Covert Communication Achieved by A Greedy Relay in Wireless Networks

Jinsong Hu, *Student Member, IEEE,* Shihao Yan, *Member, IEEE,* Xiangyun Zhou, *Senior Member, IEEE,* Feng Shu, *Member, IEEE,* Jun Li, *Senior Member, IEEE,* and Jiangzhou Wang, *Fellow, IEEE*

***Abstract*—Covert wireless communication aims to hide the very existence of wireless transmissions in order to guarantee a strong security in wireless networks. In this work, we examine the possibility and achievable performance of covert communication in amplify-and-forward one-way relay networks. Specifically, the relay is greedy and opportunistically transmits its own information to the destination covertly on top of forwarding the source's message, while the source tries to detect this covert transmission to discover the illegitimate usage of the resource (e.g., power, spectrum) allocated only for the purpose of forwarding the source's information. We propose two strategies for the relay to transmit its covert information, namely rate-control and power-control the transmission schemes, for which the source's detection limits are analysed in terms of detection error probability and the achievable effective covert rates from the relay to destination are derived. Our examination determines the conditions under which the rate-control transmission scheme outperforms the power-control transmission scheme, and vice versa, which enables the relay to achieve the maximum effective covert rate. Our analysis indicates that the relay has to forward the source's message to shield its covert transmission and the effective covert rate increases with its forwarding ability (e.g., its maximum transmit power).**

***Index Terms*—Physical layer security, covert communication, wireless relay networks, detection, transmission schemes.**

This work was supported in part by the National Natural Science Foundation of China under Grant 61771244, Grant 61727802, Grant 61501238, and Grant 61472190, in part by the Australian Research Council's Discovery Projects (DP150103905), in part by the Open Research Fund of National Key Laboratory of Electromagnetic Environment, China Research Institute of Radiowave Propagation under Grant 201500013, in part by the Open Research Fund of the National Mobile Communications Research Laboratory, Southeast University, China, under Grant 2017D04, in part by the Jiangsu Provincial Science Foundation Project under Grant BK20150786, in part by the Specially Appointed Professor Program in Jiangsu Province, 2015, in part by the Fundamental Research Funds for the Central Universities under Grant 30916011205. This paper was presented in part at IEEE Global Communication Conference (GLOBECOM 2017), Singapore, Dec. 2017 [1].

J. Hu, F. Shu, and J. Li are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. (Emails: {jinsong_hu, shufeng, jun.li}@njust.edu.cn). J. Hu is also a visiting PhD student at the Research School of Engineering, Australian National University, Canberra, ACT, Australia. F. Shu is also with the College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou, China. J. Li is also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, and with the Department of Software Engineering, Institute of Cybernetics, National Research Tomsk Polytechnic University, Tomsk, Russia.

S. Yan is with the School of Engineering, Macquarie University, Sydney, NSW, Australia (Email: shihao.yan@mq.edu.au).

X. Zhou is with the Research School of Engineering, Australian National University, Canberra, ACT, Australia (Email:xiangyun.zhou@anu.edu.au).

J. Wang is with the School of Engineering and Digital Arts, University of Kent, Canterbury CT2 7NT, U.K. (Email: j.z.wang@kent.ac.uk).

I. Introduction

A. Background and Related Works

Security and privacy are critical in existing and future wireless networks since a large amount of confidential information (e.g., credit card information, physiological information for e-health) is transferred over the open wireless medium [2–4]. Traditional security techniques offer protection against eavesdropping through encryption, guaranteeing the integrity of messages over the air [5, 6]. However, it has been shown in the recent years that even the most robust encryption techniques can be defeated by a determined adversary. Physical-layer security, on the other hand, exploits the dynamic characteristics of the wireless medium to minimize the information obtained by eavesdroppers [7–11]. However, it does not provide protection against the detection of a transmission in the first place, which can offer an even stronger level of security, as the transmission of encrypted transmission can spark suspicion in the first place and invite further probing by skeptical eavesdroppers. On the contrary, apart from protecting the content of communication, covert communication aims to enable a wireless transmission between two users while guaranteeing a negligible detection probability of this transmission at a warden and thus achieving privacy of the transmitter. Meanwhile, this strong security (i.e., hiding the wireless transmission) is desired in many application scenarios of wireless communications, such as covert military operations, location tracking in vehicular ad hoc networks and intercommunication of sensor networks or Internet of Things (IoT). Due to the broadcast nature of wireless channels, the security and privacy of wireless communications has been an ever-increasing concern, which now is the biggest barrier to the wide-spread adoption of sensor networks or IoT technologies [12]. In sensor networks or IoT, multiple hidden transmitters or receivers, which may be surrounded or monitored by wardens/cybercriminals, are trying to exchange critical information through multi-hop wireless transmissions. Each transmission should be kept covert to enable the end-to-end covert communication in order to guarantee the 'invisibility' of the transmitters. As such, the hiding of communication termed covert communication or low probability of detection communication, which aims to shield the very existence of wireless transmissions against a warden to achieve security, has recently drawn significant research interests and is emerging as a cutting-edge technique in the context of wireless communication security [13–15].

Although spread-spectrum techniques are widely used to achieve covertness in military applications of wireless commu-

nications [16], many fundamental problems have not been well addressed. This leads to the fact that the probability that the spread-spectrum techniques fail to hide wireless transmissions is unknown, significantly limiting its application. The fundamental limit of covert communication has been studied under various channel conditions, such as additive white Gaussian noise (AWGN) channels [17], binary symmetric channels [18], discrete memoryless channels [19], and multiple input multiple output (MIMO) AWGN channels [20]. It is proved that $\mathcal{O}(\sqrt{n})$ bits of information can be transmitted to a legitimate receiver reliably and covertly in n channel uses as $n \to \infty$. This means that the associated covert rate is zero due to $\lim_{n\to\infty} \mathcal{O}(\sqrt{n})/n \to 0$. Following these pioneering works on covert communication, a positive rate has been proved to be achievable when the warden has uncertainty on his receiver noise power [21, 22], or an uniformed jammer comes in to help [23]. Most recently, [24] has examined the impact of noise uncertainty on covert communication. In addition, the effect of the imperfect channel state information (CSI) and finite blocklength (i.e., finite n) on covert communication has been investigated in [25] and [26], respectively.

B. Motivation and Our Contributions

The ultimate goal of covert wireless communication is to establish shadow wireless networks [14], in which each hop transmission should be kept covert to enable the end-to-end covert communication, in order to guarantee the "invisibility" of the transmitters. Following the previous works that only focused on covert transmissions in point-to-point communication scenarios, in this work, for the first time, we consider covert communications in the context of amplify-and-forward one-way relay networks. This is motivated by the scenario where the relay (R) tries to transmit its own information to the destination (D) on top of forwarding the information from the source (S) to D. Specifically, for example, in some relay networks (possible application scenarios of sensor networks or IoT) the communication resources (e.g., spectrum, power) can be managed or owned by S, where S may not allow R to transmit its own information on top of forwarding S's messages to D. This is due to the fact that R's additional transmission may cause interference within the specific spectrum owned/managed by S and also consume more transmit power, which is possibly wirelessly transferred from S (owned by S) and should be only used for forwarding S's information. Therefore, this additional transmission of R should be kept covert from S.

We note that conceptually the covert transmission from R to D is similar to steganography, in which covert information is transmitted by hiding in innocuous objects [27]. These innocuous objects are utilized as "cover text" to carry the covert information. In our work, the innocuous objects are the forwarding transmissions from R to D. The main difference between our work and steganography is that in our work the covert information is shielded by the forwarding transmissions from R to D at the physical layer, while in steganography the covert information is hidden and transmitted by encoding or modifying some contents (e.g., shared videos or images) at the application layer (as discussed in Section III of [14]).

In the literature, covert communications with positive transmission rate are achieved in the context of point-to-point systems by considering different uncertainty sources, such as random received noise power [22], random jamming signals [23], and imperfect CSI [25]. In the considered relay networks, as mentioned above the uncertainty is inherently embedded in the forwarding strategies of the S's information from R to D, where the covert transmission with a positive rate from R to D does not require any extra uncertainty sources. The performance of the considered covert communication in relay networks and the covert communication in other point-to-point communication systems highly depends on the amount of uncertainty appeared in the system model. As such, it is hard to compare the achieved covert rate limits or warden's detection limits directly, since the uncertainty sources are different and it is hard to quantify the corresponding amount of uncertainty in the same manner.

Our main contributions are summarized below.

- We examine the possibility and achievable performance of covert communications in one-way relay networks. Specifically, we propose two strategies for R to transmit the covert information to D, namely the rate-control and power-control transmission schemes, in which the transmission rate and transmit power of the covert message are fixed and to be optimized regardless of the channel quality from R to D, respectively. We also identify the necessary conditions that the covert transmission from R to D can possibly occur without being detected by S with probability one and clarify how R hides its covert transmission in forwarding S's message to D in these two schemes.
- We derive the detection limits at S in terms of the prior probability of null hypothesis $1-\omega$, the prior probability of alternative hypothesis ω, the false alarm rate α and miss detection rate β are in closed-from expressions for the proposed two transmission schemes. Then, we determine the optimal detection threshold at S, which minimizes the detection error probability $\xi = (1-\omega)\alpha + \omega\beta$ and obtain the associated minimum detection error probability ξ^*. Our analysis leads to many useful insights. For example, we analytically prove that ξ^* increases with R's maximum transmit power, which indicates that boosting the forwarding ability of R also increases its capacity to perform covert transmissions. This demonstrates a tradeoff between the achievable effective covert rate and R's ability to aid the transmission from S to D.
- We analyze the effective covert rates achieved by these two schemes subject to the covert constraint $\xi^* \geq \min(1-\omega, \omega) - \epsilon$, where $\epsilon \in [0, 1]$ is predetermined to specify the covert constraint. Our analysis indicates that the achievable effective covert rate approaches zero as the transmission rate from S to D approaches zero, which demonstrates that covert transmission from R to D is only feasible with the legitimate transmission from S to D as the shield. Our examination shows that the rate-control transmission scheme outperforms the power-

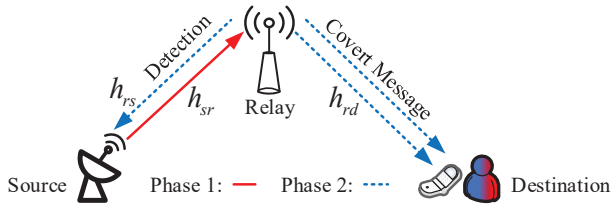


Fig. 1. Covert communication in one-way relay networks.

control transmission scheme under some specific conditions, and vise versa. Our examination enables R to switch between these two schemes in order to achieve a higher effective covert rate.

The rest of this paper is organized as follows. Section II details our system model and adopted assumptions. Section III and IV present the rate-control and power-control transmission schemes, respectively. Thorough analysis on the performance of these two transmission are provided in these two sections as well. Section V provides numerical results to confirm our analysis and provide useful insights on the impact of some parameters. Section VI draws conclusions.

Notation: Scalar variables are denoted by italic symbols. Vectors is denoted by lower-case boldface symbols. Given a complex number, $|\cdot|$ denotes the modulus. Given a complex vector, $(\cdot)^\dagger$ denotes the conjugate transpose. $\mathbb{E}[\cdot]$ denotes expectation operation.

