# Covert and Secure Transmissions for IRS-Enabled Wireless Communication Systems

Yihuai Yang, Bin Yang, Shikai Shen, Yumei She, Xiaohong Jiang and Tarik Taleb

***Abstract*—This paper explores the covert and secure transmissions in an intelligent reflecting surface (IRS)-enabled wireless communication system. With the help of an IRS, a transmitter (Lisa) attempts to conduct secure transmission with a receiver (Tony) against an eavesdropper intercepting the transmission content and also simultaneously conducts covert transmission with another receiver (John) against a warden detecting the transmission process. To achieve this goal, Lisa selectively transmits covert signals in random time slots to prevent the warden's detection while also continuously transmitting secure signals in all time slots. We first derive the detection performance at the warden under the underlay and overlay modes, respectively. Both secure and covert transmissions use the same spectrum resource under the underlay mode, while they use orthogonal spectrum resources under the overlay mode. We then model the covert and secrecy rate performances under these two modes. For each mode, we formulate an optimization problem that jointly optimizes covert transmit power, total transmit power at Lisa, and IRS reflect beamforming to achieve covert rate maximization while satisfying covertness and secrecy requirements. We also propose a hybrid mode under which Lisa can flexibly switch between the underlay and overlay modes to further improve covert rate performance with secrecy rate constraint. We present numerical results to explore how some key parameters affect the covert rate performance and also to reveal our findings.**

This work is supported in part by the National Natural Science Foundation of China under Grant 62372076, in part by the Joint Fund for Basic Research of Local Universities in Yunnan Province under Grant 202401BA070001-109, in part by the Yunnan Key Laboratory of Cross-border Digital Economy under Grant 2025RD4916CE340007, in part by the Education Department Research Foundation of Anhui Province under Grant DTR2023051, in part by the Innovation Research Team on Future Network Technology of Chuzhou University, in part by the Innovation Team on Smart Home Appliance Security and Applications of Chuzhou City, in part by the Innovative Research Team on Application of Big Data and Financial Technology of Chuzhou University, in part by the Federal Ministry of Research, Technology, and Space (BMFTR), Germany, through the Project 6GEM+ under Grant 16KIS2411, in part by the European Union's Horizon Europe research and innovation programme under the 6G-Path project under Grant 101139172, and in part by the Yunnan Provincial Major Science and Technology Special Program under Grant 202602AC080004. *(Corresponding author: Bin Yang; Shikai Shen).*

Yihuai Yang is with the School of Information Engineering, Kunming University, Kunming 650214, China (e-mail: Yihuai_Yang@126.com).

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

Shikai Shen is with the School of Electronic Information and Automation, Dianchi College, Kunming 650228, China, the School of Information Engineering, Kunming University, Kunming 650214, China, and also with the Yunnan Key Laboratory of Intelligent Logistics Equipment and Systems, Kunming 650214, China(e-mail: kmssk2000@sina.com).

Yumei She is with the School of Mathematics and Computer Science, Yunnan Minzu University, Kunming 650500, China (e-mail: sheym1965@126.com).

Xiaohong Jiang is with the School of Systems Information Science, Future University, Hakodate 041-8655, Japan (e-mail: jiang@fun.ac.jp).

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

***Keywords*-Intelligent reflecting surface (IRS), Covert transmission, Secure transmission, Internet of Things.**

## I. Introduction

In the last decade, wireless communication systems (WCSs) have experienced an unprecedented proliferation of mobile devices and a sharp rise of emerging Internet of things (IoT) applications, such as intelligent reflecting surface (IRS)-assisted communication, covert transmission, and edge computing with unmanned aerial vehicles (UAVs) [1]–[4]. Due to the inherent broadcast nature of wireless signals, WCSs are vulnerable to information leakage. Conventional cryptographic techniques typically require considerable computational complexity and energy consumption, which may not be suitable for resource-constrained IoT devices. Recently, physical layer security (PLS) has emerged as a promising paradigm that exploits channel randomness to enhance transmission security [5]–[9].

PLS techniques can be broadly categorized into secure transmission and covert transmission [10], [11]. Secure transmission aims to protect confidential information from eavesdropping, whereas covert transmission conceals the very existence of communication activities. Extensive studies have investigated secure transmissions [12]–[21] and covert transmissions [22]–[37] separately. However, in many practical IoT and mission-critical applications, multiple malicious attacks may coexist. Some adversaries attempt to eavesdrop on transmitted data, while others seek to detect the presence of communication activities. For instance, in military tactical networks, UAV reconnaissance missions, undercover law enforcement operations, emergency response coordination systems, and critical infrastructure monitoring, attackers may not only intercept confidential data but also conduct spectrum monitoring to identify active transmissions. Similarly, in smart grid control networks and industrial IoT systems, traffic detection alone may reveal sensitive system states even without successful decoding. These scenarios indicate that secrecy alone is insufficient if transmissions remain detectable, while covert communication without adequate confidentiality may still result in data leakage.

Such practical considerations naturally motivate the joint design of secure and covert transmission mechanisms, which has recently attracted growing attention [38]–[45]. In these scenarios, sensitive data transmissions are exposed to both interception and traffic analysis attacks, where unauthorized entities may attempt not only to recover the transmitted content but also to infer communication patterns to extract critical system information. Motivated by these practical requirements,

existing works have investigated joint designs in relay-assisted systems, UAV-enabled networks, and cooperative jamming frameworks. However, most of these approaches rely on active relaying, artificial noise generation, cooperative jamming, or UAV trajectory optimization, which may introduce additional power consumption, hardware complexity, and deployment constraints.

