grad}$;

$\mathcal{v}P_{ac} = \beta_2 * \mathcal{v}P_{ac} + (1 - \beta_2) * P_{ac}^{grad^2}$;

$\mathcal{m}P_j = \beta_1 * \mathcal{m}P_j + (1 - \beta_1) * P_j^{grad}$;

$\mathcal{v}P_j = \beta_2 * \mathcal{v}P_j + (1 - \beta_2) * P_j^{grad^2}$;

Compute bias-corrected estimates

$\mathcal{M}P_{ac} = \mathcal{m}P_{ac} / (1 - \beta_1{}^t)$;

$\mathcal{V}P_{ac} = \mathcal{v}P_{ac} / (1 - \beta_2{}^t)$;

$\mathcal{M}P_j = \mathcal{m}P_j / (1 - \beta_1{}^t)$;

$\mathcal{V}P_j = \mathcal{v}P_j / (1 - \beta_2{}^t)$;

Update parameters

$P_{ac} = P_{ac} - \alpha * \mathcal{M}P_{ac} / (\sqrt{\mathcal{V}P_{ac}} + \lambda)$;

$P_j = P_j - \alpha * \mathcal{M}P_j / (\sqrt{\mathcal{V}P_j} + \lambda)$;

Ensure parameters stay within valid ranges.

end for

return P_{ac}, P_j

end procedure

REFERENCES

[1] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," in *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[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," in *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2383-2397, April 2021, doi: 10.1109/TWC.2020.3041800.

[3] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and Security: Challenges and Solutions" *Applied Sciences* 10, no. 12: 4102, 2020, https://doi.org/10.3390/app10124102

[4] H. Jung and B. Lee, "Wireless Power and Bidirectional Data Transfer System for IoT and Mobile Devices," in *IEEE Trans. Ind. Electron.*, vol. 69, no. 11, pp. 11832-11836, Nov. 2022, doi: 10.1109/TIE.2021.3123609.

[5] G. Moloudian *et al*., "RF Energy Harvesting Techniques for Battery-Less Wireless Sensing, Industry 4.0, and Internet of Things: A Review," in *IEEE Sens. J.*, vol. 24, no. 5, pp. 5732-5745, Mar. 2024, doi: 10.1109/JSEN.2024.3352402.

[6] R. M. Haris and S. Al-Maadeed, "Integrating Blockchain Technology in 5G enabled IoT: A Review," in *Proc. 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. (ICIoT)*, Doha, Qatar, 2020, pp. 367-371, doi: 10.1109/ICIoT48696.2020.9089600.

[7] A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," in *Proc. 2021 IEEE Int. Conf. IoT, Electronics Mechatronics (IEMTRONICS)*, Toronto, ON, Canada, 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

[8] S. Sanaullah and B. Liu, "Information Security Challenges in the Internet of Things (IoT) Ecosystem," in *Proc. 2022 Int. Symp. Electr., Electron. Inf. Eng. (ISEEIE)*, Chiang Mai, Thailand, 2022, pp. 124-129, doi: 10.1109/ISEEIE55684.2022.00029.

[9] B. Yang, T. Taleb, G. Chen and S. Shen, "Covert Communication for Cellular and X2U-Enabled UAV Networks with Active and Passive Wardens," in *IEEE Netw.*, vol. 36, no. 1, pp. 166-173, Jan./Feb. 2022, doi: 10.1109/MNET.102.2100337.

[10] B. Yang, T. Taleb, Y. Fan and S. Shen, "Mode Selection and Cooperative Jamming for Covert Communication in D2D Underlaid UAV Networks," in *IEEE Netw.*, vol. 35, no. 2, pp. 104-111, Mar./Apr. 2021, doi: 10.1109/MNET.011.2000100.

[11] Y. Wang, S. Yan, W. Yang and Y. Cai, "Covert Communications With Constrained Age of Information," in *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 368-372, Feb. 2021, doi: 10.1109/LWC.2020.3031492.

[12] M. Wang, W. Yang, X. Lu, C. Hu, B. Liu and X. Lv, "Channel Inversion Power Control Aided Covert Communications in Uplink NOMA Systems," in *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 871-875, Apr. 2022, doi: 10.1109/LWC.2022.3149279.