II. System Model

A. Considered Scenario and Adopted Assumptions

As shown in Fig. 1, in this work we consider a one-way relay network, in which S transmits information to D with the aid of R, since a direct link from S to D is not available. As mentioned in the introduction, S allocates some resource to R in order to seek its help to relay the message to D. However, in some scenarios R may intend to use this resource to transmit its own message to D as well, which is forbidden by S and thus should be kept covert from S. As such, in the considered system model S is also the warden to detect whether R transmits its own information to D when it is aiding the transmission from S to D.

We assume the wireless channels within our system model are subject to independent quasi-static Rayleigh fading with equal block length and the channel coefficients are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with zero-mean and unit-variance. We also assume that each node is equipped with a single antenna. The channel from S to R is denoted by h_{sr} and the channel from R to D is denoted by h_{rd}. We assume R knows both h_{sr} and h_{rd} perfectly, while S only knows h_{sr} and D only knows h_{rd}. Considering channel reciprocity, we assume the channel from R to S (denoted by h_{rs}) is the same as h_{sr} and thus it is perfectly known by S. We further assume that R operates in the half-duplex mode and thus the transmission from S to D occurs in two phases: phase 1 (S transmits to R) and phase 2 (R transmits to D).

B. Transmission from Source to Relay (Phase 1)

In phase 1, the received signal at R is given by

$$\mathbf{y}_r[i] = \sqrt{P_s} h_{sr} \mathbf{x}_b[i] + \mathbf{n}_r[i], \tag{1}$$

where P_s is the fixed transmit power of S, $\mathbf{x}_b$ is the transmitted signal by S satisfying $\mathbb{E}[\mathbf{x}_b[i]\mathbf{x}_b^\dagger[i]] = 1$, $i = 1, 2, \ldots, n$ is the index of each channel use (n is the total number of channel uses in each phase), and $\mathbf{n}_r[i]$ is the AWGN at relay with σ_r^2 as its variance, i.e., $\mathbf{n}_r[i] \sim \mathcal{CN}(0, \sigma_r^2)$. In the literature, multiple approaches have been developed to estimate the noise variance at a receiver. In general, these approaches can be divided into two major categories: data-aided (DA) approaches and non-data-aided (NDA) approaches [28]. The DA approaches assume that transmitted symbols are known at the receiver and maximum-likelihood estimation can be used to estimate the noise variance. For the NDA approaches, transmit symbols are unknown at the receiver and the noise variance is based on the statistics of the received signals. In this work, we consider that R operates in the AF mode and thus R will forward a linearly amplified version of the received signal to D in phase 2. As such, the forwarded (transmitted) signal by R is given by

$$\mathbf{x}_r[i] = G\mathbf{y}_r[i] = G(\sqrt{P_s} h_{sr} \mathbf{x}_b[i] + \mathbf{n}_r[i]), \tag{2}$$

which is a linear scaled version of the received signal by a scalar G. In order to guarantee the power constraint at R, the value of G is chosen such that $\mathbb{E}[\mathbf{x}_r[i]\mathbf{x}_r^\dagger[i]] = 1$, which leads to $G = 1/\sqrt{P_s|h_{sr}|^2 + \sigma_r^2}$.

In this work, we also consider that the transmission rate from S to D is predetermined, which is denoted by R_{sd}. We also consider a maximum power constraint at R, i.e., $P_r \leq P_r^{\max}$. As such, although R knows both h_{sr} and h_{rd} perfectly, transmission outage from S to D still incurs when $C_{sd}^{\max} < R_{sd}$, where $C_{sd}^{\max}$ is the channel capacity from S to D for $P_r = P_r^{\max}$. Then, the transmission outage probability is given by $\delta = \mathcal{P}[C_{sd}^{\max} < R_{sd}]$, which has been derived in a closed-form expression [29]. We assume that all the nodes in the network do not transmit signals when the outage occurs. In practice, the pair of R_{sd} and δ determines the specific aid (i.e., the value of $P_r^{\max}$) required by S from R, which relates to the amount of resource allocated to R by S as a payback. In this work, we assume both R_{sd} and δ are predetermined, which leads to a predetermined $P_r^{\max}$.

C. Transmission Strategies at Relay (Phase 2)

In this subsection, we detail the transmission strategies of R when it does and does not transmit its own information to D. We also determine the condition that R can transmit its own message to D without being detected by S with probability one, in which the probability to guarantee this condition is also derived.

1) Relay's Transmission without the Covert Message: In the case when the relay does not transmit its own message (i.e., covert message) to Bob, it only transmits $\mathbf{x}_r$ to D. Accordingly, the received signal at D is given by

$$\begin{aligned}\mathbf{y}_d[i] &= \sqrt{P_r^0} h_{rd} \mathbf{x}_r[i] + \mathbf{n}_d[i] \\ &= \sqrt{P_r^0} G h_{rd} \sqrt{P_s} h_{sr} \mathbf{x}_b[i] + \sqrt{P_r^0} G h_{rd} \mathbf{n}_r[i] + \mathbf{n}_d[i],\end{aligned} \tag{3}$$

where P_r^0 is the transmit power of $\mathbf{x}_r$ at R in this case and $\mathbf{n}_d[i]$ is the AWGN at D with σ_d^2 as its variance, i.e., $\mathbf{n}_d[i] \sim \mathcal{CN}(0, \sigma_d^2)$. Accordingly, the signal-to-noise ratio (SNR) at the destination for $\mathbf{x}_b$, which has been derived in a closed-form expression in [30], is given by

$$\begin{aligned}\gamma_d &= \frac{P_s|h_{sr}|^2 P_r^0 |h_{rd}|^2 G^2}{P_r^0|h_{rd}|^2 G^2\sigma_r^2 + \sigma_d^2} \\ &= \frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1},\end{aligned} \tag{4}$$

where $\gamma_1 \triangleq (P_s|h_{sr}|^2)/\sigma_r^2$, $\gamma_2 \triangleq (P_r^0|h_{rd}|^2)/\sigma_d^2$, and the scalar G is defined earlier as $G = 1/\sqrt{P_s|h_{sr}|^2 + \sigma_r^2}$.

For a predetermined R_{sd}, R does not have to adopt the maximum transmit power for each channel realization in order to guarantee a specific transmission outage probability. When the transmission outage occurs (i.e., $C_{sd}^{\max} < R_{sd}$ occurs), R will not transmit (i.e., $P_r^0 = 0$). When $C_{sd}^{\max} \geq R_{sd}$, R only has to ensure $C_{sd} = R_{sd}$, where $C_{sd} = 1/2\log_2(1+\gamma_d)$. Then, following (4) the transmit power of R when $C_{sd}^{\max} \geq R_{sd}$ is given by $P_r^0 = \mu\sigma_d^2/|h_{rd}|^2$, where

$$\mu \triangleq \frac{(P_s|h_{sr}|^2 + \sigma_r^2)(2^{2R_{sd}}-1)}{[P_s|h_{sr}|^2 - \sigma_r^2(2^{2R_{sd}}-1)]}. \tag{5}$$

We note that (5) indicates that R does not use its maximum transmit power $P_r^{\max}$ to forward S's information when it does not transmit covert information to D. This is due to the fact that the transmission from S to D is of a fixed rate R_{sd} and a larger transmit power that leads to $C_{sd} > R_{sd}$ (not $C_{sd} = R_{sd}$) does not bring in extra benefit to this transmission from S to D. As such, in order to save energy R only sets its transmit power as per (5) to guarantee $C_{sd} = R_{sd}$. Noting $\gamma_d < \gamma_1$, we have $1/2\log_2(1+\gamma_1) > R_{sd}$ when $C_{sd} = R_{sd}$. As such, μ given in (5) is nonnegative. Following (4), we note that $C_{sd}^* \geq R_{sd}$ requires $|h_{rd}|^2 \geq \mu\sigma_d^2/P_r^{\max}$. As such, the transmit power of R without a covert message is given by

$$P_r^0 = \begin{cases} \frac{\mu\sigma_d^2}{|h_{rd}|^2}, & |h_{rd}|^2 \geq \frac{\mu\sigma_d^2}{P_r^{\max}}, \\ 0, & |h_{rd}|^2 < \frac{\mu\sigma_d^2}{P_r^{\max}}. \end{cases} \tag{6}$$

As per (6), we note that relay will forward message when $|h_{rd}|^2 \geq \mu\sigma_d^2/P_r^{\max}$ is met. We denote this necessary condition as $\mathbb{B}$. As such, R will forward $\mathbf{x}_b$ to D and S will perform detection whenever condition $\mathbb{B}$ is met. Considering quasi-static Rayleigh fading, the cumulative distribution function (cdf) of $|h_{rd}|^2$ is given by $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$ and thus the probability that $\mathbb{B}$ is guaranteed is given by

$$\mathcal{P}_B = \exp\left\{-\frac{\mu\sigma_d^2}{P_r^{\max}}\right\}. \tag{7}$$

2) Relay's Transmission with the Covert Message: In the case when R transmits the covert message to D on top of forwarding $\mathbf{x}_b$, the received signal at D is given by

$$\begin{aligned}\mathbf{y}_d[i] = &\sqrt{P_r^1}Gh_{rd}\sqrt{P_s}h_{sr}\mathbf{x}_b[i] + \sqrt{P_\Delta}h_{rd}\mathbf{x}_c[i] + \\ &\sqrt{P_r^1}Gh_{rd}\mathbf{n}_r[i] + \mathbf{n}_d[i],\end{aligned} \tag{8}$$

where P_r^1 is R's transmit power of $\mathbf{x}_b$ in this case and P_Δ is R's transmit power of the covert message $\mathbf{x}_c$ satisfying $\mathbb{E}[\mathbf{x}_c[i]\mathbf{x}_c^\dagger[i]] = 1$. We note that the covert transmission from R to D should not affect the transmission from S to D. Otherwise, S can easily observe this covert transmission. As such, here we assume D always first decodes $\mathbf{x}_b$ with $\mathbf{x}_c$ as interference. Following (8), the signal-to-interference-plus-noise ratio (SINR) for $\mathbf{x}_b$ is given by

$$\begin{aligned}\gamma_d &= \frac{P_s|h_{sr}|^2 P_r^1 |h_{rd}|^2 G^2}{P_r^1|h_{rd}|^2 G^2\sigma_r^2 + P_\Delta|h_{rd}|^2 + \sigma_d^2} \\ &= \frac{\gamma_1\gamma_3}{\gamma_3 + (\gamma_1+1)(\gamma_3 P_\Delta/P_r^1+1)},\end{aligned} \tag{9}$$

where $\gamma_3 \triangleq (P_r^1|h_{rd}|^2)/\sigma_d^2$. We will determine P_r^1 based on different transmission strategies of the covert message from R to D.

