Improper Gaussian Signaling Based Covert Wireless Communication in IoT Networks

Danyang Wang[1], Qifan Fu[1], Jiangbo Si[1], Ning Zhang[2], and Zan Li[1]
[1]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China*
[2]*Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, N9B 3P4, Canada*
E-mail: {dywang, jbsi, zanli}@xidian.edu.cn; qffu@stu.xidian.edu.cn; ning.zhang@uwindsor.ca

GLOBECOM 2021 - 2021 IEEE Global Communications Conference | 978-1-7281-8104-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/GLOBECOM46510.2021.9685989

***Abstract*—Covert communication, which can hide the communication behavior, has great potential in guaranteeing the security of information and transmission terminal to the greatest extent. In this paper, we propose a covert communication strategy based on improper Gaussian signaling (IGS) to increase the covert rate in the Internet of Things (IoT) system, in which the existing signals emitted by other transmitters were used as "Spectrum Shelter" to cover the IoT's communication. Specifically, we analyze the system's achievable transmission rate when the IoT node adopts IGS. Then, the optimal detection threshold and the minimum error detection probability of the warden are analyzed. Next, by jointly optimizing the transmission power and circularity coefficient of IGS, we maximize the covert rate under the constraints of the covertness. Finally, the simulation results verify that the proposed scheme can not only guarantee the covertness, but also improve the achievable covert rate.**

***Index Terms*—Covert communication, Internet of Things, power allocation, improper Gaussian signaling.**

I. Introduction

With various Internet of Things (IoT) devices adopted in our daily life, IoT has injected new vitality into many fields, e.g., structural health monitoring (SHM), wise information technology of med (WITMED), and Internet of Vehicles [1]. It is expected that the IoT system will be presented as a much more massive network in the 6G scenario [2]. Meanwhile, due to the complex deployment environment and the broadcasting nature of wireless communications, unauthorized gather and illegal utilization of sensitive and confidential information are posing a serious security threat to the IoT enabled devices. Far more attention has been paid to the communication security in IoT system [3].

Communication security in IoT systems can be divided into three levels as follow: i) semantic level: the semantic meaning carried by the communication carrier cannot be deciphered by wardens; ii) technical level: the communication carrier cannot be intercepted by wardens; iii) behavioral level: the communication behavior cannot be detected by wardens. Traditional encryption technology can guarantee the security of semantic level, which realizes the encryption and decryption of confidential information through the sharing of secret keys between transmitters and receivers [4]. However, it requires additional resources and complex structure to manage and distribute keys, which runs counter to the low resources consumption of future wireless IoT devices. Physical Layer Security (PLS) technology designs transmission strategy based on Shannon's information theory, which makes it impossible for wardens to reliably decode the received signals, thus ensuring the security at the technical level [5]. PLS is considered as an alternative and complement to secure communication mechanism and has been successfully applied in IoT systems [6].

However, in many IoT scenarios where life-critical or national defense equipment is needed (e.g., intensive care unit and military internet of things), the exposure of communication behavior puts these core devices at risk of being damaged or maliciously controlled, which means that security requirements of IoT systems have risen to the behavioral level. Therefore, covert communication, which can hide communication behavior, has attracted extensive attention recently. In covert communication, transmitters search for or create transmission conditions which worsen the signal detection and estimation performance of wardens, thus the communication behavior can be hidden in the environment. Gao *et al.* [7] proposed two kinds of relay strategies, which realize covert communication by means of relay selection to change the channel characteristics. Shahzad *et al.* [8] considered uncertainties in Gaussian channels, proving that covert users are able to realize covert transmission to some extent when there exists channel uncertainty. The work in [9] utilized the uncertainty of the noise near the warden's receiver and channel inversion power control to improve the covert performance. Liu *et al.* [10] regarded the uncertainty of total interference in the covert system as a "shadow" network to realize the undetectable of communications on the warden side. Overall, in existing covert communication strategies, transmitters need to reduce the transmission power and leverage various uncertainties (including noise uncertainty, channel uncertainty and interference uncertainty) that will form a shadow link to worsen the detection performance of warden. While lower transmission power also reduces the decoding ability of the legitimate receiver, which makes it difficult to increase the covert rate. Thus, a key issue that hinders the application of covert communication in large-scale IoT systems is *how to improve covert rate while maintaining covertness?*

To address the aforementioned issue, in this paper, we propose an improper Gaussian signaling (IGS) based covert wireless communication strategy in IoT networks, where an overt communication link between a pair of existing transceivers is used as a "spectrum shelter" to form a shadow link. Meanwhile, IoT nodes also need to decrease transmis-

978-1-7281-8104-2/21/$31.00 ©2021 IEEE

Authorized licensed use limited to: Queen Mary University of London. Downloaded on March 17,2023 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

sion power to reduce interference to existing transceivers and improve covertness, which limit the communication rate of the IoT system. Fortunately, in communication scenarios where multiple users interfere with each other, using IGS can improve the system's achievable rate compared to using proper Gaussian signaling (PGS) alone [11]. Therefore, IGS is adopted at IoT system to improve covert rate. Specifically, by jointly optimizing the transmitting power and the circularity coefficient of IGS transmitted by IoT nodes, the covert rate can be improved while the covertness is guaranteed. Finally, the simulation results show that the proposed covert strategy can improve the covert rate compared with PGS one.