Meanwhile, intelligent reflecting surface (IRS) has emerged as a promising technology for reconfiguring the wireless propagation environment in a programmable manner [46]–[48]. By intelligently adjusting the phase shifts of its passive elements, IRS enables passive beamforming to enhance legitimate links and suppress undesired signal leakage without requiring additional transmit power or active radio-frequency chains. In the context of PLS, IRS has been widely investigated to improve secrecy performance by strengthening legitimate channels and degrading eavesdropping links [14], [16], [49], [50]. Moreover, IRS has also been exploited to facilitate covert communications by shaping spatial signal distributions and increasing detection uncertainty at the warden [35]–[37]. Some preliminary efforts have begun to explore joint secure and covert designs in IRS-enabled systems [43], [51]. These results demonstrate the significant potential of IRS in enhancing either confidentiality or transmission stealth individually. However, existing studies typically assume fixed spectrum-access models or specific system configurations. A systematic investigation of joint secure-and-covert transmission design in IRS-enabled systems under multiple spectrum-sharing modes remains lacking. In particular, the impact of underlay, overlay, and adaptive hybrid spectrum-sharing strategies on the secrecy–covertness trade-off has not yet been comprehensively characterized. The main contributions of this study are summarized as follows:

- We consider an IRS-enabled WCS, where with the assistance of an IRS that passively reconfigures the wireless propagation environment, a transmitter attempts to conduct secure transmission with a receiver, and also to conduct covert transmission with another receiver in the presence of both an eavesdropper and a warden. In the WCS, we derive the expressions for the false alarm rate and miss detection rate under the underlay and overlay modes, respectively. We then further derive the optimal detection thresholds for achieving the minimum total detection error rates under these modes.
- Under each mode, we formulate covert rate maximization as an optimization problem subject to the requirements of covertness and secrecy. We further jointly optimize the covert transmit power, total transmit power at Lisa, and IRS reflect beamforming to obtain the maximum covert rate while satisfying secure transmission requirement.
- We further propose a hybrid mode to obtain a better covert rate performance with secrecy rate constraint. Under the mode, the legitimate transmitter can flexibly switch between the underlay and overlay modes.
- We conduct extensive numerical results to explore the impact of some crucial parameters on covert transmission performance while satisfying the requirements for secure transmission under the underlay, overlay and hybrid modes. We also do a performance comparison study between our IRS-aided scenario and no IRS-aided scenario.

The rest of this paper is structured as follows: Section II introduces the system model, while Section III concentrates on examining the detection performance from the warden's perspective. Sections IV, V, and VI delve into covert transmissions under the underlay mode, overlay mode, and hybrid mode, respectively. Section VII provides numerical results, and Section VIII concludes this work.

In this paper, vectors and matrices are denoted by bold lowercase and uppercase letters, respectively. The abbreviations and notations used throughout the paper are summarized in Table I.

TABLE I
ABBREVIATION AND NOTATIONS

| Abbreviation /Notations | Description |
|---|---|
| IRS | Intelligent Reflecting Surface |
| CSI | Channel State Information |
| PN | Pseudo Noise |
| AWGN | Additive White Gaussian Noise |
| SINR | Signal-to-Interference-plus-Noise Ratio |
| SNR | Signal-to-Noise Ratio |
| CVX | Convex Optimization Toolbox |
| NLoS | Non-Line-of-Sight |
| $\mathbf{h_{XY}}$ | Channel vector fading coefficient between nodes $X$ and $Y$ |
| $\mathbf{\Theta}$ | The diagonal phase-shifting matrix of IRS |
| $P$ | The total transmit power limit of Lisa |
| $\varepsilon$ | Covertness requirement |
| $\mathbf{x_s}, \mathbf{x_c}$ | The secure and covert vector signals, respectively |
| $P_s$, $P_c$ | Transmit powers of secure and covert signals, respectively |
| $\sigma_T^2$, $\sigma_J^2$ | Noise variances at Tony and John, respectively |
| $\sigma_E^2$, $\sigma_W^2$ | Noise variances at Eavesdropper and Warden, respectively |
| $R_c^U$, $R_c^O$ | Covert rates under underlay and overlay mode, respectively |
| $R_s^U$, $R_s^O$ | Secrecy rates under underlay and overlay mode, respectively |

## II. SYSTEM MODEL

### A. System Model

As illustrated in Fig. 1, we examine an IRS-enabled wireless communication system with the requirements of simultaneous covert and secure transmissions. The system is composed of a source (Lisa), two authorized users (Tony and John), an IRS, and two unauthorized users (an Eavesdropper and a Warden). Due to fading effects caused by obstacles such as forests or tall buildings, both Tony and John, as well as Warden and Eavesdropper, are unable to receive Lisa's signals directly. They all take advantage of the same IRS in an attempt to obtain their respective useful signals. In this study, Lisa simultaneously sends covert and secure message to both John and Tony. John desires to covertly obtain information without being detected by the Warden, while Tony seeks to securely obtain information without being intercepted by the Eavesdropper. We explore two modes of spectrum resource sharing: underlay and overlay. In the underlay mode, Lisa transmits covert and secure signals over the same frequency

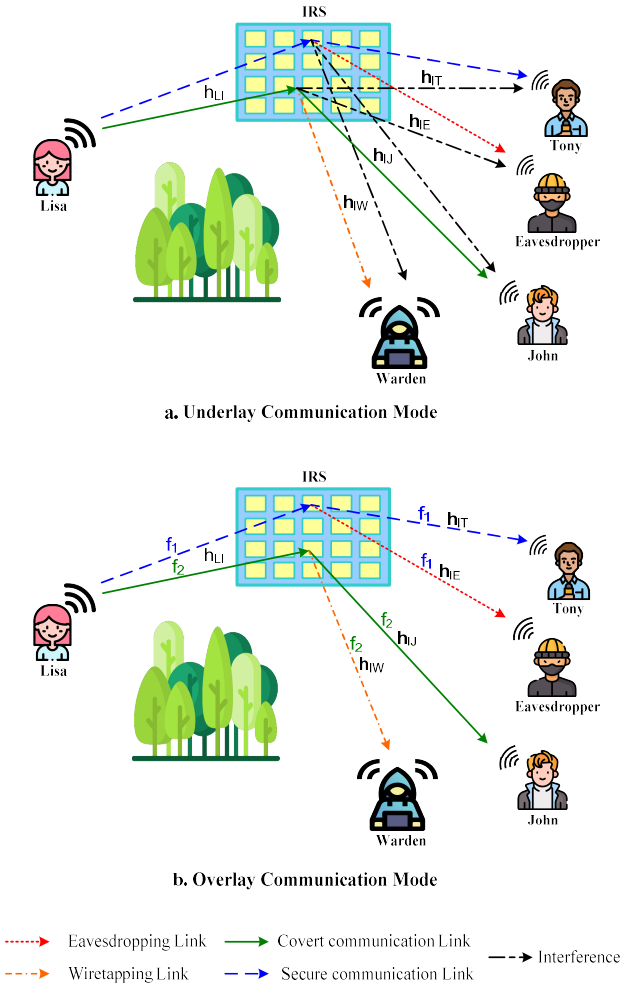


Fig. 1. System Model

band, inevitably causing interference at the receiving nodes, which impacts both legitimate and unauthorized users.