D. Decoding of the Covert Message

As discussed above, the covert transmission from R to D should not affect the transmission from S to D and thus we have to guarantee the successful decoding of $\mathbf{x}_b$ even when $\mathbf{x}_c$ is treated as interference to $\mathbf{x}_b$. We also note that this covert transmission cannot happen when the transmission outage from S to D occurs. This is, for example, due to the fact that when the transmission outage occurs R will request a retransmission from S, which enables S to detect R's covert transmission with probability one if the covert transmission happened. Therefore, the covert transmission from R to D only occur when the successful transmission from S to D is guaranteed (i.e., when $\mathbf{x}_b$ is successfully decoded at D). As such, when the covert message is transmitted by R, successive interference cancellation (SIC) that allows a receiver to decode different signals that arrive simultaneously is implemented at D. Taking advantage of SIC, D decodes the stronger signal (i.e., $\mathbf{x}_b$) first, subtracts it from the combined signal $\mathbf{y}_d$ given in (8), and finally decodes the weaker one (i.e., $\mathbf{x}_c$) from the residue. We also note that D cannot jointly decode $\mathbf{x}_b$ and $\mathbf{x}_c$ due to the fact that the codebooks used for encoding $\mathbf{x}_b$ and $\mathbf{x}_c$ are different in order to guarantee that the codebook for $\mathbf{x}_c$ is unknown while the codebook for $\mathbf{x}_b$ is known to the S. Hence, the effective received signal used to decode the covert message $\mathbf{x}_c$ is given by

$$\tilde{\mathbf{y}}_d[i] = \sqrt{P_\Delta}h_{rd}\mathbf{x}_c[i] + \sqrt{P_r^1}h_{rd}G\mathbf{n}_r[i] + \mathbf{n}_d[i]. \tag{10}$$

Then, following (10) the SINR for $\mathbf{x}_c$ is

$$\gamma_\Delta = \frac{P_\Delta|h_{rd}|^2}{P_r^1|h_{rd}|^2 G^2\sigma_r^2 + \sigma_d^2}. \tag{11}$$

E. Binary Detection at Source and the Covert Constraint

In this subsection, we present the optimal detection strategy adopted by S (i.e., Source).

In phase 2 when R transmits to D, S will detect whether R transmits the covert message $\mathbf{x}_c$ on top of forwarding S's message $\mathbf{x}_b$ to D. R does not transmit $\mathbf{x}_c$ in the null hypothesis $\mathcal{H}_0$ while it does in the alternative hypothesis $\mathcal{H}_1$. Then, the

received signal at S in phase 2 is given by

$$\mathbf{y}_s[i] = \begin{cases} \sqrt{P_r^0}h_{rs}\mathbf{x}_r[i]+\mathbf{n}_s[i], & \mathcal{H}_0, \\ \sqrt{P_r^1}h_{rs}\mathbf{x}_r[i]+\sqrt{P_\Delta}h_{rs}\mathbf{x}_c[i]+\mathbf{n}_s[i], & \mathcal{H}_1, \end{cases}$$
$$= \begin{cases} \frac{\sqrt{P_r^0}h_{rs}}{\sqrt{P_s|h_{sr}|^2+\sigma_r^2}}(\sqrt{P_s}h_{sr}\mathbf{x}_b[i]+\mathbf{n}_r[i])+\mathbf{n}_s[i], & \mathcal{H}_0, \\ \frac{\sqrt{P_r^1}h_{rs}}{\sqrt{P_s|h_{sr}|^2+\sigma_r^2}}(\sqrt{P_s}h_{sr}\mathbf{x}_b[i]+ \\ \mathbf{n}_r[i])+\sqrt{P_\Delta}h_{rs}\mathbf{x}_c[i]+\mathbf{n}_s[i], & \mathcal{H}_1. \end{cases} \quad (12)$$

Noting that $\mathbf{x}_b[i]$ is known by S, hence, S can cancel the corresponding component from its received signal $\mathbf{y}_s[i]$, due to the fact the infinite blocklength is considered in this work and S can exactly estimate the scale factor of $\mathbf{x}_b[i]$. Then, the effective received signal used for detection at S is given by

$$\tilde{\mathbf{y}}_s[i] = \begin{cases} \frac{\sqrt{P_r^0}h_{rs}}{\sqrt{P_s|h_{sr}|^2+\sigma_r^2}}\mathbf{n}_r[i]+\mathbf{n}_s[i], & \mathcal{H}_0, \\ \frac{\sqrt{P_r^1}h_{rs}}{\sqrt{P_s|h_{sr}|^2+\sigma_r^2}}\mathbf{n}_r[i]+\sqrt{P_\Delta}h_{rs}\mathbf{x}_c[i]+\mathbf{n}_s[i], & \mathcal{H}_1. \end{cases} \quad (13)$$

Following (13), the probability density functions of the observations $\tilde{\mathbf{y}}_s$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are, respectively, given by

$$f(\tilde{\mathbf{y}}_s|\mathcal{H}_0) = \prod_{i=1}^{n} f(\tilde{\mathbf{y}}_s[i]|\mathcal{H}_0)$$
$$= \frac{1}{\left(2\pi\sigma_{\mathcal{H}_0}^2\right)^{\frac{n}{2}}} \exp\left\{-\frac{1}{2\sigma_{\mathcal{H}_0}^2}\sum_{i=1}^{n}|\tilde{\mathbf{y}}_s[i]|^2\right\}, \quad (14)$$

$$f(\tilde{\mathbf{y}}_s|\mathcal{H}_1) = \prod_{i=1}^{n} f(\tilde{\mathbf{y}}_s[i]|\mathcal{H}_1)$$
$$= \frac{1}{\left(2\pi\sigma_{\mathcal{H}_1}^2\right)^{\frac{n}{2}}} \exp\left\{-\frac{1}{2\sigma_{\mathcal{H}_1}^2}\sum_{i=1}^{n}|\tilde{\mathbf{y}}_s[i]|^2\right\}, \quad (15)$$

where $\sigma_{\mathcal{H}_0}^2 \triangleq P_r^0|h_{rs}|^2\sigma_r^2/(P_s|h_{sr}|^2+\sigma_r^2)+\sigma_s^2$ and $\sigma_{\mathcal{H}_1}^2 \triangleq P_r^1|h_{rs}|^2\sigma_r^2/(P_s|h_{sr}|^2+\sigma_r^2)+P_\Delta|h_{rs}|^2+\sigma_s^2$. Following (14) and (15), based on the Fisher-Neyman factorization theorem [31], we note that the term $T(n) = \sum_{i=1}^{n}|\tilde{\mathbf{y}}_s[i]|^2$ is the sufficient test statistic for the detector at S. As such, the detector at S for an arbitrary threshold is given by

$$\frac{1}{n}T(n) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \tau, \quad (16)$$

where τ is the threshold for (1/n)$T(n)$, which will be determined later, $\mathcal{D}_1$ and $\mathcal{D}_0$ are the binary decisions that infer whether R transmits covert message or not, respectively. We will examine how S sets the optimal value of τ in order to minimize the detection error probability in the following sections for considered different transmission strategies. Considering infinite blocklength, i.e., $n \to \infty$, we have

$$\lim_{n\to\infty}\frac{1}{n}T(n) = \begin{cases} P_r^0|h_{rs}|^2\phi+\sigma_s^2, & \mathcal{H}_0, \\ P_r^1|h_{rs}|^2\phi+P_\Delta|h_{rs}|^2+\sigma_s^2, & \mathcal{H}_1, \end{cases} \quad (17)$$

where $\phi \triangleq \sigma_r^2/(P_s|h_{sr}|^2+\sigma_r^2)$.

The detection performance of S is normally measured by its detection error probability, which is defined as

$$\xi \triangleq (1-\omega)\alpha+\omega\beta, \quad (18)$$

where $\omega = \mathcal{P}(\mathcal{H}_1)$ is the probability that R transmits a covert message, $1-\omega = \mathcal{P}(\mathcal{H}_0)$ is the probability that R does not transmit a covert message, $\alpha = \mathcal{P}(\mathcal{D}_1|\mathcal{H}_0)$ is S's false alarm rate, and $\beta = \mathcal{P}(\mathcal{D}_0|\mathcal{H}_1)$ is S's miss detection rate.

In practice, it is hard to know ξ at R since the threshold τ adopted by S is unknown. In this work, we consider the worst-case scenario where τ is optimized at S to minimize ξ. As such, the covert constraint considered in this work is $\xi^* \geq \min\{1-\omega,\omega\}-\epsilon$, where ξ^* is the minimum detection error probability achieved at S.

III. Rate-Control Transmission Scheme

In this section, we consider the rate-control transmission scheme, in which R transmits a covert message to D with a constant rate when some specific realizations of $|h_{rd}|^2$ are guaranteed. To this end, R varies its transmit power as per h_{rd} such that $P_\Delta|h_{rd}|^2$ is fixed as Q. Specifically, we first determine R's transmit power in $\mathcal{H}_1$ and then analyze the detection error probability at S, based on which we also derive S's optimal detection threshold. Furthermore, we derive the effective covert rate achieved by the rate-control transmission scheme.

A. Transmit Power at Relay under $\mathcal{H}_1$

Following (9) and defining $Q = P_\Delta|h_{rd}|^2$, in order to guarantee $C_{sd} = R_{sd}$ under $\mathcal{H}_1$, P_r^1 is given as

$$P_r^1 = \frac{\mu(Q+\sigma_d^2)}{|h_{rd}|^2}, \quad (19)$$

which requires $C_{sd}^* \geq R_{sd}$ that leads to $|h_{rd}|^2 \geq (\mu\sigma_d^2+\mu Q+Q)/P_r^{\max}$. We note that P_r^1 is the transmit power of the relay to forward the signal from S to D. In practical scenario, R can set the value of P_r^1 as per the system parameters h_{sr}, h_{rd}, P_s, σ_r^2, σ_d^2, R_{sd}, and Q. The values of these system parameters are known by R. Specifically, h_{sr} can h_{rd} can be obtained through channel estimations. The values of σ_r^2 and σ_d^2 can be achieved through *a priori* measurements collected from the environment, where σ_d^2 is fed back from D to R. The value of R_{sd} is predetermined by the QoS requirement of the communication from S to D, while the value of Q is a design parameter to determine at R. Considering the maximum power constraint at R (i.e., $P_r^1+P_\Delta \leq P_r^{\max}$ under this case), R has to give up the transmission of the covert message (i.e., $P_\Delta = 0$) when $P_r^1 > P_r^{\max}-P_\Delta$ and sets P_r^1 the same as P_r^0 given in (6). This is due to the fact that S knows h_{rs} and it can detect with probability one when the total transmit power of R is greater than $P_r^{\max}$. Then, the transmit power of $\mathbf{x}_r$ under $\mathcal{H}_1$ for the rate-control transmission scheme is given by

$$P_r^1 = \begin{cases} \frac{\mu(Q+\sigma_d^2)}{|h_{rd}|^2}, & |h_{rd}|^2 \geq \frac{\mu\sigma_d^2+\mu Q+Q}{P_r^{\max}}, \\ \frac{\mu\sigma_d^2}{|h_{rd}|^2}, & \frac{\mu\sigma_d^2}{P_r^{\max}} \leq |h_{rd}|^2 < \frac{\mu\sigma_d^2+\mu Q+Q}{P_r^{\max}}, \\ 0, & |h_{rd}|^2 < \frac{\mu\sigma_d^2}{P_r^{\max}}. \end{cases} \quad (20)$$

As per (20), when R cannot support the transmission from S to D (i.e., when $|h_{rd}|^2 < \mu\sigma_d^2/P_r^{\max}$), R or D will send the retransmission request to S and R should not forward $\mathbf{x}_b$, since this forwarding will definitely fail. In the meantime, S is aware of that the received energy comes from the R's covert transmission if R has transmitted the covert message during this period. Due to that the CSI of all the channels is available to R, R knows exactly when the transmission outage from R to D occurs and thus R will not transmit covert information to D when this outage occurs. In summary, S cannot detect R's covert transmission with probability one only when the condition $|h_{rd}|^2 \geq (\mu\sigma_d^2 + \mu Q + Q)/P_r^{\max}$ is guaranteed. We denote this necessary condition for covert communication as $\mathbb{C}$. Considering quasi-static Rayleigh fading, the cumulative distribution function (cdf) of $|h_{rd}|^2$ is given by $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$ and thus the probability that $\mathbb{C}$ is guaranteed is given by

$$\mathcal{P}_C = \exp\left\{-\frac{\mu\sigma_d^2 + \mu Q + Q}{P_r^{\max}}\right\}. \tag{21}$$

We note that $\mathcal{P}_C$ is a monotonically decreasing function of Q, which indicates that the probability that R will transmit a covert message decreases as Q increases.