II. System Model And Parameter Analysis

A. System Model

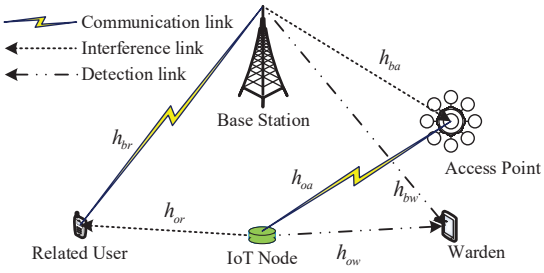

Fig. 1. "Spectrum shelter" based covert communication IoT network.

As shown in Fig. 1, we consider a "spectrum shelter" based covert communication IoT network, which consists an IoT node intending to covertly communicate with an access point and a base station communicating with a related user. In addition, an adversary warden is trying to detect the IoT node's communication behavior. When base station communicates with related user, IoT node has the opportunity to communicate with access point through the same frequency band. Specifically, leveraging power recognition sensing [12], the IoT system can judge the existence of shadow link and carry out covert communication through the same frequency band under the shadow of the existing signal. To improve the transmission rate, in this system model, the IoT devices use IGS to communicate, while the base station and related user uses PGS to communicate. Then the received signals at related user and access point are given by

$$\begin{aligned} y_r[i] &= \sqrt{P_b}h_{br}x_b[i] + \sqrt{P_o}h_{or}x_o[i] + n_r[i], \\ y_a[i] &= \sqrt{P_o}h_{oa}x_o[i] + \sqrt{P_b}h_{ba}x_b[i] + n_a[i], \end{aligned} \tag{1}$$

where P_b and P_o are the transmit power of base station and IoT node, respectively; $x_b[i]$ is the PGS transmitted at base station; $x_o[i]$ is the IGS symbol with circularity coefficient κ used by IoT node; h_{pq} denotes the channels from p to q, $p = b, o$ and $q = a, r$, respectively; $n_r[i]$ and $n_a[i]$ are the circularly-symmetric complex additive white Gaussian noise (AWGN) at the related user and access point, respectively. Specifically, both $n_r[i]$ and $n_a[i]$ are with zero-mean and variance σ^2, *i.e.*, $n_r[i] \sim \mathcal{CN}(0, \sigma_r^2)$ and $n_a[i] \sim \mathcal{CN}(0, \sigma_a^2)$, respectively. We assume that all the devices are equipped with a single antenna and the perfect channel state information (CSI) of these channels are available to IoT device, since the base station can cooperate with IoT device for sharing the CSIs.

B. Achievable Rates With IGS

Considering a zero-mean complex Gaussian random variable (RV) x, if x is a proper complex Gaussian RV, then its full statistical characteristics can be described by the mean and variance. But it is not sufficient to describe the statistical characteristics of the improper complex Gaussian RV by mean and variance. Therefore, besides the traditional variance defined as $\sigma_x^2 = \mathbb{E}\{|x|^2\}$, the pseudo-variance of x defined as $\hat{\sigma}_x^2 = \mathbb{E}\{x^2\}$ is needed. Then x is called proper if its pseudo-variance is equal to zero, otherwise it is improper. The circularity coefficient is used to measure the impropriety degree of improper complex Gaussian RV, which is defined as $\kappa = |\hat{\sigma}_x^2|/\sigma_x^2$, where $0 \le \kappa \le 1$. There are two ways to generate improper signals. For one thing, we can obtain improper signals through some inherently asymmetric signaling modulation methods, such as Binary Phase Shift Keying (BPSK), Pulse Amplitude Modulation (PAM) and *etc*. For another, we can also introduce asymmetry into symmetric discrete constellations through Probabilistic Shaping, Geometric Shaping, Orthogonal/Non-Orthogonal Sharing and Hybrid Signaling to produce improper signals. The improper signals provide a new dimension that offers an additional degree of freedom in the system design, which can help improving the transmission performance in covert communication systems.