In contrast, the overlay mode employs a more sophisticated strategy. Lisa transmits secure signals to Tony on frequency $f_1$, while simultaneously sending covert signals to John on a separate frequency $f_2$. The considerable separation between $f_1$ and $f_2$ ensures that there is no interference between the covert and secure signals at any of the receiving nodes. Moreover, Lisa can dynamically switch between the overlay and underlay modes by controlling whether the covert and secure signals are transmitted on the same frequency band. In practice, Lisa may employ orthogonal frequency-division multiplexing (OFDM) to implement the overlay strategy, assigning different subcarriers (or sub-bands) to covert and secure transmissions. The orthogonality of OFDM subcarriers helps eliminate mutual interference while enhancing spectral efficiency.

### B. Channel Model

In this work, covert communication is embedded within ongoing secure transmissions. Specifically, the transmitter continuously sends secure signals, while covert signals are superimposed in selected time slots according to a pre-shared random sequence. Thus, the warden's task is to distinguish between "secure transmission only" and "secure transmission with additional covert signaling", i.e., detecting the presence of covert information embedded within ongoing transmissions.

We consider a discrete time-slotted block fading channel, where each time slot (or fading block) spans $L$ symbols. Lisa transmits both a secure signal vector $\mathbf{x_s}$ and a covert signal vector $\mathbf{x_c}$ simultaneously in each time slot, with the assistance of an Intelligent Reflecting Surface (IRS). Each element of $\mathbf{x_s}$ and $\mathbf{x_c}$ is independently drawn from a circularly symmetric complex Gaussian distribution, i.e., $x_s[i], x_c[i] \sim \mathcal{CN}(0,1)$, independently for all $i$.

Lisa transmits $\mathbf{x_s}$ continuously across all slots, while $\mathbf{x_c}$ is transmitted only in selected slots according to a pre-shared Pseudo-Noise (PN) sequence. Let $\mathbf{x_s} = [x_s[1], x_s[2], \ldots, x_s[L]]$ and $\mathbf{x_c} = [x_c[1], x_c[2], \ldots, x_c[L]]$, where $L$ denotes the number of symbols per time slot (or fading block), and we assume $L \to \infty$ for analytical tractability.

Each symbol is subject to a unit power constraint, specifically, $\mathbb{E}[|x_s[i]|^2] = 1$ and $\mathbb{E}[|x_c[i]|^2] = 1$ for all $i \in \{1, 2, \ldots, L\}$, where $\mathbb{E}[\cdot]$ denotes the expectation operator.

The total transmit power is denoted by $P = P_s + P_c$, constrained by $0 < P \leq P_{\max}$, where $P_s$ and $P_c$ represent the transmit powers allocated to the secure and covert transmissions, respectively, and $P_{\max}$ is the maximum allowable transmit power at the transmitter.

We use $L$, $J$, $T$, $E$, $W$, and $I$ to denote Lisa, John, Tony, Eavesdropper, Warden, and IRS, respectively. The channel from node $X$ to node $Y$ is denoted as $\mathbf{h}_{XY}$, where $X, Y \in \{L, J, T, E, W, I\}$. All users are assumed to be slot-synchronized. We adopt a quasi-static Rayleigh fading channel model in which the channel coefficients remain constant within each slot but change independently from one slot to the next. We assume that the eavesdropper behaves as an active but untrusted user participating in the network, which enables the transmitter to estimate its channel state information (CSI) via standard pilot-based methods or long-term channel learning [38], [39]. In addition, its approximate location may be obtained through sensing or network-side information, which can further assist channel estimation. In contrast, the warden is passive and does not transmit any pilots, preventing the transmitter from acquiring its instantaneous CSI. Instead, only approximate location information of the warden is assumed to be available, which may be obtained through long-term observation or deployment knowledge. Such a modeling approach allows tractable analysis of the considered system. In practice, only partial or statistical CSI may be available, which can be incorporated into a robust design framework. This setup corresponds to a conservative design, where the warden is assumed to have full CSI for detection and thus strong detection capability, while the transmitter operates with limited information [35], [52].

### C. IRS Model

We consider an intelligent reflecting surface (IRS) consisting of $N$ passive reflecting elements, which aims to maximize the covert transmission rate for John while satisfying the secrecy rate requirement for Tony.

The IRS reflection matrix is denoted as $\mathbf{\Theta} = \text{diag}\left(q_1 e^{j\theta_1}, q_2 e^{j\theta_2}, \ldots, q_N e^{j\theta_N}\right)$, where $\mathbf{\Theta} \in \mathbb{C}^{N\times N}$ is a diagonal matrix. Here, $\theta_n \in [0, 2\pi)$ and $q_n \in [0, 1]$ denote the phase shift and amplitude reflection coefficient of the $n$-th IRS element, respectively, for $n = 1, 2, \ldots, N$. Each IRS element adjusts the incident signal by applying a complex reflection coefficient $q_n e^{j\theta_n}$, allowing flexible control of the wireless propagation environment.

### *D. Detecting Decision at Warden*

From the Warden's perspective, decisions are made by assessing observations to determine whether communication between Lisa and John is taking place. As a result, Warden utilizes binary hypothesis testing to evaluate the observed data. Under the null hypothesis, $\mathcal{H}_0$, it is assumed that Lisa is not presently transmitting a covert signal. Conversely, the alternative hypothesis, $\mathcal{H}_1$, posits the existence of an ongoing covert transmission.