In this work, we consider quasi-static Rayleigh fading channels where the channels remain constant within each transmission period and vary independently from one period to another. We would like to clarify that R could possibly transmit a covert message to D without being detected during a retransmission from S to D (i.e., new transmission period) when the condition $\mathbb{C}$ is met.

B. Detection Error Probability at Source

In this subsection, we derive S's false alarm rate, i.e., α, and miss detection rate, i.e., β.

***Theorem** 1:* When the condition $\mathbb{B}$ is guaranteed, for a given τ, the false alarm and miss detection rates at S are derived as

$$\alpha = \begin{cases} 1, & \tau < \sigma_s^2, \\ 1 - \mathcal{P}_B^{-1}\kappa_1(\tau), & \sigma_s^2 \leq \tau \leq \rho_1, \\ 0, & \tau > \rho_1, \end{cases} \tag{22}$$

$$\beta = \begin{cases} 0, & \tau < \sigma_s^2, \\ \mathcal{P}_B^{-1}\kappa_2(\tau), & \sigma_s^2 \leq \tau \leq \rho_2, \\ 1, & \tau > \rho_2, \end{cases} \tag{23}$$

where

$$\begin{aligned} \rho_1 &\triangleq P_r^{\max}|h_{rs}|^2\phi + \sigma_s^2, \\ \rho_2 &\triangleq P_r^{\max}|h_{rs}|^2\left(\phi + \frac{(\phi\mu+1)Q}{\mu\sigma_d^2}\right) + \sigma_s^2, \\ \kappa_1(\tau) &\triangleq \exp\left\{-\frac{\phi\mu\sigma_d^2|h_{rs}|^2}{\tau - \sigma_s^2}\right\}, \\ \kappa_2(\tau) &\triangleq \exp\left\{-\frac{\left(\phi\mu\sigma_d^2 + (\phi\mu+1)\,Q\right)|h_{rs}|^2}{\tau - \sigma_s^2}\right\}. \end{aligned} \tag{24}$$

Proof: Considering the maximum power constraint at R under $\mathcal{H}_0$ (i.e., $P_r^0 \leq P_r^{\max}$) and following (6), (16), and (17), the false alarm rate under the condition $\mathbb{B}$ is given by

$$\begin{aligned} \alpha &= \mathcal{P}\left[\frac{\mu\sigma_d^2}{|h_{rd}|^2}|h_{rs}|^2\phi + \sigma_s^2 \geq \tau \middle| \mathbb{B}\right] \\ &= \begin{cases} 1, & \tau < \sigma_s^2, \\ \mathcal{P}\left[\frac{\mu\sigma_d^2}{P_r^{\max}} \leq |h_{rd}|^2 \leq \frac{\mu\sigma_d^2|h_{rs}|^2\phi}{\tau - \sigma_s^2}\right]\mathcal{P}_B^{-1}, & \sigma_s^2 \leq \tau \leq \rho_1, \\ 0, & \tau > \rho_1. \end{cases} \end{aligned} \tag{25}$$

Then, substituting $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$ into the above equation (h_{rs} is perfectly known by S and thus it is not a random variable here) we achieve the desired result in (22).

Considering the maximum power constraint at R under $\mathcal{H}_1$ (i.e., $P_r^1 + P_\Delta \leq P_r^{\max}$) and following (16), (17), and (20), the miss detection rate under the condition $\mathbb{B}$ is given by

$$\begin{aligned} \beta &= \mathcal{P}\left[\frac{\mu(Q+\sigma_d^2)|h_{rs}|^2\phi}{|h_{rd}|^2} + \frac{Q|h_{rs}|^2}{|h_{rd}|^2} + \sigma_s^2 < \tau \middle| \mathbb{B}\right] \\ &= \begin{cases} 0, & \tau < \sigma_s^2, \\ \mathcal{P}\left[|h_{rd}|^2 \geq \frac{\left(\phi\mu\left(\sigma_d^2+Q\right)+Q\right)|h_{rs}|^2}{\tau - \sigma_s^2}\right]\mathcal{P}_B^{-1}, & \sigma_s^2 \leq \tau \leq \rho_2, \\ 1, & \tau > \rho_2. \end{cases} \end{aligned} \tag{26}$$

Then, substituting $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$ into (26) we achieve the desired result in (23). ■

We note that the false alarm and miss detection rates given in Theorem 1 are functions of the threshold τ and we next examine how S sets the value of τ to minimize its detection error probability in the following subsection.

C. Optimization of the Detection Threshold at Source

In this subsection, we derive the optimal value of the detection threshold τ that minimizes the detection error probability ξ for the rate-control transmission scheme.

***Theorem** 2:* The optimal threshold that minimizes ξ for the rate-control transmission scheme is given by

$$\tau^* = \begin{cases} \rho_1, & \tau^\ddagger \leq \sigma_s^2, \\ \min\left\{\tau^\ddagger, \rho_1\right\}, & \tau^\ddagger > \sigma_s^2, \end{cases} \tag{27}$$

where

$$\tau^\ddagger \triangleq \frac{(\phi\mu+1)Q|h_{rs}|^2}{\ln\left(\frac{\omega_1}{1-\omega_1}\left(1 + \frac{(\phi\mu+1)Q}{\phi\mu\sigma_d^2}\right)\right)} + \sigma_s^2, \tag{28}$$

$$\omega_1 \triangleq \frac{1}{2}\exp\left\{-\frac{(\mu+1)Q}{P_r^{\max}}\right\}. \tag{29}$$

Proof: As discussed before, S will perform detection whenever condition $\mathbb{B}$ is met and R can transmit covert message when condition $\mathbb{C}$ is guaranteed. In our work, we assume that R will transmit a covert message with probability 50% when $\mathbb{C}$ is true. As per (7) and (21), the probability $\mathcal{P}(\mathcal{H}_1)$ is given by

$$\mathcal{P}(\mathcal{H}_1) = \frac{1}{2}\mathcal{P}\left[\mathbb{C}\middle|\mathbb{B}\right] = \omega_1. \tag{30}$$

Then, $\mathcal{P}(\mathcal{H}_0)$ is given by

$$\mathcal{P}(\mathcal{H}_0) = 1 - \mathcal{P}(\mathcal{H}_1) = 1 - \omega_1. \tag{31}$$

Since $\rho_2 > \rho_1$ as given in Theorem 1, following (22) and (23), we have the detection error probability at S as

$$\xi = \begin{cases} 1-\omega_1, & \tau \le \sigma_s^2, \\ 1-\omega_1-\mathcal{P}_B^{-1}[(1-\omega_1)\kappa_1(\tau)- & \\ \omega_1\kappa_2(\tau)], & \sigma_s^2 < \tau \le \rho_1, \\ \omega_1\mathcal{P}_B^{-1}\kappa_2(\tau), & \rho_1 \le \tau < \rho_2, \\ \omega_1, & \tau \ge \rho_2. \end{cases} \quad (32)$$

We first note that $\xi = 1-\omega_1$ or ω_1 are the worst case for S and thus S does not set $\tau \le \sigma_s^2$ or $\tau > \rho_2$. Following (32), we derive the first derivative of ξ with respect to τ when $\rho_1 \le \tau < \rho_2$ as

$$\frac{\partial(\xi)}{\partial\tau} = \frac{\omega_1\mathcal{P}_B^{-1}\left(\phi\mu\left(\sigma_d^2+Q\right)+Q\right)|h_{rs}|^2}{(\tau-\sigma_s^2)^2}\kappa_2(\tau) > 0. \quad (33)$$

This demonstrates that ξ is an increasing function of τ when $\rho_1 \le \tau < \rho_2$. Thus, S will set ρ_1 as the threshold to minimize ξ if $\rho_1 \le \tau < \rho_2$. We next derive the first derivative of ξ with respect to τ for $\sigma_s^2 < \tau \le \rho_1$ as

$$\begin{aligned} \frac{\partial(\xi)}{\partial\tau} &= \frac{\mathcal{P}_B^{-1}|h_{rs}|^2}{(\tau-\sigma_s^2)^2}\Big[\omega_1\left(\phi\mu\left(\sigma_d^2+Q\right)+Q\right)\kappa_2(\tau)- \\ &\qquad (1-\omega_1)\phi\mu\sigma_d^2\kappa_1(\tau)\Big] \\ &= \frac{\omega_1\mathcal{P}_B^{-1}\left(\phi\mu\left(\sigma_d^2+Q\right)+Q\right)|h_{rs}|^2\kappa_2(\tau)}{(\tau-\sigma_s^2)^2}\times \\ &\quad \left\{1-\frac{(1-\omega_1)\phi\mu\sigma_d^2}{\omega_1\left(\phi\mu(\sigma_d^2+Q)+Q\right)}\exp\left\{\frac{(\phi\mu+1)Q|h_{rs}|^2}{\tau-\sigma_s^2}\right\}\right\}. \end{aligned} \quad (34)$$

We note that $\omega_1\mathcal{P}_B^{-1}\left(\phi\mu\left(\sigma_d^2+Q\right)+Q\right)|h_{rs}|^2\kappa_2(\tau)/(\tau-\sigma_s^2)^2 > 0$ due to $\sigma_s^2 < \tau$ and $\kappa_2(\tau) > 0$ as given in Theorem 1. As such, without the constraint $\tau \le \rho_1$, the value of τ that ensures $\partial(\xi)/\partial\tau = 0$ in (34) is given by $\tau^\ddagger$. We note that $\partial(\xi)/\partial\tau < 0$, for $\tau < \tau^\ddagger$, and $\partial(\xi)/\partial\tau > 0$, for $\tau > \tau^\ddagger$. This is due to the term $\exp\{(\phi\mu+1)Q|h_{rs}|^2/(\tau-\sigma_s^2)\}$ in (34) is monotonically decreasing with respect to τ. This indicates that $\tau^\ddagger$ minimizes ξ without the constraint $\tau \le \rho_1$. We also note that ξ given in (32) is a not a continuous function of τ following Theorem 1 when $\tau^\ddagger \le \sigma_s^2$. This is due to that $1-\omega_1-\mathcal{P}_B^{-1}[(1-\omega_1)\kappa_1(\tau)-\omega_1\kappa_2(\tau)]$ is monotonically increasing with respect to τ when $\tau^\ddagger \le \sigma_s^2$. We note that ξ is also monotonically increasing with respect to τ for $\rho_1 \le \tau < \rho_2$, thus will lead to $\omega_1 \ge 1-\omega_1$. As such, if $\tau^\ddagger \le \sigma_s^2$, the optimal threshold is $\tau^* = \rho_1$.. If $\tau^\ddagger > \sigma_s^2$, following (33) and noting ξ is a continuous function of τ, we can conclude that the optimal threshold is $\tau^* = \min\left\{\tau^\ddagger, \rho_1\right\}$. This completes the proof of Theorem 2. ∎

Following Theorem 2, we obtain the minimum detection error probability at S in the following corollary.