According to Eq. (1), each signal sent by the base station and IoT node is considered as the desired signal at its corresponding receiver while being treated as interference at the other. Assuming that the IGS interference at related user is treated as an additional noise appending to the inherent Gaussian background noise at the receiver of related user, then the achievable rate of related user can be expressed as [13]

$$\begin{aligned} &R_r(P_o, \kappa) = \\ &\log_2\left[1 + \frac{P_b|h_{br}|^2}{P_o|h_{or}|^2 + \sigma_r^2}\right] + \frac{1}{2}\log_2\left[\frac{1-\mathcal{K}_{yo}^2}{1-\mathcal{K}_{Io}^2}\right], \end{aligned} \tag{2}$$

where $\mathcal{K}_{yo}$ and $\mathcal{K}_{Io}$ are the circularity coefficients of the received signals and interference-plus-noise signals at the related user, respectively, which are given by

$$\begin{aligned} \mathcal{K}_{yo} &= (P_o|h_{or}|^2\kappa)/(P_o|h_{or}|^2 + P_b|h_{br}|^2 + \sigma_r^2), \\ \mathcal{K}_{Io} &= (P_o|h_{or}|^2\kappa)/(P_o|h_{or}|^2 + \sigma_r^2). \end{aligned} \tag{3}$$

It can be seen that the second term of Eq. (2) represents the additional rate achievement when IoT node adopts IGS rather than PGS for communication. Besides, from Eq. (2) and Eq. (3) we can draw a conclusion that the second term of Eq. (2) is always positive, which means that adopting IGS can always achieve rate improvement than PGS. Define the channel-to-noise ratio (CNR) of the channel from base station to the related user as $\gamma_{br} = |h_{br}|^2/\sigma_r^2$ and the interference

Authorized licensed use limited to: Queen Mary University of London. Downloaded on March 17,2023 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

CNR of the channel from the IoT node to the related user as $I_{or} = |h_{or}|^2/\sigma_r^2$. Then Eq. (2) can be simplified as

$$R_r\left(P_o,\kappa\right) = \frac{1}{2}\log_2\left(\frac{\left(P_o I_{or} + P_b\gamma_{br} + 1\right)^2 - \left(P_o I_{or}\kappa\right)^2}{\left(P_o I_{or} + 1\right)^2 - \left(P_o I_{or}\kappa\right)^2}\right). \tag{4}$$

For the IoT transmission, the circularity coefficient of the interference term equals zero, and then the achievable rate at sink can be expressed as

$$R_a\left(P_o,\kappa\right) = \log_2\left[1 + \frac{P_o|h_{oa}|^2}{P_b|h_{ba}|^2 + \sigma_a^2}\right] + \frac{1}{2}\log_2\left[1 - \mathcal{K}_{ya}^2\right], \tag{5}$$

where $\mathcal{K}_{ya}$ is the circularity coefficients of the received signals at the access point, which is given by $\mathcal{K}_{ya} = (P_o|h_{oa}|^2\kappa)/(P_o|h_{oa}|^2 + P_b|h_{ba}|^2 + \sigma_a^2)$.

Define the CNR of the channel from IoT node to the access point as $\gamma_{oa} = |h_{oa}|^2/\sigma_a^2$ and the interference CNR of the channel from the base station to the access point as $I_{oa} = |h_{ba}|^2/\sigma_a^2$. Then Eq. (5) can be simplified as

$$R_a\left(P_o,\kappa\right) = \frac{1}{2}\log_2\left(\frac{\left(P_o\gamma_{oa} + P_b I_{ba} + 1\right)^2 - \left(P_o\gamma_{oa}\kappa\right)^2}{\left(P_b I_{ba} + 1\right)^2}\right). \tag{6}$$

C. Detection Performance of The Warden

The ultimate goal of warden is to judge whether IoT node is in communication state through a binary hypothesis testing model. As "Spectrum Shelter" based covert communication strategy is adopted at the IoT node, only when the base station is active is it possible for IoT node to communicate. According to the working status of the transmitters at all the devices in this scenario, the received signals at the warden can be categorized into two different cases. Consequently, the warden needs to determine whether the IoT node is in communication state via a binary hypothesis test containing $\mathcal{H}_0$ and $\mathcal{H}_1$. To be specific, in hypothesis $\mathcal{H}_0$, which represents that the IoT node is silence, the received signals at warden consist of the signals transmitted from the base station and the background noise. While in hypothesis $\mathcal{H}_1$, which represents that the IoT node is active, the received signals at warden comprise signals transmitted from the IoT device, signals transmitted from the base station and the background noise. Above all, the received signals at the warden can be expressed as:

$$y_w\left[i\right] = \begin{cases} \sqrt{P_b}h_{bw}x_b\left[i\right] + n_w\left[i\right], & \mathcal{H}_0, \\ \sqrt{P_o}h_{ow}x_o\left[i\right] + \sqrt{P_b}h_{bw}x_b\left[i\right] + n_w\left[i\right], & \mathcal{H}_1, \end{cases} \tag{7}$$

where h_{bw} and h_{ow} represent the fading channels from the base station and the IoT node to the warden, with the channel gain $|h_{bw}|^2$ and $|h_{ow}|^2$ modeled as exponential distribution with parameters λ_{bw} and λ_{ow}, respectively; and $n_w\left[i\right]$ is the circularly-symmetric complex AWGN at the warden with zero-mean and variance σ_w^2. We suppose that the warden only has the statistical CSI of channels from base station and IoT device to the warden.