By assessing the received signal power, the Warden determines whether Lisa transmitted covert information. Denoted as $\mathcal{D}_0$ and $\mathcal{D}_1$, these represent Warden's decisions in favor of $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. Thus, the overall detection error rate at Warden is expressed as

$$\xi = \pi_0 P\left\{\mathcal{D}_1 | \mathcal{H}_0\right\} + \pi_1 P\left\{\mathcal{D}_0 | \mathcal{H}_1\right\}, \tag{1}$$

where, $\pi_0$ and $\pi_1$ are the priori probabilities for the hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. Then, we define the false alarm probability as $P_{FA} = P\{\mathcal{D}_1 | \mathcal{H}_0\}$ and the missed detection probability as $P_{MD} = P\{\mathcal{D}_0 | \mathcal{H}_1\}$. Under the assumption of equal a priori probabilities for the null and alternative hypotheses (i.e., $\pi_0 = \pi_1 = 0.5$), this choice is grounded in the principle of indifference. When there is no prior knowledge or reason to favor one hypothesis over the other, assigning equal probabilities ensures a neutral starting point before observing any data. The total detection error rate, $\xi$, is simplified as:

$$\xi = P_{FA} + P_{MD}, \tag{2}$$

which serves as a measure of covertness.

Given these assumptions, we utilize $y_W^U[i]$ and $y_W^O[i]$ to denote the received signal at Warden for the $i$-th channel use under the underlay and overlay modes, respectively.

*1) Underlay Mode:* As depicted in Fig.1(a), under the underlay mode, the received signal at Warden for the $i$-th channel use is expressed as

$$\mathbf{y}_W^U[i] = \begin{cases} \sqrt{P_s}(\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}})\mathbf{x_s}[i] + \mathbf{n}_W[i], & \mathcal{H}_0 \\ \sqrt{P_s}(\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}})\mathbf{x_s}[i] + \mathbf{n}_W[i] & \\ \quad + \sqrt{P_c}(\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}})\,\mathbf{x_c}[i], & \mathcal{H}_1 \end{cases} \tag{3}$$

where the noise at Warden is denoted as $\mathbf{n}_W \sim \mathcal{CN}(0, \sigma_W^2)$.

The objective of Warden is to discern whether $\mathbf{y}_W^U[i]$ originates from the interference plus noise or if it includes Lisa's signal along with the interference and noise in the interference-limited network. A radiometer is adopted by Warden as the detector, and the received average power of Warden under the underlay mode in a slot is calculated as

$$T^U = \frac{1}{L}\sum_{i=1}^{L}\left|\mathbf{y}_W^U[i]\right|^2. \tag{4}$$

Conditioned on the quasi-static channel realization within each fading block, $\mathbf{y}_W^U[i]$ is a linear combination of independent circularly symmetric complex Gaussian signals and additive Gaussian noise. Hence, it remains circularly symmetric complex Gaussian distributed, and its variance depends on the hypothesis. Accordingly, we have

$$\begin{cases} \mathcal{CN}\left(0, \left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2 P_s + \sigma_W^2\right), & \mathcal{H}_0 \\ \mathcal{CN}\left(0, \left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2 P_c + \left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2 P_s + \sigma_W^2\right), & \mathcal{H}_1 \end{cases} \tag{5}$$

Subsequently, the average signal power at Warden under the underlay mode is determined by

$$T^U = \begin{cases} \left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2 P_s + \sigma_W^2, & \mathcal{H}_0 \\ \left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2 P_c + \left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2 P_s + \sigma_W^2, & \mathcal{H}_1 \end{cases} \tag{6}$$

In the pursuit of minimizing detection errors, Lisa employs the optimal Neyman-Pearson test [53]. The threshold for the average received power in a time slot is specified as

$$T^U \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \gamma^U, \tag{7}$$

where $\gamma^U$ is the chosen threshold under the underlay mode. To optimize Warden's detection performance, Warden will optimize $\gamma^U$ to attain the minimum value of $\xi^U$, denoted as $\xi_U^*$. Consequently, the covertness constraint can be formulated as

$$\xi_U^* \geq 1 - \varepsilon, \quad \varepsilon \geq 0, \tag{8}$$

where, $\varepsilon$ represents the covertness requirement, serving as a very small value to ensure robust covertness and push Warden into the regime of high detection errors.

*2) Overlay Mode:* As illustrated in Fig.1(b), under the overlay mode, the received signal at Warden for the $i$-th channel use is formulated as

$$\mathbf{y}_W^O[i] = \begin{cases} \mathbf{n}_W[i], & \mathcal{H}_0 \\ \sqrt{P_c}(\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}})\,\mathbf{x_c}[i] + \mathbf{n}_W[i], & \mathcal{H}_1 \end{cases} \tag{9}$$

The objective of Warden is to ascertain whether $\mathbf{y}_W^O[i]$ arises solely from Gaussian white noise or if it incorporates Lisa's signal along with the noise. In this mode, the Warden also utilizes a similar radiometer as that used in the underlay mode for detection. Thus, the received average power of Warden under the overlay mode for the $i$-th channel use is determined by

$$T^O = \frac{1}{L}\sum_{i=1}^{L}\left|\mathbf{y}_W^O[i]\right|^2. \tag{10}$$

Given the independent and i.i.d. nature of the received vector $\mathbf{y}_W^O[i]$ at Warden, it conforms to a distribution specified by

$$\begin{cases} \mathcal{CN}\left(0, \sigma_W^2\right), & \mathcal{H}_0 \\ \mathcal{CN}\left(0, |\mathbf{h_{IW}\Theta h_{LI}}|^2 P_c + \sigma_W^2\right). & \mathcal{H}_1 \end{cases} \tag{11}$$

Following this, the average signal power at Warden under the overlay mode is calculated as

$$T^O = \begin{cases} \sigma_W^2, & \mathcal{H}_0 \\ |\mathbf{h_{IW}\Theta h_{LI}}|^2 P_c + \sigma_W^2, & \mathcal{H}_1 \end{cases} \tag{12}$$

Under this mode, Lisa also employs the LRT. The threshold test on the average received power in a slot is expressed as

$$T^O \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \gamma^O, \tag{13}$$

where, $\gamma^O$ is the chosen threshold under the overlay mode.

For optimal enhancement of Warden's detection performance, Warden will carefully select the $\gamma^O$ to achieve the minimum value of $\xi^O$, denoted as $\xi_O^*$. Accordingly, the covertness constraint can be expressed as

$$\xi_O^* \geq 1 - \varepsilon, \quad \varepsilon \geq 0, \tag{14}$$

where $\varepsilon$ is a very small value.