Corollary 1: The minimum value of ξ at S is

$$\xi^* = \begin{cases} (1-\omega_1)\Bigg\{1-\exp\left(\frac{\mu\sigma_d^2}{P_r^{\max}}\right)\times \\ \left(1-\frac{\phi\mu\sigma_d^2}{\phi\mu\sigma_d^2+(\phi\mu+1)Q}\right)\times \\ \left(\frac{\omega_1}{1-\omega_1}\left(1+\frac{(\phi\mu+1)Q}{\phi\mu\sigma_d^2}\right)\right)^{-\frac{\phi\mu\sigma_d^2}{(\phi\mu+1)Q}}\Bigg\}, & \tau^* = \tau^\ddagger, \\ \omega_1\exp\left\{-\frac{(\phi\mu+1)Q}{\phi P_r^{\max}}\right\}, & \tau^* = \rho_1. \end{cases} \quad (35)$$

Proof: Substituting τ^* into (32), we obtain the minimum value of ξ as $\xi^* = 1-\omega_1-\mathcal{P}_B^{-1}[(1-\omega_1)\kappa_1(\tau)-\omega_1\kappa_2(\tau)]$, which completes the proof of Corollary 1. ∎

Based on Theorem 1, Theorem 2, and Corollary 1, we draw the following useful insights.

Remark 1: We conclude that detection error probability ξ^* tends to 0 when R's additional covert power Q approaches infinity. This follows from (27) for $\tau^* = \rho_1$, since when $Q \to \infty$ we have $\tau^\ddagger < \sigma_s^2$ as per (28) and thus $\tau^* = \rho_1$.

Remark 2: When the maximum power constraint $P_r^{\max}$ approaches infinity, the minimum detection error probability ξ^* approaches a fixed value given by

$$\lim_{P_b^{\max}\to\infty}\xi^* = \frac{1}{2}\Bigg\{1-\underbrace{\left(1-\frac{\phi\mu\sigma_d^2}{\phi\mu\sigma_d^2+(\phi\mu+1)Q}\right)}_{f_1(Q)}\times \underbrace{\left(1+\frac{(\phi\mu+1)Q}{\phi\mu\sigma_d^2}\right)^{-\frac{\phi\mu\sigma_d^2}{(\phi\mu+1)Q}}}_{f_2(Q)}\Bigg\}. \quad (36)$$

The result in (36) follows from (27) for $\tau^* = \tau^\ddagger$, since when $P_r^{\max} \to \infty$ we have $\rho_1 \to \infty$ as per (24) and thus $\rho_1 > \tau^\ddagger$ (then $\tau^* = \tau^\ddagger$). Following (36), we can conclude that ξ^* monotonically decreases with Q when $P_r^{\max} \to \infty$. In order to prove this conclusion, we next prove that $f_2(Q)$ in (36) monotonically increases with Q, since $f_1(Q)$ in (36) is a monotonically increasing function of Q. Defining $(\phi\mu+1)Q/\mu\sigma_d^2 = x$, following (35) we have $f_2(Q) = f_2(x)$, where

$$f_2(x) = (1+x)^{-1/x}. \quad (37)$$

In order to determine the monotonicity of $f_2(x)$ with respect to x, we derive its first derivative as

$$\frac{\partial f_2(x)}{\partial x} = \exp\left\{-\frac{\ln(1+x)}{x}\right\}\frac{(1+x)\ln(1+x)-x}{x^2(1+x)}. \quad (38)$$

We note that whether $\partial f_2(x)/\partial x > 0$ or $\partial f_2(x)/\partial x < 0$ depends on $g(x) \triangleq (1+x)\ln(1+x)-x$. As such, we derive the first derivative of $g(x)$ with respect to x as

$$\frac{\partial g(x)}{\partial x} = \ln(1+x). \quad (39)$$

Noting that $x \ge 0$ and $\partial g(x)/\partial x \ge 0$, we conclude that $g(x)$ monotonically decreases with x. Then, we have $g(x) \ge g(0) = 0$ and thus $\partial f_2(x)/\partial x \ge 0$. This leads to that $f_2(Q)$ monotonically increases with Q and thus ξ^* monotonically

decreases with Q for $\tau^* = \tau^\ddagger$.
When $P_r^{\max} \to \infty$, ω_1 approaches 1/2 as per (29) and $\xi^* = \omega_1 - \epsilon$ can be written as

$$\underbrace{\left(1 - \frac{\phi\mu\sigma_d^2}{\phi\mu\sigma_d^2 + (\phi\mu+1)Q}\right)}_{f_1(Q)} \underbrace{\left(1 + \frac{(\phi\mu+1)Q}{\phi\mu\sigma_d^2}\right)^{-\frac{\phi\mu\sigma_d^2}{(\phi\mu+1)Q}}}_{f_2(Q)} = 2\epsilon. \tag{40}$$

Defining $y = \phi\mu\sigma_d^2/((\phi\mu+1)Q)$ and following the expression of $f_2(Q)$ in (40), we have

$$\lim_{y\to 0} f_2(Q) = \lim_{y\to 0}\left(\frac{y}{y+1}\right)^y = 0^0 = 1. \tag{41}$$

As per (40), for $y \to 0$ the approximated close-form expression of Q^ϵ is given by

$$Q^\epsilon = \frac{\phi\mu\sigma_d^2}{(\phi\mu+1)}\left(\frac{1}{1-2\epsilon} - 1\right). \tag{42}$$

***Remark** 3:* We have that the minimum detection error probability ξ^* tends to 0 when the data transmission rate R_{sd} approaches 0 or infinity. As $R_{sd} \to 0$, as per (5) we have $\mu \to 0$ and thus $\tau^\ddagger \to \sigma_s^2$ (then optimal threshold τ^* is equal to $\tau^\ddagger$) following (28). Then, from (35) for $\tau^* = \tau^\ddagger$ we can see that $\xi^* \to 0$ as $\mu \to 0$. As $R_{sd} \to \infty$, following (5) again we note that μ will be negative and thus the transmission from S to D fails, which leads to $\xi^* \to 0$ as discussed in Section III-A. This result means that there exists an optimal value of R_{sd} that maximizes ξ^* and thus maximizes the effective covert rate for given other system parameters. We will numerically examine the impact of R_{sd} on covert communications in Section V.

D. Optimization of Effective Covert Rate

In this section, we examine the effective covert rate achieved in the considered system subject to a covert constraint.

1) Effective Covert Rate: From (11), the SINR of $\mathbf{x}_c$ at D in the rate-control transmission scheme is given as

$$\gamma_\Delta = \frac{P_\Delta |h_{rd}|^2}{P_r^1 |h_{rd}|^2 G^2 \sigma_r^2 + \sigma_d^2} = \frac{Q}{\frac{\mu(Q+\sigma_d^2)}{\eta|h_{sr}|^2+1} + \sigma_d^2}, \tag{43}$$

where $\eta \triangleq P_s/\sigma_r^2$. Then, the covert rate achieved by R is $R_\Delta = \log_2(1+\gamma_\Delta)$. As such, we can see that the covert rate is fixed when Q is fixed as per (43). We next derive the effective covert rate, i.e., the covert rate averaged over all realizations of $|h_{rd}|^2$, in the following theorem.

***Theorem** 3:* The achievable effective covert rate R_c by R in the rate-control transmission scheme is derived as a function of Q given by

$$R_c = R_\Delta \mathcal{P}_C = \log_2\left(1 + \frac{Q}{\frac{\mu(Q+\sigma_d^2)}{\eta|h_{sr}|^2+1} + \sigma_d^2}\right) \times \exp\left\{-\frac{\mu\sigma_d^2 + \mu Q + Q}{P_r^{\max}}\right\}. \tag{44}$$

Based on Theorem 3, we note that R_c is not an increasing function of Q and thus R_Δ, since as Q increases R_Δ increases as per (44) while $\mathcal{P}_C$ decreases following (21). This indicates that there may exists an optimal value of Q that maximizes the effective covert rate, which motivates our following optimization of Q in the considered system model.

2) Maximization of R_c with the Covert Constraint: As per (30) and (31), note that $\omega_1 \le 1/2$, the covert constraint is given by

$$\xi^* \ge \min\{1-\omega, \omega\} - \epsilon = \omega_1 - \epsilon. \tag{45}$$

Following Theorem 2, the optimal value of Q that maximizes R_c subject to the covert constraint $\xi^* \ge \omega_1 - \epsilon$ can be obtained through numerical search, which is given by

$$\begin{aligned} Q^* = &\operatorname*{argmax}_Q R_c, \\ &\text{s.t.} \quad \xi^* \ge \omega_1 - \epsilon. \end{aligned} \tag{46}$$

We note that the optimization problem (46) is of one dimension, which can be solved by efficient numerical search. The maximum value of R_c is then achieved by substituting Q^* into (44), which is denoted by R_c^*.

IV. Power-Control Transmission Scheme

In this section, we consider the power-control transmission scheme, in which R transmits a covert message to D with a constant transmit power if possible. Specifically, we first determine R's transmit power in $\mathcal{H}_1$ and then analyze the detection error probability at S, based on which we also derive S's optimal detection threshold. Furthermore, we derive the effective covert rate achieved by the power-control transmission scheme.

A. Transmit Power at Relay

Following (9), when $C_{sd} = R_{sd}$ we have

$$P_r^1 = \mu P_\Delta + \frac{\mu\sigma_d^2}{|h_{rd}|^2}. \tag{47}$$

We note that $C_{sd} = R_{sd}$ requires $C_{sd}^* \ge R_{sd}$ and thus $|h_{rd}|^2 \ge \mu\sigma_d^2/[P_r^{\max} - (\mu+1)P_\Delta]$. Considering the maximum power constraint at R (i.e., $P_r^1 + P_\Delta \le P_r^{\max}$ under this case), R has to give up the transmission of the covert message (i.e., $P_\Delta = 0$) when $P_r^1 > P_r^{\max} - P_\Delta$ and sets P_r^1 the same as P_r^0 given in (6). This is due to the fact that S knows h_{rs} and it can detect the covert transmission with probability one when the total transmit power of R is greater than $P_r^{\max}$. Then, the transmit power of $\mathbf{x}_r$ under $\mathcal{H}_1$ for the power-control transmission scheme is given by

$$P_r^1 = \begin{cases} \mu P_\Delta + \frac{\mu\sigma_d^2}{|h_{rd}|^2}, & |h_{rd}|^2 \ge \frac{\mu\sigma_d^2}{P_r^{\max} - (\mu+1)P_\Delta}, \\ \frac{\mu\sigma_d^2}{|h_{rd}|^2}, & \frac{\mu\sigma_d^2}{P_r^{\max}} \le |h_{rd}|^2 < \frac{\mu\sigma_d^2}{P_r^{\max} - (\mu+1)P_\Delta}, \\ 0, & |h_{rd}|^2 < \frac{\mu\sigma_d^2}{P_r^{\max}}. \end{cases} \tag{48}$$

As per (48), we note that R also does not transmit a covert message when it cannot support the transmission from S to D (i.e., when $|h_{rd}|^2 < \mu\sigma_d^2/P_r^{\max}$). This is due to the fact that a

transmission outage occurs when $|h_{rd}|^2 < \mu\sigma_d^2/P_r^{\max}$ and R or D would request a retransmission from S, which enables S to detect R's covert transmission with probability one if this covert transmission happened, since R cannot and thus does not forward S's information to D when $|h_{rd}|^2 < \mu\sigma_d^2/P_r^{\max}$. In summary, R could possibly transmit a covert message without being detected only when the condition $|h_{rd}|^2 \geq \mu\sigma_d^2/[P_r^{\max} - (\mu+1)P_\Delta]$ is guaranteed. We again denote this necessary condition for covert communication as $\mathbb{C}$. Noting $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$, the probability that $\mathbb{C}$ is guaranteed is given by

$$\mathcal{P}_C = \exp\left\{-\frac{\mu\sigma_d^2}{P_r^{\max} - (\mu+1)P_\Delta}\right\}. \tag{49}$$

We note that $\mathcal{P}_C$ is a monotonically decreasing function of P_Δ, which indicates that the probability that R can transmit a covert message (without being detected with probability one) decreases as P_Δ increases. Following (47) and noting $P_r^1 + P_\Delta \leq P_r^{\max}$, we have $P_r^{\max} > (\mu+1)P_\Delta$.