The warden attempts to make a decision between these two hypotheses to discriminate whether the IoT device transmits or not based on N observations within a period of sampling time. Then the sufficient test statistic and the decision rule for this binary hypothesis testing is given by [14]

$$T(N) = 1/N\sum\nolimits_{i=1}^{N}\left|y_w\left[i\right]\right|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma, \tag{8}$$

where γ is the detection threshold to distinguish two hypotheses, which decides the detection performance of warden. Based on the considered signal model and basic assumptions and considering infinite blocklength as in [15], we have

$$\lim_{N\to\infty} T\left(N\right) = \begin{cases} P_b|h_{bw}|^2 + \sigma_w^2, & \mathcal{H}_0, \\ P_o|h_{ow}|^2 + P_b|h_{bw}|^2 + \sigma_w^2, & \mathcal{H}_1. \end{cases} \tag{9}$$

To evaluate the detection performance of warden, we use two types of error detection for the warden's binary hypothesis test in the following analysis. Firstly, we define the probability of false alarm as the probability that decision $\hat{\mathcal{H}}_1$ is made at the warden while $\mathcal{H}_0$ is true in practice, denoted by $\mathbb{P}_{FA}$. Moreover, the probability of miss detection is defined as the probability that the warden makes a decision $\hat{\mathcal{H}}_0$ while $\mathcal{H}_1$ is true, and is denoted by $\mathbb{P}_{MD}$. Hence the error detection performance of warden's hypothesis test is measured by $\mathbb{P}_E$, which is given as $\mathbb{P}_E$=$\mathbb{P}_{FA}$+$\mathbb{P}_{MD}$.

To improve the reliability of eavesdropping, the warden needs to set an optimal threshold γ^* that minimizing $\mathbb{P}_E$, which demonstrates both the optimum detection performance of warden and the worst covert situation for IoT node. We can easily find that the optimal detection threshold lies in the region $\left(\sigma_w^2,\infty\right)$. The optimal solution is obtained by monotonicity as shown below

$$\gamma^* = \begin{cases} \dfrac{\ln\lambda_1 - \ln\lambda_2}{\lambda_1 - \lambda_2} + \sigma_w^2, & \lambda_1 \neq \lambda_2, \\ \dfrac{1}{\lambda_1} + \sigma_w^2, & \lambda_1 = \lambda_2. \end{cases} \tag{10}$$

Therefore, the warden can achieve the minimum error detection probability by setting the optimal detection threshold:

$$\mathbb{P}_E^*= \begin{cases} 1 - e^{-\lambda_2\frac{\ln\lambda_1 - \ln\lambda_2}{\lambda_1 - \lambda_2}}, & \lambda_1 \neq \lambda_2, \\ 1 - 1/e, & \lambda_1 = \lambda_2. \end{cases} \tag{11}$$

III. Transmission Strategy Design For Covert Communication

In this section, we study the transmission strategy design with IGS for covert communication. By optimizing the statistical signal parameters P_o and κ jointly, the covert rate of IoT node can be further improved when the IGS is adopted. In addition, at the end of this chapter, covert rate of PGS communication is also given as a benchmark.

A. Improper Gaussian Signaling Design

When the IGS scheme is adopted at IoT device, we aims to jointly optimize P_o and κ to maximize the achievable covert rate while holding a required quality of service (QoS) of

Authorized licensed use limited to: Queen Mary University of London. Downloaded on March 17,2023 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

related user. To this end, the optimization problem can be formulated as

$$\begin{aligned} \max_{P_o,\kappa} \quad & R_a\left(P_o,\kappa\right) \\ s.t. \quad & R_r\left(P_o,\kappa\right) \geq R_{\min}, \\ & 0 \leq P_o \leq P_{\max}, \\ & \mathbb{P}_E^* \geq 1-\varepsilon, \\ & 0 \leq \kappa \leq 1, \end{aligned} \tag{12}$$

where $R_{\min}$ is the minimum rate requirement for the related user; $P_{\max}$ is the maximum transmit power budget of IoT node, ε is predetermined to specify the covert constraint, and $\mathbb{P}_E^*$ is the minimum detection error probability achieved at warden.

Considering that the "spectrum shelter" based covert communication strategy requires the signals of the base station to be the covert, the first constraint condition in Eq. (12) must be satisfied before the IoT nodes can carry out covert communication while satisfying the QoS requirement of related user. When the IoT node is silent, i.e., $P_o = 0$ and $\kappa_x = 0$, related user can reach its maximum achievable rate $R_0 = \log_2(1 + P_b|h_{bu}|^2/\sigma_u^2)$. Therefore, only when the condition $R_0 < R_{\min}$ is satisfied can IoT node have the opportunity to adopt covert communication.