## III. Detection Performance of Warden

In this section, we explore the false alarm rate and miss detection rate at the warden from his perspective under both underlay and overlay modes.

### A. Underlay Mode

**Lemma 1.** *under the underlay mode, the false alarm rate $P_{FA}^U$ and miss detection rate $P_{MD}^U$ at Warden are expressed as follows*

$$P_{FA}^U = \begin{cases} 1, & \gamma^U < \sigma_W^2 \\ \exp\left[\lambda_A \frac{\left(\sigma_W^2 - \gamma^U\right)}{P_s}\right], & \sigma_W^2 \leq \gamma^U \leq \phi_1 \\ 0, & \gamma^U > \phi_1 \end{cases} \tag{15}$$

*and*

$$P_{MD}^U = \begin{cases} 0, & \gamma^U < \phi_1 \\ 1 - \exp\left[\lambda_A \left(\frac{\sigma_W^2 - \gamma^U}{P_c + P_s}\right)\right], & \phi_1 \leq \gamma^U \leq \phi_2 \\ 1, & \gamma^U > \phi_2 \end{cases} \tag{16}$$

*where $\phi_1 = |\mathbf{h_{IW}\Theta h_{LI}}|^2 P_s + \sigma_W^2$,*
*$\phi_2 = |\mathbf{h_{IW}\Theta h_{LI}}|^2 P_c + |\mathbf{h_{IW}\Theta h_{LI}}|^2 P_s + \sigma_W^2$ and $|\mathbf{h_{IW}\Theta h_{LI}}|^2$ follows an exponential distribution with parameter $\lambda_A$.*

### B. Overlay Mode

**Lemma 2.** *under the overlay mode, the false alarm rate $P_{FA}^O$ and miss detection rate $P_{MD}^O$ at Warden are expressed as follows*

$$P_{FA}^O = \begin{cases} 1, & \gamma^O < \sigma_W^2 \\ 0, & \gamma^O \geq \sigma_W^2 \end{cases} \tag{17}$$

*and*

$$P_{MD}^O = \begin{cases} 0, & \gamma^O < \sigma_W^2 \\ 1 - \exp\left[\lambda_A \left(\frac{\sigma_W^2 - \gamma^O}{P_c}\right)\right], & \sigma_W^2 \leq \gamma^O \leq \phi_1 \\ 1. & \gamma^O > \phi_1 \end{cases} \tag{18}$$

## IV. Covert Transmission under Underlay Mode

In this section, under the underlay mode, we first examine the covert transmission requirement and secrecy rate constraint. Next, we derive the transmission outage probability from Lisa to John with the assistance of an IRS. Based on this probability, we calculate the covert rate for John and formulate an optimization problem to maximize his covert rate, and solve it.

### A. Covert transmission Requirement

**Theorem 1.** *We use $\gamma_U^*$ to denote the optimal value of $\gamma^U$ achieving minimum $\xi^U$ of Warden, and then*

$$\gamma_U^* = \phi_1, \tag{19}$$

*where $\phi_1 = |\mathbf{h_{IW}\Theta h_{LI}}|^2 P_s + \sigma_W^2$ and the corresponding minimum detection error rate of Warden is given by*

$$\xi_U^* = \min\left[\exp(\eta), 1 - \exp\left(\frac{\eta}{P_c + P_s}\right)\right], \tag{20}$$

*where $\eta = -\lambda_A |\mathbf{h_{IW}\Theta h_{LI}}|^2$.*

### B. Secrecy Rate Constraint

We assume that Tony is unaware of the PN sequence shared between Lisa and John. So, when Lisa transmits both covert and secrecy signals, the signal received by Tony under the underlay mode is expressed as follows:

$$\begin{aligned} \mathbf{y}_T^U[i] = &\sqrt{P_s}\left(\mathbf{h_{IT}\Theta h_{LI}}\right)\mathbf{x_s}[i] + \\ &\sqrt{P_c}\left(\mathbf{h_{IT}\Theta h_{LI}}\right)\mathbf{x_c}[i] + \mathbf{n_T}[i], \end{aligned} \tag{21}$$

where $\mathbf{n_T}[i]$ represents the additive white Gaussian noise (AWGN) signal received at Tony for the $i$-th channel use, and $\mathbf{n}_T$ follows a complex normal distribution, specifically $\mathbf{n_T}[i] \sim \mathcal{CN}(0, \sigma_T^2)$.

Hence, the Signal-to-Interference-plus-Noise Ratio (SINR) under the underlay mode is given by

$$\Gamma_T^U = \frac{P_s |\mathbf{h_{IT}\Theta h_{LI}}|^2}{P_c |\mathbf{h_{IT}\Theta h_{LI}}|^2 + \sigma_T^2}, \tag{22}$$

where $\sigma_T^2$ represents the variance of Gaussian white noise received by Tony.

For current slot, the Eavesdropper receives signal expressed as

$$\begin{aligned}\mathbf{y}_E^U[i] = &\sqrt{P_s}\left(\mathbf{h_{IE}}\mathbf{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_s}[i]+\\ &\sqrt{P_c}\left(\mathbf{h_{IE}}\mathbf{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_c}[i]+\mathbf{n_E}[i],\end{aligned} \tag{23}$$

where the noise at the Eavesdropper is denoted as $\mathbf{n}_E \sim \mathcal{CN}(0,\sigma_E^2)$.Therefore, the SINR for the Eavesdropper under the underlay mode is:

$$\Gamma_E^U = \frac{P_s\left|\mathbf{h_{IE}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2}{P_c\left|\mathbf{h_{IE}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2+\sigma_E^2}, \tag{24}$$

where the Eavesdropper's noise variance is denoted as $\sigma_E^2$.Hence, the secrecy rate at Tony under the underlay mode is expressed as

$$R_s^U = \left[\log_2\left(1+\Gamma_T^U\right)-\log_2\left(1+\Gamma_E^U\right)\right]^+, \tag{25}$$

where $[z]^+ \triangleq \max(z,0)$.