B. Detection Error Probability at Source

In this subsection, we derive S's false alarm rate, i.e., $\alpha = \mathcal{P}(\mathcal{D}_1|\mathcal{H}_0)$, and miss detection rate, i.e., $\beta = \mathcal{P}(\mathcal{D}_0|\mathcal{H}_1)$.

Theorem 4: When the condition $\mathbb{B}$ is guaranteed, for a given τ, the false alarm and miss detection rates at S are derived as

$$\alpha = \begin{cases} 1, & \tau < \sigma_s^2, \\ 1 - \mathcal{P}_B^{-1}\kappa_1(\tau), & \sigma_s^2 \leq \tau \leq \rho_1, \\ 0, & \tau > \rho_1, \end{cases} \tag{50}$$

$$\beta = \begin{cases} 0, & \tau < \rho_3, \\ \mathcal{P}_B^{-1}\kappa_3(\tau), & \rho_3 \leq \tau \leq \rho_4, \\ 1, & \tau > \rho_4, \end{cases} \tag{51}$$

where

$$\rho_3 \triangleq (\phi\mu+1)P_\Delta|h_{rs}|^2 + \sigma_s^2,$$
$$\rho_4 \triangleq (P_r^{\max}\phi + (\phi\mu+1)P_\Delta)\,|h_{rs}|^2 + \sigma_s^2,$$
$$\kappa_3(\tau) \triangleq \exp\left\{-\frac{\phi\mu\sigma_d^2|h_{rs}|^2}{\tau - \rho_3}\right\},$$

and ρ_1 and $\kappa_1(\tau)$ are defined in (24).

Proof: Considering the maximum power constraint at R under $\mathcal{H}_0$ (i.e., $P_r^0 \leq P_r^{\max}$) and following (6), (16), and (17), the false alarm rate under the condition $\mathbb{B}$ is given by

$$\alpha = \mathcal{P}\left[\frac{\mu\sigma_d^2}{|h_{rd}|^2}|h_{rs}|^2\phi + \sigma_s^2 \geq \tau \middle| \mathbb{B}\right]$$
$$= \begin{cases} 1, & \tau < \sigma_s^2, \\ \mathcal{P}\left[\frac{\mu\sigma_d^2}{P_r^{\max}} \leq |h_{rd}|^2 \leq \frac{\mu\sigma_d^2|h_{rs}|^2\phi}{\tau - \sigma_s^2}\right]\mathcal{P}_B^{-1}, & \sigma_s^2 \leq \tau \leq \rho_1, \\ 0, & \tau > \rho_1. \end{cases} \tag{52}$$

Then, substituting $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$ into the above equation we achieve the desired result in (50).

We first clarify that we have $\rho_3 < \rho_4$. Then, considering the maximum power constraint at R under $\mathcal{H}_1$ (i.e., $P_r^1 + P_\Delta \leq P_r^{\max}$) and following, (16), (17), and (48), the miss detection rate under the condition $\mathbb{B}$ is given by

$$\beta = \mathcal{P}\left[\left(\mu P_\Delta + \frac{\mu\sigma_d^2}{|h_{rd}|^2}\right)|h_{rs}|^2\phi + P_\Delta|h_{rs}|^2 + \sigma_s^2 < \tau \middle| \mathbb{B}\right]$$
$$= \begin{cases} 0, & \tau < \rho_3, \\ \mathcal{P}\left[|h_{rd}|^2 \geq \frac{\phi\mu\sigma_d^2|h_{rs}|^2}{\tau - (\phi\mu+1)P_\Delta|h_{rs}|^2 - \sigma_s^2}\right]\mathcal{P}_B^{-1}, & \rho_3 \leq \tau \leq \rho_4, \\ 1, & \tau > \rho_4. \end{cases} \tag{53}$$

Then, substituting $F_{|h_{rd}|^2}(x) = 1 - e^{-x}$ into the above equation we achieve the desired result in (51). ∎

We note that the false alarm and miss detection rates given in Theorem 4 are functions of the threshold τ and we examine how S sets the value of τ to minimize its detection error probability in the following subsection.

C. Optimization of the Detection Threshold at Source

In this subsection, we first derive a constraint (i.e., an upper bound) on P_Δ to ensure a non-zero detection error probability at S. Then, under this constraint we derive the lower and upper bounds on the optimal value of τ that minimizes the detection error probability ξ for the power-control transmission scheme.

Theorem 5: R's transmit power of the covert message P_Δ should satisfy

$$P_\Delta \leq P_\Delta^u \triangleq \frac{\phi P_r^{\max}}{\phi\mu + 1} \tag{54}$$

in order to guarantee $\xi > 0$ and when (54) is guaranteed the optimal τ at S that minimizes ξ should satisfy $\rho_3 \leq \tau^* \leq \rho_1$.

Proof: As discussed before, S will perform detection whenever condition $\mathbb{B}$ is met. In our work, we assume that R will transmit a covert message with probability 50% when $\mathbb{C}$ is guaranteed. As per (7) and (49), the probability $\mathcal{P}(\mathcal{H}_1)$ is given by

$$\mathcal{P}(\mathcal{H}_1) = \frac{1}{2}\mathcal{P}(\mathbb{C}|\mathbb{B}) = \omega_2, \tag{55}$$

where

$$\omega_2 \triangleq \frac{1}{2}\exp\left\{-\frac{\mu(\mu+1)\sigma_d^2 P_\Delta}{(P_r^{\max}\,(P_r^{\max} - (\mu+1)P_\Delta))}\right\}. \tag{56}$$

Then, $\mathcal{P}(\mathcal{H}_0)$ is given by

$$\mathcal{P}(\mathcal{H}_0) = 1 - \mathcal{P}(\mathcal{H}_1) = 1 - \omega_2. \tag{57}$$

When $\rho_1 < \rho_3$ that requires $P_\Delta > \phi P_r^{\max}/(\phi\mu+1)$ as per Theorem 4, following (50) and (51), we have

$$\xi = \begin{cases} 1 - \omega_2, & \tau \leq \sigma_s^2, \\ (1-\omega_2)\left(1 - \mathcal{P}_B^{-1}\kappa_1(\tau)\right), & \sigma_s^2 < \tau < \rho_1, \\ 0, & \rho_1 \leq \tau \leq \rho_3, \\ \omega_2\mathcal{P}_B^{-1}\kappa_3(\tau), & \rho_3 < \tau < \rho_4, \\ \omega_2, & \tau \geq \rho_4. \end{cases} \tag{58}$$

This indicates that S can simply set $\tau \in [\rho_1, \rho_3]$ to ensure $\xi = 0$ when $P_\Delta > \phi P_r^{\max}/(\phi\mu+1)$, i.e., S can detect the covert transmission with probability one. As such, P_Δ should satisfy (54) in order to guarantee $\xi > 0$.

We next prove $\rho_3 \leq \tau^* \leq \rho_1$. When $P_\Delta \leq \phi P_r^{\max}/(\phi\mu+1)$, i.e., $\rho_3 < \rho_1$, following (50) and (51), we have

$$\xi = \begin{cases} 1-\omega_2, & \tau \leq \sigma_s^2, \\ (1-\omega_2)\left(1-\mathcal{P}_B^{-1}\kappa_1(\tau)\right), & \sigma_s^2 < \tau \leq \rho_3, \\ 1-\omega_2-\mathcal{P}_B^{-1}\times & \\ \left[(1-\omega_2)\kappa_1(\tau)-\omega_2\kappa_3(\tau)\right], & \rho_3 < \tau < \rho_1, \\ \omega_2\mathcal{P}_B^{-1}\kappa_3(\tau), & \rho_1 \leq \tau < \rho_4, \\ \omega_2, & \tau \geq \rho_4. \end{cases} \tag{59}$$

Obviously, S will not set $\tau \leq \sigma_s^2$ or $\tau \geq \rho_4$, since $\xi = 1-\omega_1$ or ω_1 are the worst case for S.

For $\sigma_s^2 < \tau \leq \rho_3$, we derive the first derivative of ξ with respect to τ as

$$\frac{\partial(\xi)}{\partial\tau} = -\frac{(1-\omega_2)\mathcal{P}_B^{-1}\phi\mu\sigma_d^2|h_{rs}|^2}{(\tau-\sigma_s^2)^2}\kappa_1(\tau) < 0. \tag{60}$$

This demonstrates that ξ is a decreasing function of τ when $\sigma_s^2 < \tau \leq \rho_3$. For $\rho_1 \leq \tau < \rho_4$, we derive the first derivative of ξ with respect to τ as

$$\frac{\partial(\xi)}{\partial\tau} = \frac{\omega_2\mathcal{P}_B^{-1}\phi\mu\sigma_d^2|h_{rs}|^2}{(\tau-\rho_3)^2}\kappa_3(\tau) > 0. \tag{61}$$

This proves that ξ is an increasing function of τ when $\rho_1 \leq \tau < \rho_4$. Noting that ξ is a continuous function of τ and considering (60) and (61), we can conclude that τ^* should satisfy $\rho_3 \leq \tau^* \leq \rho_1$, no mater what is the value of ξ for $\rho_3 < \tau < \rho_1$. ∎

The lower and upper bounds on τ^* given in Theorem 5 significantly facilitate the numerical search for τ^* at S. Then, following Theorem 5 and (59), τ^* can be obtained through

$$\tau^* = \underset{\rho_3\leq\tau\leq\rho_1}{\operatorname{argmin}} \left\{1-\omega_2-\mathcal{P}_B^{-1}\left[(1-\omega_2)\kappa_1(\tau)-\omega_2\kappa_3(\tau)\right]\right\}. \tag{62}$$

Substituting τ^* into (59), we can obtain the minimum detection error probability ξ^* for the power-control transmission scheme.

D. Optimization of Effective Covert Rate

In this section, we examine the effective covert rate achieved by the power-control transmission scheme subject to the covert constraint.

1) Effective Covert Rate: Following (11), the SINR at destination for covert communication is given as

$$\begin{aligned}\gamma_\Delta &= \frac{P_\Delta|h_{rd}|^2}{P_r^1|h_{rd}|^2G^2\sigma_r^2+\sigma_d^2} \\ &= \frac{P_\Delta(\eta|h_{sr}|^2+1)|h_{rd}|^2}{\mu P_\Delta|h_{rd}|^2+(\eta|h_{sr}|^2+\mu+1)\sigma_d^2}.\end{aligned} \tag{63}$$

Then, the covert rate achieved by R is $R_\Delta = \log_2(1+\gamma_\Delta)$. We next derive the effective covert rate, i.e., averaged R_Δ over all realizations of $|h_{rd}|^2$, in the following theorem.