Based on Eq. (4), the first constraint can be reformulated as the following quadratic inequality in terms of P_o:

$$\left(1-\kappa^2\right)\varphi(P_o I_{or})^2 + 2\alpha P_o I_{or} + \beta \leq 0, \tag{13}$$

where $\varphi = 2^{2R_{\min}} - 1$, $\alpha = 2^{2R_{\min}} - P_b\gamma_{br} - 1$, and $\beta = 2^{2R_{\min}} - (P_b\gamma_{br}+1)^2$. We here denote the left-hand-side of Eq. (13) by $f(P_o)$. To derive the constraint on transmit power P_o in guaranteeing the QoS of related user, we first calculate the roots of $f\left(P_o\right) = 0$. According to the above discussion, only when condition $R_0 < R_{\min}$ is satisfied will the node of the IoT carry out covert communication. We can figure out $\varphi > 0$ and $\beta < 0$ from $R_0 < R_{\min}$. Since $\beta < 0$, then the equation $f\left(P_o\right) = 0$ exists one positive root and one negative root. Therefore, the feasible transmit power bound is given by $P_o(\kappa) = [(\sqrt{\alpha^2 - \varphi(1-\kappa^2)\beta} - \alpha)/(I_{or}\varphi(1-\kappa^2))]^+$ and the first constraint can be equivalent to $P_o \leq P_o\left(\kappa\right)$.

Noting that the minimum error detection probability is not affected by the coefficient factor κ, from the third covertness constraint, P_ε can be derived as

$$P_\varepsilon = \begin{cases} (\lambda_{ow}P_b W\left(\varepsilon\ln\varepsilon\right))/(\lambda_{bw}\ln\varepsilon), & \varepsilon \leq 1/e, \\ (\lambda_{ow}P_b W_{-1}\left(\varepsilon\ln\varepsilon\right))/(\lambda_{bw}\ln\varepsilon), & \varepsilon > 1/e, \end{cases} \tag{14}$$

where $W_k\left(\cdot\right)$ is Lambert W function. Therefore, the third covertness constraint in Eq. (12) can also be simplified as $P_o \leq P_\varepsilon$. Additionally, the secondary and third constraint can be merged as $0 \leq P_o \leq P_\Delta \triangleq \min\left\{P_{\max}, P_\varepsilon\right\}$. Thus, the first three constraints in Eq. (12) related to the transmit power P_o can be re-expressed as $P_d \leq \min\left\{P_\Delta, P_d\left(\kappa\right)\right\}$. Then, the transmit power P_o and circular coefficients κ will be jointly optimized to obtain the solution.

The feasible transmit power bound $P_o\left(\kappa\right)$ is strictly increasing with κ over the interval $\kappa \in [0,1)$. Moreover, when $\kappa \to 1$, the limit of $P_o\left(\kappa\right)$ can be obtained as

$$\lim_{\kappa\to 1} P_o\left(\kappa\right) = \begin{cases} -\frac{\beta}{2I_{or}\alpha}, & \alpha \geq 0, \\ +\infty, & \alpha < 0. \end{cases} \tag{15}$$

When $\min\left\{P_\Delta, P_o\left(\kappa\right)\right\} = P_\Delta$, the Eq. (12) reduces to

$$\begin{aligned} \max_{\kappa} \quad & R_a\left(P_\Delta,\kappa\right) \\ s.t. \quad & 0 \leq \kappa \leq 1. \end{aligned} \tag{16}$$

Since $R_a(P_\Delta,\kappa)$ is decreasing with κ, the optimal solution reduces to the PGS communication, *i.e.*, $(P_o^*,\kappa^*) = (P_\Delta, 0)$. When $\lim_{\kappa\to 1}P_o(\kappa) \leq P_\Delta$, the problem can be solved by using the monotonic properties of the objective function and the constraints. For $\forall\kappa \in [0,1]$, we can easily show $R_a(P_o,\kappa)$ is monotonically increasing with P_o for a given κ. Hence, P_o should be assigned the maximum value of the constraint for maximizing the achievable covert rate. Then the optimization problem with IGS can be reformulated as

$$\begin{aligned} \max_{\kappa} \quad & R_a\left(\kappa\right) \\ s.t. \quad & 0 \leq P_o\left(\kappa\right) \leq P_\Delta, \\ & 0 \leq \kappa \leq 1, \end{aligned} \tag{17}$$

where $R_a\left(\kappa\right)$ is derived by substituting the $P_o = P_o(\kappa)$ into the achievable covert rate of IoT device. Note that $P_o = P_o\left(\kappa\right)$ is a root of $f\left(P_a\right) = 0$, so from Eq. (13) we can deduce

$$P_o^2(\kappa) = ((-2\alpha P_o(\kappa) I_{or} - \beta)/((1-\kappa^2)\varphi I_{or}^2)). \tag{18}$$