[13] C. Gao, B. Yang, D. Zheng, X. Jiang and T. Taleb, "Cooperative Jamming and Relay Selection for Covert

Communications in Wireless Relay Systems," in *IEEE Trans. Commun.*, vol. 72, no. 2, pp. 1020-1032, Feb. 2024, doi: 10.1109/TCOMM.2023.3327272.

[14] R. He, G. Li, H. Wang, Y. Jiao and J. Cai, "Adaptive Power Control for Cooperative Covert Communication With Partial Channel State Information," in *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1428-1432, Jul. 2022, doi: 10.1109/LWC.2022.3172683.

[15] X. -Y. Hu, C. Bai and H. -P. Ren, "A Chaotic Pseudo Orthogonal Covert Communication System," in *Proc. 2022 6th Int. Conf. Commun. Inf. Syst. (ICCIS)*, Chongqing, China, 2022, pp. 61-65, doi: 10.1109/ICCIS56375.2022.9998136.

[16] J. Wang, Y. Li, W. Tang, X. Li and S. Li, "Channel State Information Based Optimal Strategy for Covert Communication," in *Proc. 2019 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Xi'an, China, 2019, pp. 1-6, doi: 10.1109/WCSP.2019.8928142.

[17] X. Lu, W. Yang and S. Yan, "Short-Packet Covert Communication with Transmission Time Uncertainty," in *Proc. 2022 7th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Wuhan, China, 2022, pp. 628-632, doi: 10.1109/ICCCS55155.2022.9846514.

[18] B. Che, C. Gao, R. Ma, X. Zheng and W. Yang, "Covert Wireless Communication in Multichannel Systems," in *IEEE Wireless Commun. Lett.*, vol. 11, no. 9, pp. 1790-1794, Sep. 2022, doi: 10.1109/LWC.2022.3180993.

[19] W. Xiong, Y. Yao, X. Fu and S. Li, "Covert Communication With Cognitive Jammer," in *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1753-1757, Oct. 2020, doi: 10.1109/LWC.2020.3003472.

[20] L. Lv, Q. Wu, Z. Li, Z. Ding, N. Al-Dhahir and J. Chen, "Covert Communication in Intelligent Reflecting Surface-Assisted NOMA Systems: Design, Analysis, and Optimization," in *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1735-1750, Mar. 2022, doi: 10.1109/TWC.2021.3106346.

[21] O. Shmuel, A. Cohen and O. Gurewitz, "Multi-Antenna Jamming in Covert Communication," in *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4644-4658, Jul. 2021, doi: 10.1109/TCOMM.2021.3067386.

[22] L. Tao, W. Yang, X. Lu, M. Wang and Y. Song, "Achieving Covert Communication in Uplink NOMA Systems via Energy Harvesting Jammer," in *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 3785-3789, Dec. 2021, doi: 10.1109/LCOMM.2021.3114231.

[23] M. Forouzesh, P. Azmi, A. Kuhestani and P. L. Yeoh, "Joint Information-Theoretic Secrecy and Covert Communication in the Presence of an Untrusted User and Warden," in *IEEE Internet Things J.* vol. 8, no. 9, pp. 7170-7181, May 2021, doi: 10.1109/JIOT.2020.3038682.

[24] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li and J. Wang, "Covert Communication Achieved by a Greedy Relay in Wireless Networks," in *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766-4779, Jul. 2018, doi: 10.1109/TWC.2018.2831217.

[25] Y. Su, H. Sun, Z. Zhang, Z. Lian, Z. Xie and Y. Wang, "Covert Communication With Relay Selection," in *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 421-425, Feb. 2021, doi: 10.1109/LWC.2020.3033786.

[26] X. Jiang *et al*., "Covert Communication in UAV-Assisted Air-Ground Networks," in *IEEE Commun. Lett.*, vol. 28, no. 4, pp. 190-197, Aug. 2021, doi: 10.1109/MWC.001.2000454.

[27] C. Wang *et al*., "Covert Communication Assisted by UAV-IRS," in *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 357-369, Jan. 2023, doi: 10.1109/TCOMM.2022.3220903.

[28] C. Gao, B. Yang, X. Jiang, H. Inamura and M. Fukushi, "Covert Communication in Relay-Assisted IoT Systems," in *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6313-6323, Apr. 2021, doi: 10.1109/JIOT.2021.3051694.