***Theorem** 6:* The achievable effective covert rate R_c by R with the power-control transmission scheme is derived as a function of P_Δ given by

$$\begin{aligned}R_c = &\frac{1}{\ln 2}\exp\left\{-\frac{\mu\sigma_d^2}{P_r^{\max}-(\mu+1)P_\Delta}\right\}\times \\ &\left[\ln\left(\frac{\beta_1}{\beta_2}\right)+e^{\frac{\beta_2}{\alpha_2}}\mathbf{Ei}\left(-\frac{\beta_2}{\alpha_2}\right)-e^{\frac{\beta_1}{\alpha_1}}\mathbf{Ei}\left(-\frac{\beta_1}{\alpha_1}\right)\right],\end{aligned} \tag{64}$$

where

$$\begin{aligned}\beta_1 &\triangleq [\eta|h_{sr}|^2+\mu+1](P_r^{\max}-P_\Delta)\sigma_d^2, \\ \beta_2 &\triangleq \left\{\frac{\eta|h_{sr}|^2+\mu+1}{[P_r^{\max}-(\mu+1)P_\Delta]^{-1}}+\mu^2P_\Delta\right\}\sigma_d^2, \\ \alpha_1 &\triangleq P_\Delta\left[\eta|h_{sr}|^2+(\mu+1)\right]\left[P_r^{\max}-(\mu+1)P_\Delta\right], \\ \alpha_2 &\triangleq \mu P_\Delta[P_r^{\max}-(\mu+1)P_\Delta],\end{aligned}$$

and the exponential integral function $\mathbf{Ei}(\cdot)$ is given by

$$\mathbf{Ei}(x) = -\int_{-x}^{\infty}\frac{e^{-t}}{t}dt, \quad [x<0]. \tag{65}$$

Proof: A positive covert rate is only achievable under the condition $\mathbb{C}$ and thus R_c is given by

$$\begin{aligned}R_c &= \int_{\frac{\mu\sigma_d^2}{P_r^{\max}-(\mu+1)P_\Delta}}^{\infty} R_\Delta f(|h_{rd}|^2)d|h_{rd}|^2 \\ &\overset{a}{=} \frac{1}{\ln 2}\exp\left\{-\frac{\mu\sigma_d^2}{P_r^{\max}-(\mu+1)P_\Delta}\right\}\times \\ &\quad\int_0^\infty \ln\left(\frac{\beta_1+\alpha_1 x}{\beta_2+\alpha_2 x}\right)e^{-x}dx,\end{aligned} \tag{66}$$

where $\overset{a}{=}$ is achieved by setting $x = |h_{rd}|^2 - \mu\sigma_d^2/[P_r^{\max}-(\mu+1)P_\Delta]$. We then solve the integral in (66) with the aid of [32, Eq. (4.337.1)]

$$\int_0^\infty e^{-\nu x}\ln(\theta+x)dx = \frac{1}{\nu}\left[\ln\theta+e^{\nu\theta}\mathbf{Ei}(-\theta\nu)\right], \tag{67}$$

and achieve the result given in (64). ∎

Based on Theorem 6, we note that R_c is not an increasing function of P_Δ, since as P_Δ increases R_Δ increases but $\mathcal{P}_C$ (i.e., the probability that the condition $\mathbb{C}$ is guaranteed) decreases. This motivates our following optimization of P_Δ in order to maximize the effective covert rate subject to the covert constraint.

2) Maximization of R_c with the Covert Constraint: As per (55) and (57), note that $\omega_2 \leq 1/2$, the covert constraint is given by

$$\xi^* \geq \min\{1-\omega,\omega\}-\epsilon = \omega_2-\epsilon. \tag{68}$$

Following Theorem 5 the optimal value of P_Δ that maximizes R_c subject to this constraint can be obtained through

$$\begin{aligned}P_\Delta^* = &\underset{0\leq P_\Delta\leq P_\Delta^u}{\operatorname{argmax}} R_c \\ &\text{s.t.} \quad \xi^* \geq \omega_2-\epsilon.\end{aligned} \tag{69}$$

We note that this is a two-dimensional optimization problem that can be solved by efficient numerical searches. Specifically, for each given P_Δ, ξ^* should be obtained based on (62) where τ^* is also numerically searched. We note that the numerical search of P_Δ^* and τ^* is efficient since their lower and upper bounds are explicitly given. The maximum value of R_c is denoted by R_c^*.

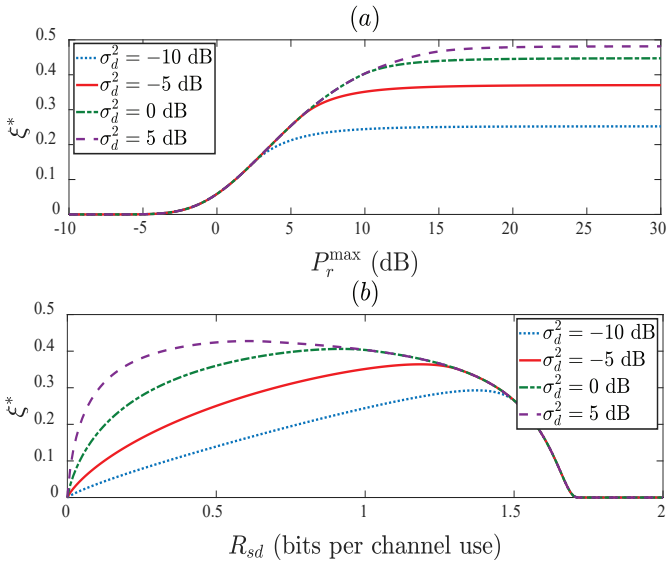


Fig. 2. (a) ξ^* versus $P_r^{\max}$ with different value of σ_d^2 for the rate-control transmission scheme, where $P_s = 10$ dB, $\sigma_r^2 = 0$ dB, $R_{sd} = 1$ bits per channel use, $|h_{sr}|^2 = |h_{rs}|^2 = 1$, and $Q = 0.1$. (b) ξ^* versus R_{sd} with different value of σ_d^2 for the rate-control transmission scheme, where $P_s = P_r^{\max} = 10$ dB, $\sigma_r^2 = 0$ dB, $|h_{sr}|^2 = |h_{rs}|^2 = 1$, and $Q = 0.1$.

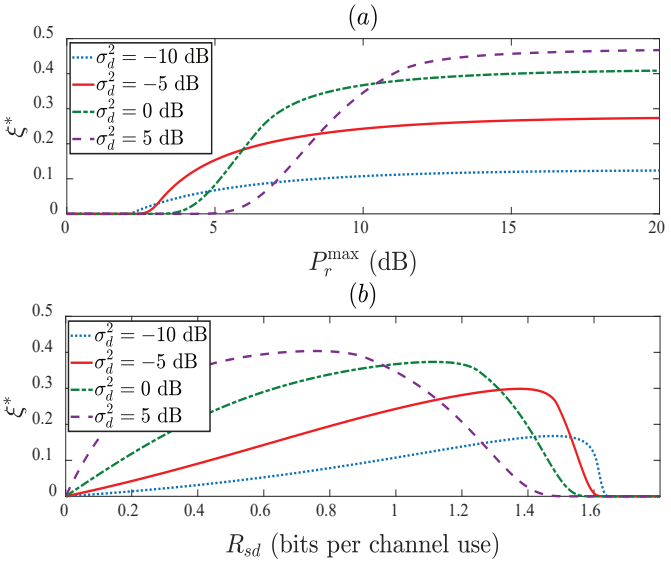


Fig. 3. (a) ξ^* versus $P_r^{\max}$ with different value of σ_d^2 for the power-control transmission scheme, where $P_s = 10$ dB, $\sigma_r^2 = 0$ dB, $R_{sd} = 1$ bits per channel use, $|h_{sr}|^2 = |h_{rs}|^2 = 1$, and $P_\Delta = -10$ dB. (b) ξ^* versus R_{sd} with different value of σ_d^2 for the power-control transmission scheme, where $P_s = P_r^{\max} = 10$ dB, $\sigma_r^2 = 0$ dB, $|h_{sr}|^2 = |h_{rs}|^2 = 1$, and $P_\Delta = -10$ dB.

V. Numerical Results

In this section, we first present numerical results to verify our analysis on the performance of covert communications in relay networks. Then, we provide a thorough performance comparison between the rate-control and power-control transmission schemes. Based on our examination, we draw many useful insights with regard to the impact of some system parameters (e.g., $P_r^{\max}$, R_{sd}, and ϵ) on covert communications in wireless relay networks.

A. Rate-Control Transmission Scheme

In Fig. 2 (a), we plot the minimum detection error probability ξ^* versus R's maximum transmit power $P_r^{\max}$ and observe that ξ^* increases with $P_r^{\max}$. This shows that the covert transmission becomes easier as the desired performance of the normal transmission increases, since the transmission outage probability decreases with $P_r^{\max}$ for a fixed R_{sd}. We also observe ξ^* approach to a specific value as $P_r^{\max} \to \infty$, which is discussed in Remark 2. This observation demonstrates that the covert transmission can still be possibly detected by S even without the maximum power constraint at R. In Fig. 2 (b), we plot ξ^* versus the transmission rate from S to D (i.e., R_{sd}). We first observe that ξ^* is not a monotonic function of R_{sd} and $\xi^* \to 0$ as $R_{sd} \to 0$ or $R_{sd} \to \infty$. This observation indicates that there may exist an optimal value of R_{sd} that maximizes ξ^*. In Fig. 2, we finally observe that ξ^* is a monotonic increasing function of σ_d^2.

B. Power-Control Transmission Scheme

In Fig. 3 (a), we plot the minimum detection error probability ξ^* versus R's maximum transmit power $P_r^{\max}$ and observe that ξ^* increases with $P_r^{\max}$. This shows that the covert transmission becomes easier as the desired performance of the normal transmission increases, since the transmission outage probability decreases with $P_r^{\max}$ for a fixed R_{sd}. We also observe ξ^* does not approach 1/2 (but a specific value that is lower than 1/2) as $P_r^{\max} \to \infty$, which is the same as the result discussed in Remark 2 for the rate-control transmission scheme. This observation demonstrates that the covert transmission can still be possibly detected by S even without the maximum power constraint at R. Fig. 3 (b), we plot ξ^* versus the transmission rate from S to D (i.e., R_{sd}). We first observe that ξ^* is not a monotonic function of R_{sd} and $\xi^* \to 0$ as $R_{sd} \to 0$ or $R_{sd} \to \infty$. This observation indicates that there may exist an optimal value of R_{sd} that maximizes ξ^*. In Fig. 3, we finally observe that ξ^* is not a monotonic function of σ_d^2.