Then substituting Eq. (18) into Eq. (6), we can get

$$g(\kappa) = (P_b I_{ba} + 1 - \frac{\alpha\gamma_{oa}}{\varphi I_{or}})P_o(\kappa) - \frac{\beta\gamma_{oa}}{\varphi I_{or}^2}. \tag{19}$$

As the logarithm function is monotonically increasing in its domain, the monotonicity of $R_a\left(\kappa\right)$ is consistent with $g\left(\kappa\right)$ defined by Eq. (19). Denote $R_1 = \frac{1}{2}\log_2((P_b I_{ba} I_{or} + I_{or} - P_b\gamma_{br}\gamma_{oa} - \gamma_{oa})/(P_b I_{ba} I_{or} + I_{or} - \gamma_{oa}))$. Then when $R_{\min} \geq R_1$, $R_a\left(\kappa\right)$ is monotonically increasing with κ and IoT node should use IGS with maximum possible transmit power for achieving the maximum achievable covert rate. Otherwise $R_a\left(\kappa\right)$ is monotonously decreasing with κ. Hence, the optimal solution pair of Eq (12) with $\lim_{\kappa\to 1}P_o\left(\kappa\right) \leq P_\Delta$ can be derived as

$$(P_o^*,\kappa^*) = \begin{cases} \left(\lim_{\kappa\to 1}P_o\left(\kappa\right), 1\right), & R_{\min} \geq R_1, \\ \left(P_o\left(0\right), 0\right), & R_{\min} < R_1. \end{cases} \tag{20}$$

When $\lim_{\kappa\to 1}P_o\left(\kappa\right) > P_\Delta$, an intersection point between $P_o\left(\kappa\right)$ and P_Δ exists, whose x-coordinate can be given as $\kappa_{\text{int}} = \sqrt{(2\alpha(P_\Delta I_{or}) + \beta)/(\varphi(P_\Delta I_{or})^2) + 1}$. Then the interval of κ can be divided into two sub-intervals, we optimize the transmit power and circularity coefficient in each sub-interval. Over the sub-interval $0 \leq \kappa \leq \kappa_{\text{int}}$, we have $\min\left\{P_\Delta, P_o\left(\kappa\right)\right\} = P_o\left(\kappa\right)$ and the optimization problem is expressed as

$$\begin{aligned} \max_{\kappa} \quad & R_a\left(\kappa\right) \\ s.t. \quad & 0 \leq \kappa \leq \kappa_{\text{int}}. \end{aligned} \tag{21}$$

Authorized licensed use limited to: Queen Mary University of London. Downloaded on March 17,2023 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

When $R_{\min} \geq R_1$, the solution reduces to $(P_o^*, \kappa^*) = (P_o(\kappa_{\text{int}}), \kappa_{\text{int}})$. When $R_{\min} < R_1$, the solution reduces to $(P_o^*, \kappa^*) = (P_o(0), 0)$. Over the sub-interval $\kappa_{\text{int}} \leq \kappa \leq 1$, the optimization solution reduces to $(P_o^*, \kappa^*) = (P_\Delta, \kappa_{\text{int}})$.

B. Proper Gaussian Signaling Design

When the IoT device adopts PGS scheme, i.e. $\kappa = 0$, the achivable covert rate can be expressed as

$$R_a(P_o, 0) = \log_2((P_o\gamma_{oa} + P_bI_{ba} + 1)/(P_bI_{ba} + 1)). \quad (22)$$

We focus on maximizing the achievable covert rate by adjusting the transmit power of IoT device. Such an optimization problem can be formulated as

$$\begin{aligned} \max_{P_o} \quad & R_a(P_o, 0) \\ s.t. \quad & R_r(P_o, 0) \geq R_{\min}, \\ & 0 \leq P_o \leq P_{\max}, \\ & \mathbb{P}_E^* \geq 1 - \varepsilon. \end{aligned} \quad (23)$$

In a feasible "spectrum shelter" based covert communication system with PGS scheme adopted at IoT device, the transmit power P_o is optimally designed as

$$P_o = \begin{cases} \min\{P_{\max}, P_\varepsilon\}, & R_{\min} < R_2, \\ \min\{P_I, P_\varepsilon\}, & R_2 < R_{\min} < R_0, \end{cases} \quad (24)$$

where P_I is expressed as

$$P_I = ((P_b\gamma_{br}/(2^{R_{\min}} - 1) - 1)/I_{or}), \quad (25)$$

and R_2 is defined as

$$R_2 = \log_2(1 + P_b|h_{br}|^2/(P_{\max}|h_{or}|^2 + \sigma_r^2)). \quad (26)$$