### C. Transmission Outage Probability

When Lisa simultaneously transmits both covert and secure signals under the underlay mode, the received signal at John can be expressed as

$$\begin{aligned}\mathbf{y_J^U}[i] =&\sqrt{P_c}\left(\mathbf{h_{IJ}}\mathbf{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_c}[i]+\\ &\sqrt{P_s}\left(\mathbf{h_{IJ}}\mathbf{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_s}[i]+\mathbf{n_J}[i],\end{aligned} \tag{26}$$

where $\mathbf{n_J}[i]$ and $\sigma_J^2$ denote the receive AWGN signal at John for the $i$-th channel use, and the noise variance, respectively. Thus, the SINR at John is given by

$$\Gamma_J^U = \frac{P_c\left|\mathbf{h_{IJ}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2}{P_s\left|\mathbf{h_{IJ}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2+\sigma_J^2}. \tag{27}$$

To ensure quality of service (QoS), we require a desired transmission rate $R$ from Lisa to John. Due to the uncertainty of interference and noise, The outage from Lisa to John will occur once if $\log_2\left(1+\Gamma_J^U\right) < R$.

**Lemma 3.** *The transmission outage probability $\delta_J^U$ from Lisa to John, assisted by an IRS under the underlay mode, is expressed as*

$$\delta_J^U = 1-\exp\left[-\frac{\lambda_B\sigma_J^2\left(2^R-1\right)}{P_c-P_s\left(2^R-1\right)}\right], \tag{28}$$

*where $\lambda_B$ is the rate parameter of the exponential distribution of $\left|\mathbf{h_{IJ}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2$.*

### D. Covert Rate

Building upon the result of Lemma 3, the covert rate under the underlay mode, denoted as $R_c^U$, from Lisa to John with the assistance of an IRS is determined as follows

$$R_c^U = \kappa\left(1-\delta_J^U\right) = \kappa\exp\left[-\frac{\lambda_B\sigma_J^2\left(2^R-1\right)}{P_c-P_s\left(2^R-1\right)}\right], \tag{29}$$

where $\kappa$ is the coefficient of the preset desired transmission rate $R$.

### E. Problem Formulation

To maximize the covert rate under the underlay mode, this section jointly optimizes the covert and the total transmit powers of Lisa, as well as the configurations of the IRS. This is an optimization problem with the constraints of the covertness requirement, the amplitude and phase-shift of the elements on the IRS, and the limitations of maximum covert and the total transmit powers of Lisa, which is formulated as

$$\begin{aligned}\boldsymbol{P1}: \quad &\max_{P_c,P,\mathbf{\Theta}} \quad R_c^U = \kappa\exp\left[\frac{-\lambda_B\sigma_J^2\left(2^R-1\right)}{P_c-P_s\left(2^R-1\right)}\right] && \text{(30a)}\\ &\text{s.t.} \quad \xi_U^* \geq 1-\varepsilon, && \text{(30b)}\\ &\quad R_s^U \geq R_s^{\min}, && \text{(30c)}\\ &\quad 0 \leq q_n \leq 1, \forall n = 1,2,\cdots,N, && \text{(30d)}\\ &\quad 0 \leq \theta_n \leq 2\pi, \forall n = 1,2,\cdots,N, && \text{(30e)}\\ &\quad 0 < P_c \leq P_{c\max}, && \text{(30f)}\\ &\quad 0 < P \leq P_{\max}, && \text{(30g)}\end{aligned}$$

where (30b) is the covertness constraint corresponding to the worst case at the Warden, (30c) represents the secure rate constraint, indicating the QoS requirement. Here, $R_s^{\min}$ denotes the minimum secure rate requirement for Tony, Equations (30d) and (30e) represent the constraints for the amplitude and phase shift of the reflecting elements, respectively. Meanwhile, Equations (30f) and (30g) correspond to the covert and total communication transmit power requirements, respectively. $P_{c\max}$ and $P_{\max}$ denote the maximum covert and total transmit powers of Lisa, respectively. Addressing this problem is challenging, given the intricate interdependence of the optimization variables $P_c$, $P$, and $\mathbf{\Theta}$, together with the non-convex nature of the optimal problem $\boldsymbol{P1}$. To address the non-convexity issue in problem $\boldsymbol{P1}$, we employ a strategy of transforming it into a convex counterpart. We then solve the resulting transformed convex problem using CVX, a MATLAB-based convex optimization framework that simplifies the formulation and solving of convex optimization problems [54], [55].

### F. Problem Solution

When Lisa transmits both covert and secure signals, We observe from Equation (6) that the average power received at the Warden under the underlay mode as

$$\left(P_c+P_s\right)\left|\mathbf{h_{IW}}\mathbf{\Theta}\mathbf{h_{LI}}\right|^2+\sigma_W^2, \tag{31}$$

which can be rearranged as

$$\begin{aligned}&\left(P_c+P_s\right)\left|\sigma_{IW}^2\sum_{n=1}^{N}\left|h_{LI_n}\right|q_n e^{j\left(\theta_n+\arg\left(h_{IW_n}\right)+\arg\left(h_{LI_n}\right)\right)}\right|^2\\ &+\sigma_W^2.\end{aligned} \tag{32}$$

To minimize the received signal power at the Warden, we have designed the optimal phase shift of the IRS as follows

$$\theta_n^* = -\left(\arg\left(h_{IT_n}\right) + \arg\left(h_{LI_n}\right)\right), \forall n = 1, 2, \cdots, N \quad (33)$$

and (32) is simplified as

$$\begin{aligned}&\left(P_c + P_s\right)\sigma_{IW}^2\left(\sum_{n=1}^{N} q_n^2 |h_{LI_n}|^2\right) + \sigma_W^2 \\ =&PA + \sigma_W^2.\end{aligned} \quad (34)$$

Here, as denoted before, $P = P_s + P_c$, and $A = \sigma_{IW}^2\left(\sum_{n=1}^{N} q_n^2 |h_{LI_n}|^2\right)$. Therefore, the optimal problem $\boldsymbol{P1}$ can be reformulated as $\boldsymbol{P1.1}$.