[29] M. Forouzesh, P. Azmi, A. Kuhestani and P. L. Yeoh, "Covert Communication and Secure Transmission Over Untrusted Relaying Networks in the Presence of Multiple Wardens," in *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737-3749, Jun. 2020, doi: 10.1109/TCOMM.2020.2978206.

[30] J. Hu, S. Yan, F. Shu and J. Wang, "Covert Transmission With a Self-Sustained Relay," in *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4089-4102, Aug. 2019, doi: 10.1109/TWC.2019.2920961.

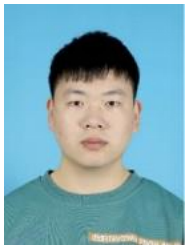
[31] Y. Jiang, L. Wang, H. Zhao and H. -H. Chen, "Covert Communications in D2D Underlaying Cellular Networks With Power Domain NOMA," in *IEEE Syst. J.*, vol. 14, no. 3, pp. 3717-3728, Sep. 2020, doi: 10.1109/JSYST.2020.2967089.

[32] H. Ta and S. W. Kim, "Covert Non-Orthogonal Multiple Access," in *Proc. 2020 IEEE Wireless Commun. Networking Conf. (WCNC)*, Seoul, Korea (South), 2020, pp. 1-6, doi: 10.1109/WCNC45663.2020.9120812.

[33] L. Tao, W. Yang, S. Yan, D. Wu, X. Guan and D. Chen, "Covert Communication in Downlink NOMA Systems With Random Transmit Power," in *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 2000-2004, Nov. 2020, doi: 10.1109/LWC.2020.3011191.

[34] Q. Li, P. Ren, D. Xu and Y. Xie, "Covert Non-Orthogonal Multiple Access Vehicular Communications with Friendly Jamming," in *Proc. 2020 IEEE Globecom Workshops (GC Wkshps)*, Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GCWkshps50303.2020.9367492.

[35] M. Reyad, A. Sarhan, and M. Arafa, "A modified Adam algorithm for deep neural network optimization," *Neural Comput. Appl.*, vol. 35, pp. 17095–17112, 2023, doi: 10.1007/s00521-023-08568-z.



Hao Lv received the B.S. degree from Tianjin University of Science and Technology in 2022. He is currently pursuing the M.S. degree in network and information security with Anhui University, and Chuzhou University, in China.

His research interest focuses on the covert communication in the 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.

Xiuwen Sun received his Ph.D. degree in computer science from Xi'an Jiao tong University in 2019 and is now an assistant professor in the school of computer science and technology at Anhui University. His research interests are computer networks and network security.

Chan Gao received the B.S. and M.S. degrees from the Xi'an University of Posts and Telecommunications, Xi'an, China, in 2014 and 2018, respectively, and the Ph.D. degree in systems information science from Future University Hakodate, Japan, in 2021. She is currently an Assistant Professor with the National Engineering Research Center for Secured Wireless, Xi'an University of Posts and Telecommunications. Her research interests include covert communication in physical layer.

Bao Gui received the M.S. degree from Anhui University of Science and Technology, China, in 2022. Currently, he is with the School of Computer and Information Engineering, Chuzhou University, Anhui, China. His research interests include vehicular networks and wireless communication.

Tarik Taleb (Senior Member, IEEE) 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 Full Professor at Ruhr University Bochum, Germany. He was a Professor with the Center of Wireless Communications, University of Oulu, Oulu, Finland. He is the founder of ICTFICIAL Oy, and the founder and the Director of the MOSA!C Lab. From October 2014 to December 2021, he was an Associate Professor with the School of Electrical Engineering, Aalto University, Espoo, Finland. Prior to that, he was working as a Senior Researcher and a 3GPP Standards Expert with NEC Europe Ltd., Heidelberg, Germany. Before joining NEC and till March 2009, he worked as an Assistant Professor with the Graduate School of Information Sciences, Tohoku University, in a lab fully funded by KDDI. From 2005 to 2006, he was a Research Fellow with the Intelligent Cosmos Research Institute, Sendai. Taleb has been directly engaged in the development and standardization of the Evolved Packet System as a member of the 3GPP System Architecture Working Group. His current research interests include AI-based network management, architectural enhancements to mobile core networks, network softwarization and slicing, mobile cloud networking, network function virtualization, software-defined networking, software-defined security, and mobile multimedia streaming.

.