IV. Discussions And Simulations

In this section, we present simulation results to verify our theoretical analysis on the performance of the proposed spectrum mask based covert communications. The transmit power at base station is set as $P_b = 30$dBm. The minimum rate requirement for the related user is set as $R_{\min} = 3$bit/s/Hz. Without loss of generality, we set the received noise variance at related user, access point and warden as $\sigma_r^2 = \sigma_a^2 = \sigma_w^2 = 1$. Unless otherwise stated, we set the channel gains from base station to related user and the access point as $|h_{br}|^2 = 16$dB and $|h_{ba}|^2 = 6$dB, respectively. In addition, the channel gains from IoT node to access point and related user are set as $|h_{oa}|^2 = 20$dB and $|h_{or}|^2 = 10$dB. The parameters of Rayleigh fading channels from base station and IoT node to the warden are set by $\lambda_{bw} = 2$ and $\lambda_{ow} = 3$, respectively. The maximum transmit power of the IoT node is limited by $P_{\max} = 25$dBm. The predetermined covertness constraint is set as $\varepsilon = 0.2$.

Fig. 2 describes the achievable cover rate R_a for the PGS and IGS versus the CNR γ_{oa}. When $\gamma_{br} = 11, 15, 25$dB, the achievable covert rate of IGS communication is better than that of PGS one. Additionally, the performance gain between the IGS and PGS scheme when $\gamma_{br} = 15$dB is greater than that when $\gamma_{br} = 11, 25$dB. While when $\gamma_{br} = 25$dB, the gain achieved by IGS is almost negligible. This is because when the channel between the base station and related user is good enough, related user has a high tolerance to interference. Thus the IoT node can adopt the maximum power budget to communicate. As can be seen from the curve of $\gamma_{bo} = 11$dB, when $\gamma_{oa} \leq 28$dB, the performance gain can be achieved by adopting IGS, while when $\gamma_{oa} > 28$dB, this gain will disappear, which means that when the channel gain between IoT node and access point is large enough, the IGS scheme is no more necessary, since using IGS will deteriorate its own transmission performance, validated by Eq. (5). In this case, the PGS is adopted, and the transmit power depends only on the interference tolerance of the related user.

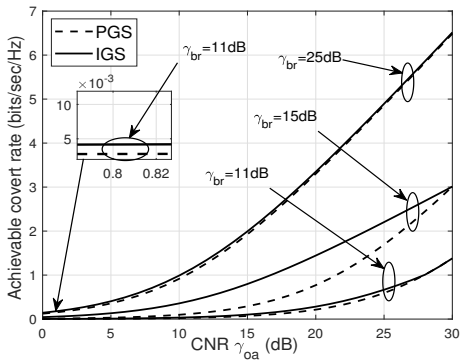

Fig. 2. The achievable covert rate R_a for the proper and improper Gaussian signaling versus the CNR γ_{oa} with different value of γ_{br}.

The achievable covert rate R_a for the PGS and IGS versus the CNR γ_{br} is shown in Fig. 3. It reveals that the covert rate of IoT node monotonically increase with the CNR γ_{br}. With a low γ_{br}, the achievable covert rate of IoT node is 0, which means the IoT node is not allowed to covertly transmit its own message. In other words, the QoS of the related user can not be satisfied although the IoT device remains silent. While there has a certain interference tolerance at the related user with a large γ_{br}. Thus, the IoT node can adjust the transmit power and circularity coefficient of IGS to achieve performance improvement. A point that indicates the maximum performance improvement value by leveraging IGS scheme exists. Before that, the IoT node always chooses $\kappa = 1$ to reduce the interference introduced to related user, and the allowed transmit power increases with γ_{br}. Moreover, the gaps between IGS and PGS scheme get large as the γ_{br} increases, which is due to the reason an additional rate improvement achieves, i.e., the second term in Eq. (5). While after the maximum point, the IoT system do not need to choose a large κ to reduce the interference, until the κ tends to zero, then the IGS scheme reduces to PGS one.

Fig. 4 plots the variation of achievable covert rate R_a w.r.t. the covert requirement ε. When $\varepsilon \leq 0.063$, the achievable covert rate of IGS communication is the same as PGS one. This is due to the fact that IoT node must communicate at a lower transmitting power under high covert requirement. Thus, the related user can tolerate interference even if the maximum transmission power budget is used. When $\varepsilon > 0.063$, the

Authorized licensed use limited to: Queen Mary University of London. Downloaded on March 17,2023 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