C. Performance Comparisons between the Rate-Control and Power-Control Transmission Schemes

Fig. 4 illustrates R_c^* versus $P_r^{\max}$ with different values of P_s for the rate-control and power-control transmission schemes using (46) and (69), respectively. In this figure, we first observe that for both schemes R_c^* monotonically increases as $P_r^{\max}$ increases, which demonstrates that the covert message becomes easier to be transmitted when more power is available at R. we also observe that R_c^* is not a monotonic function of P_s. In Fig. 4, it illustrates that the power-control transmission scheme outperforms the rate-control transmission scheme when $P_r^{\max}$ is in the low regime. However, when $P_r^{\max}$ is larger than some specific values (e.g., when $P_r^{\max} \geq 13$ dB), the performance of rate-control transmission scheme is better than that of the power-control transmission scheme. This is mainly due to the fact that the transmit power constraints are not limits of

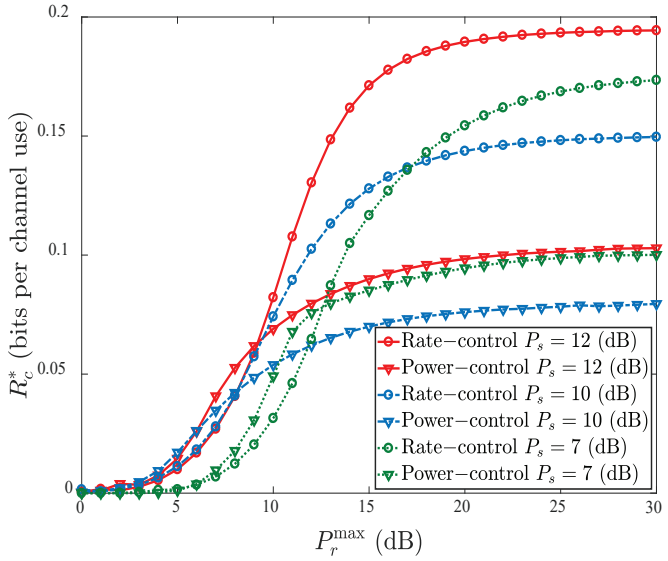


Fig. 4. R_c^* versus $P_r^{\max}$ under different value of P_s, where $\sigma_r^2 = \sigma_d^2 = 0$ dB, $\epsilon = 0.1$, $R_{sd} = 1$ bits per channel use, and $|h_{sr}|^2 = 1$.

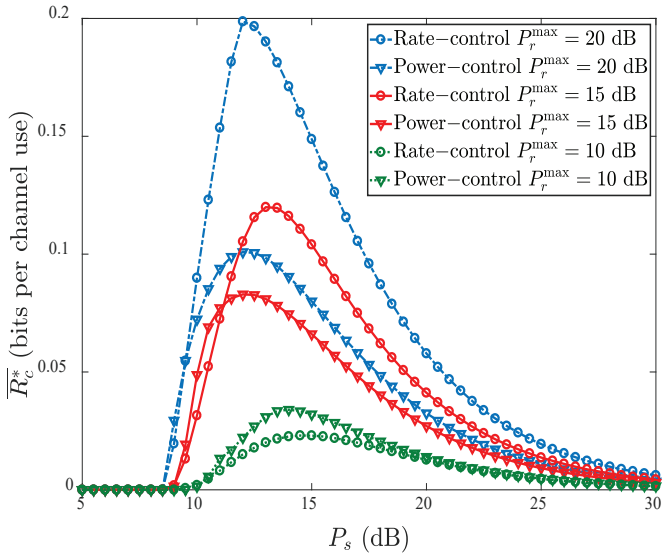


Fig. 5. $\overline{R_c^*}$ versus P_s under different value of $P_r^{\max}$, where $\sigma_r^2 = \sigma_d^2 = 0$ dB, $\epsilon = 0.1$, and $R_{sd} = 1.5$ bits per channel use.

the covert transmission when $P_r^{\max}$ is large, and thus under this case selecting a proper covert transmission rate (in the rate-control transmission scheme) can gain more benefit. We note that this observation demonstrates the significance of our work, since with our analysis R can easily determine which transmission is better under the specific system settings.

In Fig. 5, we plot the averaged maximum effective covert rate, i.e., $\overline{R_c^*}$, which is achieved by averaging R_c^* over $|h_{sr}|^2$, versus S's transmit power P_s with different values of R's maximum transmit power $P_r^{\max}$. In this figure, we first observe that $\overline{R_c^*}$ is zero when P_s is effectively small (e.g., due to the fact that S is far from R and D). This is due to the fact that when P_s is sufficient small, the normal transmission from S to D with the fixed rate R_{sd} may not be supported and R does not forward S's information to D. Meanwhile, the covert transmission from R to D cannot be achieved due to the lack of the shield from the normal transmission. We also observe that $\overline{R_c^*} \to 0$ when $P_s \to \infty$. This is due to the fact that ϕ given in (17) decreases (and thus $P_r^0|h_{rs}|^2\phi$ and $P_r^1|h_{rs}|^2\phi$ decrease) with P_s, which leads to a lower detection error probability at S as per (35) and (62) (i.e., it becomes easier for S to detect the covert transmission). In Fig. 5, we further observe that the achieved $\overline{R_c^*}$ decreases significantly as $P_r^{\max}$ decreases (e.g., when R is with less transmit power than S), which demonstrates that it is the power constraint at R that mainly limits the performance of the covert transmission. Based on this observation, we can predict that $\overline{R_c^*} \to 0$ when $P_r^{\max} \to 0$. This is due to the fact that as $P_r^{\max} \to 0$ R cannot support the normal transmission from S to D, not to mention the covert transmission from itself to D (due to the lack of the shield). Finally, we observe that the power-control transmission scheme outperforms the rate-control transmission scheme when P_s or $P_r^{\max}$ is low. This observation is consistent with that found in Fig. 4.

VI. Conclusion

This work examined covert communication in one-way relay networks over quasi-static Rayleigh fading channels, in which R opportunistically transmits its own information to the destination covertly on top of forwarding S's message in AF mode, while S tries to detect this covert transmission. Specifically, we proposed the rate-control and power-control transmission schemes for R to convey covert information to D. We analyzed S's detection limits of the covert transmission from R to D in terms of the detection error probability and determined the achievable effective covert rates subject to $\xi^* \geq \min\{1-\omega, \omega\} - \epsilon$ for these two schemes. Our examination showed that the rate-control transmission scheme outperforms the power-control transmission scheme under some specific conditions, and otherwise the power-control transmission scheme outperforms the rate-control transmission scheme. As such, our conducted analysis enabled R to switch between these two strategies to achieve the maximum covert rate. Our investigation also demonstrated that covert communication in the considered relay networks is feasible and the effective covert rate achieved by R increases with its forwarding ability.

References

[1] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," in *Proc. IEEE GLOBECOM*, Dec. 2017, pp. 1–6.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[3] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[4] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[6] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction*. Cambridge University Press, 2006.

[7] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

[8] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Aritificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.

[9] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[10] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, Jan. 2017.

[11] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[12] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[13] P. H. Che, S. Kadhe, M. Bakshi, C. Chan, S. Jaggi, and A. Sprintson, "Reliable, deniable and hidable communication: A quick survey," in *Proc. IEEE Inf. Theory Workshop*, Nov. 2014, pp. 227–231.

[14] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

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

[16] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, 1st ed. McGraw-Hill, 1994.

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

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

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

[20] A. Abdelaziz and C. E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel," *arXiv preprint*, pp. 1–20, May 2017, arXiv:1705.02303v3.

[21] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. T. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[22] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, Apr. 2017.

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

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

[25] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *Proc. IEEE VTC Spring*, Jun. 2017, pp. 1–5.

[26] S. Yan, B. He, Y. Cong, and X. Zhou, "Covert communication with finite blocklength in AWGN channels," in *Proc. IEEE ICC*, May 2017, pp. 1–6.

[27] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 99, no. 3, pp. 32–44, May 2003.

[28] T. Cui and C. Tellambura, "Power delay profile and noise variance estimation for OFDM," *IEEE Commun. Lett.*, vol. 10, no. 1, pp. 25–27, Apr. 2006.

[29] M. Molu and N. Goertz, "An analytical approach to the outage probability of amplify-and-forward relaying with an MRC receiver," in *Proc. IEEE VTC Spring*, Jun. 2013, pp. 1–5.

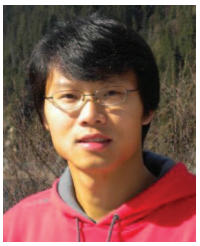
[30] Y. Deng, K. J. Kim, T. Q. Duong, M. Elkashlan, G. K. Karagiannidis, and A. Nallanathan, "Full-duplex spectrum sharing in cooperative single carrier systems," *IEEE Trans. Cogn. Commun. and Netw.*, vol. 2, no. 1, pp. 68–82, Mar. 2016.

[31] M. H. DeGroot, *Probability and Statistics*, 4th ed. Pearson, 2011.

[32] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.

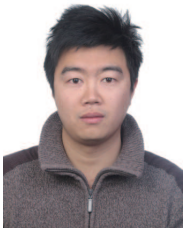
Jinsong Hu received the B.S. degree from the Nanjing University of Science and Technology, Nanjing, China, in 2013. He is currently pursuing the Ph.D. degree with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. He is also a Visiting Ph.D. Student with the Australian National University from 2017 to 2018. His research interests include array signal processing, covert communications, and physical layer security.

Shihao Yan (S'11-M'15) received the Ph.D degree in Electrical Engineering from The University of New South Wales, Sydney, Australia, in 2015. He received the B.S. in Communication Engineering and the M.S. in Communication and Information Systems from Shandong University, Jinan, China, in 2009 and 2012, respectively. From 2015 to 2017, he was a Postdoctoral Research Fellow in the Research School of Engineering, The Australia National University, Canberra, Australia. He is currently a University Research Fellow in the School of Engineering, Macquarie University, Sydney, Australia. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, covert communications, and location spoofing detection.



Xiangyun Zhou (SM'17) is a Senior Lecturer at the Australian National University (ANU). He received the Ph.D. degree from ANU in 2010. His research interests are in the fields of communication theory and wireless networks. He has been serving as an Editor for various IEEE journals, including IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS LETTERS and IEEE COMMUNICATIONS LETTERS. He served as a guest editor for IEEE COMMUNICATIONS MAGAZINE's feature topic on wireless physical layer security in 2015. He also served as symposium/track and workshop co-chairs for major IEEE conferences. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC'11 and IEEE ComSoc Asia-Pacific Outstanding Paper Award in 2016. He was named the Best Young Researcher in the Asia-Pacific Region in 2017 by IEEE ComSoc Asia-Pacific Board.

Feng Shu was born in 1973. He received the Ph.D., M.S., and B.S. degrees from the Southeast University, Nanjing, in 2002, XiDian University, Xian, China, in 1997, and Fuyang teaching College, Fuyang, China, in 1994, respectively. From Sept. 2009 to Sept. 2010, he is a visiting post-doctor at the University of Texas at Dallas. In October 2005, he joined the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China, where he is currently a Professor and supervisor of Ph.D and graduate students. He is also with Fujian Agriculture and Forestry University and awarded with Mingjian Scholar Chair Professor in Fujian Province. His research interests include wireless networks, wireless location, and array signal processing. He has published about 200 papers, of which more than 100 are in archival journals including more than 40 papers on IEEE Journals and more than 70 SCI-indexed papers. He holds six Chinese patents.



Jun Li (M'09-SM'16) received the Ph.D. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2009. From January 2009 to June 2009, he was with the Department of Research and Innovation, Alcatel Lucent Shanghai Bell, as a Research Scientist. Since 2015, he is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. His research interests include network information theory, channel coding theory, wireless network coding, and cooperative communications.

Jiangzhou Wang (F'17) is currently Head of the School of Engineering and Digital Arts and a Professor at the University of Kent, United Kingdom. He has authored over 300 papers in international journals and conferences in the areas of wireless mobile communications and three books. He is an IEEE Fellow and IET Fellow. He received the Best Paper Award from IEEE GLOBECOM2012 and was an IEEE Distinguished Lecturer from 2013 to 2014. He is the Technical Program Chair of IEEE ICC2019 in Shanghai. He was the Executive Chair of IEEE ICC2015 in London and the Technical Program Chair of IEEE WCNC2013. He was an Editor for IEEE Transactions on Communications from 1998 to 2013 and was a Guest Editor for IEEE Journal on Selected Areas in Communications, IEEE Communications Magazine, and IEEE Wireless Communications. His research interests include massive MIMO, Cloud RAN, NOMA, D2D, and secure communications.