$$\begin{aligned}\boldsymbol{P1.1}: \quad \max_{P_c, P, \boldsymbol{q_n}} \quad & R_c^U = \kappa \exp\left[\frac{-\lambda_B \sigma_J^2\left(2^R - 1\right)}{P_c - P_s\left(2^R - 1\right)}\right] && (35a)\\ \text{s.t.} \quad & \xi_U^* \geq 1 - \varepsilon, && (35b)\\ & R_s^U \geq R_s^{\min}, && (35c)\\ & 0 \leq q_n \leq 1, \forall n = 1, 2, \cdots, N, && (35d)\\ & 0 < P_c \leq P_{c\max}, && (35e)\\ & 0 < P \leq P_{\max}. && (35f)\end{aligned}$$

We employ the Block Coordinate Descent (BCD) algorithm, which fixes the total power of Lisa, $P$, and the amplitude $\boldsymbol{q_n}$ of the reflecting elements matrix on the IRS. We then discuss the monotonicity of $P_c$. To determine the monotonicity of $R_c^U$ with respect to $P_c$, we examine the derivatives of $R_c^U$ with respect to $P_c$, which is expressed as

$$\frac{\partial R_c^U}{\partial P_c} = \frac{\kappa \lambda_B \sigma_J^2\left(2^R - 1\right)}{\left[P_c - P_s\left(2^R - 1\right)\right]^2 \exp\left[\frac{\lambda_B \sigma_J^2 (2^R - 1)}{P_c - P_s(2^R - 1)}\right]} > 0. \quad (36)$$

So, $R_c^U$ is a monotonically increasing function of $P_c$. Therefore, to maximize the covert rate, Lisa should transmit the covert signal with the maximum allowable transmit power under the covert transmission requirement and the secrecy rate power constraint.

**Proposition 1.** *The objective function given by Equation (35a) is convex over the domain $P_c - \beta P_s > 0$.*

Next, we discuss the covert constraint (35b). We observe from (34) that the covertness requirement (35b) can be reformulated as $PA + \sigma_W^2 \leq V(\tau)$ for a given $\tau$, where $V(\tau)$ represents the value of $(PA + \sigma_W^2)$ that satisfies (35b). Then, (35b) can be reformed as the following convex formulation

$$P\sigma_{IW}^2 \mathbf{q}^{\boldsymbol{T}} \mathbf{H_{LI}} \mathbf{q} + \sigma_W^2 \leq V^U(\tau). \quad (37)$$

where $\mathbf{q} = [q_1, q_2, \cdots, q_N]^T$, $q_n$ is the $i$-th element of $\mathbf{q}$.

Now, the optimization problem $\boldsymbol{P1.1}$ remains non-convex due to the inclusion of secure rate constraints, as expressed in (35c). Given a pre-set minimum secure rate $R_s^{\min} > 0$, it follows that $R_s^U$ is non-negative. Consequently, we can simplify equation (25) as

$$R_s^U = \log_2\left(1 + \Gamma_T^U\right) - \log_2\left(1 + \Gamma_E^U\right). \quad (38)$$

To reveal the non-convexity of (35c), we reformulate (38) as

$$R_s^U = \vartheta_1 - \vartheta_2, \quad (39)$$

where

$$\begin{cases}\vartheta_1 = \log_2\left(P|\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2 + \sigma_T^2\right) \\ +\log_2\left[\left(P - P_s\right)|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2 + \sigma_E^2\right], \\ \vartheta_2 = \log_2\left(P|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2 + \sigma_E^2\right) \\ +\log_2\left[\left(P - P_s\right)|\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2 + \sigma_T^2\right].\end{cases} \quad (40)$$

Then, by employing the difference of convex functions (DC) method, we approximate $\vartheta_2$ as $\tilde{\vartheta}_2$ as

$$\begin{aligned}\tilde{\vartheta}_2(P) =& \vartheta_2\left(P(\mu - 1)\right) \\ &-\nabla\vartheta_2\left(P(\mu - 1)\right)\left(P - P(\mu - 1)\right),\end{aligned} \quad (41)$$

where $\nabla$ is the gradient operator, $\mu$ is the iteration number, and $\nabla\vartheta_2\left(P(\mu - 1)\right)$ is calculated as

$$\begin{aligned}\nabla\vartheta_2\left(P(\mu - 1)\right) =& \frac{|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2}{\ln 2\left(P(\mu - 1)|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2 + \sigma_E^2\right)} \\ &+\frac{|\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2}{\ln 2\left[(P(\mu - 1) - P_s)|\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}|^2 + \sigma_T^2\right]}.\end{aligned} \quad (42)$$

We approximate (35c) as $\vartheta_1 - \tilde{\vartheta}_2 - R_s^{\min} \geq 0$, which is concave. Thus, we can express the optimal problem $\boldsymbol{P1.1}$ as $\boldsymbol{P1.2}$.

$$\begin{aligned}\boldsymbol{P1.2}: \quad \max_{P_c, P, \boldsymbol{q_n}} \quad & R_c^U = \kappa \exp\left[\frac{-\lambda_B \sigma_J^2\left(2^R - 1\right)}{P_c - P_s\left(2^R - 1\right)}\right] && (43a)\\ \text{s.t.} \quad & P\sigma_{IW}^2 \mathbf{q}^{\boldsymbol{T}} \mathbf{H_{LI}} \mathbf{q} + \sigma_W^2 \leq V^U(\tau), && (43b)\\ & \vartheta_1 - \tilde{\vartheta}_2 - R_s^{\min} \geq 0, && (43c)\\ & 0 \leq q_n \leq 1, \forall n = 1, 2, \cdots, N, && (43d)\\ & 0 < P_c \leq P_{c\max}, && (43e)\\ & 0 < P \leq P_{\max}. && (43f)\end{aligned}$$

Now, the optimization problem $\boldsymbol{P1.2}$ is convex and can be effectively solved using CVX, i.e., a Matlab-based modeling package designed for convex program specification and solution [54], [55].

## V. Covert Transmission under Overlay Mode

In this section, under the overlay mode, we first investigate the covert transmission requirement and secrecy rate constraint. Subsequently, we analyze the transmission outage probability from Lisa to John with the assistance of an IRS. Using this probability, we calculate John's covert rate and model an optimization problem to maximize it.