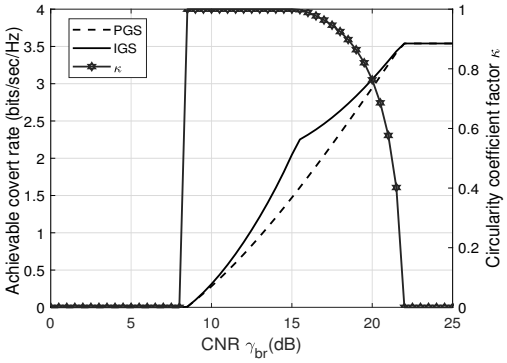

Fig. 3. The achievable covert rate and corresponding circularity coefficient factor of IGS versus the CNR γ_{br}.

maximum transmission power is determined by the constant value $\min\{P_{\max}, P_I\}$ in the case of PGS usage, so the achievable covert rate of PGS communication will remain constant. In contrast, when $\varepsilon > 0.063$, the covert rate gain by using IGS communications is apparent. Specifically, when $\varepsilon \in [0.063, 0.272]$, the achievable covert rate will increase with the increase of covert requirement. This is due to the fact that IoT node can use higher transmission power in the case of IGS usage, and the adverse effect on the transmission rate of related user can be compensated by increasing the circularity coefficient κ of IGS. In addition, when $\varepsilon > 0.272$, the achievable covert rate of IGS communication stops rising and remains the same level, but it is still 0.831 bit/s/Hz higher than the achievable covert rate of PGS communication.This is because in this case the circularity coefficient has reached its maximum value, i.e. $\kappa = 1$, and the transmit power is limited by the maximum power budget of IoT node.

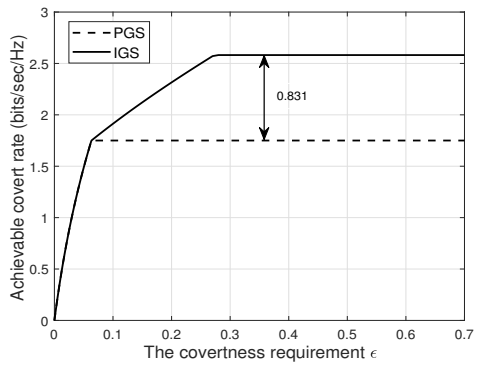

Fig. 4. The achievable covert rate versus the covertness requirement.

V. Conclusions

In this paper, we have investigated an IGS based covert communication strategy in IoT networks, which uses the existing signals as "spectrum shelter" to shield the IoT communication. To improve the covert rate, the IoT nodes use IGS signals to communicate. We also analyze the transmission rate of the IoT system and warden's detection performance when the IoT node adopts IGS. Besides, a joint optimization problem of IGS transmitted power and circular coefficient is designed, and we derive the closed-form solution of optimal transmitted power and circular coefficient based on the QoS of the existing transceivers. Finally, numerical results are provided to demonstrate the feasibility of the proposed strategy and the benefits of adopting IGS scheme compared to PGS one.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under grant 61901328, 61971337; in part by the National Natural Science Foundation for Distinguished Young Scholar 61825104; in part by the Industry-University-Academy Cooperation Program of Xidian University-Chongqing IC Innovation Research Institute under grant CQIRI-2021CXY-Z07; in part by the Fundamental Research Funds for the Central Universities under grant XJS210109.

References

[1] I. A. Zualkernan, F. Aloul, S. A. Qasimi, A. AlShamsi, M. A. Marashda, and A. Ahli, "Digimesh-based social internet of vehicles (siov) for driver safety," in *2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI)*, 2018, pp. 1–5.

[2] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, "Enabling massive iot toward 6g: A comprehensive survey," *IEEE Internet Things J.*, pp. 1–1, 2021.

[3] 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, 2020.

[4] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for vanet with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, 2020.

[5] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Artificial-noise-aided optimal beamforming in layered physical layer security," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 72–75, 2019.

[6] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless communication and security issues for cyber–physical systems and the internet-of-things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, 2018.

[7] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted iot systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6313–6323, 2021.

[8] K. Shahzad and X. Zhou, "Covert wireless communications under quasi-static fading with channel uncertainty," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1104–1116, 2021.

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

[10] 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, 2018.

[11] H. D. Tuan, A. A. Nasir, H. H. Nguyen, T. Q. Duong, and H. V. Poor, "Non-orthogonal multiple access with improper gaussian signaling," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 496–507, 2019.

[12] D. Wang, N. Zhang, Z. Li, F. Gao, and X. Shen, "Leveraging high order cumulants for spectrum sensing and power recognition in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1298–1310, 2018.

[13] Y. Zeng, R. Zhang, E. Gunawan, and Y. L. Guan, "Optimized transmission with improper gaussian signaling in the K-User MISO interference channel," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6303–6313, 2013.

[14] M. H. DeGroot, "Probability and statistics, 4th ed." *London, U.K.: Pearson*, 2012.

[15] 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, 2018.

Authorized licensed use limited to: Queen Mary University of London. Downloaded on March 17,2023 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.