### A. Covert Transmission Requirement

**Theorem 2.** *We use $\gamma_O^*$ to denote the optimal value of $\gamma^O$ achieving minimum $\xi^O$ of Warden. Then, we have*

$$\gamma_O^* = \sigma_W^2, \tag{44}$$

*and the corresponding minimum detection error rate of Warden is given by*

$$\xi_O^* = 0. \tag{45}$$

### B. Secrecy Rate Constraint

Under the overlay mode, Lisa efficiently avoids signal interference by transmitting covert and secrecy signals on separate non-interfering channels. Consequently, at the respective receiving nodes, signals remain undisturbed by mutual interference. So, when Lisa transmits both covert and secrecy signals under the overlay mode, the expression for the received signal at Tony is given by

$$\mathbf{y}_T^O[i] = \sqrt{P_s}\left(\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_s}[i] + \mathbf{n_T}[i]. \tag{46}$$

Hence, the Signal-to-Noise Ratio (SNR) at Tony is

$$\Gamma_T^O = \frac{P_s\left|\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2}{\sigma_T^2}. \tag{47}$$

At the same time, the signal received by the Eavesdropper is formulated as

$$\mathbf{y}_E^O[i] = \sqrt{P_s}\left(\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_s}[i] + \mathbf{n_E}[i]. \tag{48}$$

Hence, the SNR for the Eavesdropper is given by

$$\Gamma_E^O = \frac{P_s\left|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2}{\sigma_E^2}, \tag{49}$$

where Eavesdropper's noise variance is denoted as $\sigma_E^2$. As a result, the secrecy rate at Tony under the overlay mode is expressed as

$$R_s^O = \left[\log_2\left(1+\Gamma_T^O\right) - \log_2\left(1+\Gamma_E^O\right)\right]^+, \tag{50}$$

where $[z]^+ \triangleq \max(z, 0)$.

### C. Transmission Outage Probability

When Lisa transmits both covert and secure signals under the overlay mode, the received signal at John can be expressed as

$$\mathbf{y_J^O}[i] = \sqrt{P_c}\left(\mathbf{h_{IJ}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right)\mathbf{x_c}[i] + \mathbf{n_J}[i]. \tag{51}$$

Thus, the Signal-to-Noise Ratio (SNR) at John is given by

$$\Gamma_J^O = \frac{P_c\left|\mathbf{h_{IJ}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2}{\sigma_J^2}. \tag{52}$$

**Lemma 4.** *The transmission outage probability $\delta_J^O$ from Lisa to John, assisted by an IRS under the overlay mode, is expressed as*

$$\delta_J^O = 1 - \exp\left[-\frac{\lambda_B\sigma_J^2\left(2^R-1\right)}{P_c}\right], \tag{53}$$

*where $\lambda_B$ is the rate parameter of the exponential distribution of $\left|\mathbf{h_{IJ}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2$.*

### D. Covert Rate

Based on Lemma 4, we derive the covert rate, denoted as $R_c^O$, under the overlay mode for the communication from Lisa to John with the assistance of an IRS. It is expressed as

$$R_c^O = \kappa\exp\left[-\frac{\lambda_B\sigma_J^2\left(2^R-1\right)}{P_c}\right], \tag{54}$$

where $\kappa$ is the coefficient associated with the preset desired rate.

### E. Problem Formulation

In this subsection, we maximize the covert rate under the overlay mode by jointly optimizing Lisa's covert and total transmit powers, along with IRS configurations. This is subject to the same constraints as the underlay mode. The formulated optimization problem is as follows

$$\begin{aligned}
\boldsymbol{P2}: \quad \max_{P_c,P,\boldsymbol{\Theta}} \quad & R_c^O = \kappa\exp\left[-\frac{\lambda_B\sigma_J^2\left(2^R-1\right)}{P_c}\right] && \text{(55a)}\\
\text{s.t.} \quad & \xi_O^* \geq 1-\varepsilon, && \text{(55b)}\\
& R_s^O \geq R_s^{\min}, && \text{(55c)}\\
& 0 \leq q_n \leq 1, \forall n = 1,2,\cdots,N, && \text{(55d)}\\
& 0 \leq \theta_n \leq 2\pi, \forall n = 1,2,\cdots,N, && \text{(55e)}\\
& 0 < P_c \leq P_{c\max}, && \text{(55f)}\\
& 0 < P \leq P_{\max}, && \text{(55g)}
\end{aligned}$$

where (55b) is the covertness constraint, (55c) is the secure rate requirement, (55d) and (55e) are the constraints for the amplitudes and phase shift of reflecting elements, respectively. (55f) and (55g) represent the covert and the total transmit power constraints, respectively.

### F. Problem Solution

When Lisa transmits both covert and secure signals, we observe from Equation (12) that the average power received at the Warden under the overlay mode as

$$\left|\mathbf{h_{IW}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2 P_c + \sigma_W^2, \tag{56}$$

which can be rearranged as

$$P_c\left|\sigma_{IW}^2\sum_{n=1}^{N}\left|h_{LI_n}\right|q_n e^{j\left(\theta_n+\arg\left(h_{IW_n}\right)+\arg\left(h_{LI_n}\right)\right)}\right|^2 + \sigma_W^2. \tag{57}$$

To minimize the received signal power at the Warden, the optimal phase shift of the IRS is strategically determined as follows

$$\theta_n^* = -\left(\arg\left(h_{IT_n}\right) + \arg\left(h_{LI_n}\right)\right), \forall n = 1, 2, \cdots, N \quad (58)$$

and (57) is simplified as

$$\begin{aligned} &P_c\sigma_{IW}^2\left(\sum_{n=1}^{N} q_n^2 |h_{LI_n}|^2\right) + \sigma_W^2 \\ =&P_c A + \sigma_W^2, \end{aligned} \quad (59)$$

where as defined early, $A = \sigma_{IW}^2\left(\sum_{n=1}^{N} q_n^2 |h_{LI_n}|^2\right)$. Therefore, the optimal problem $\boldsymbol{P2}$ can be reformulated as $\boldsymbol{P2.1}$.

$$\begin{aligned} \boldsymbol{P2.1}: \quad \max_{P_c, P, \boldsymbol{q_n}} \quad & R_c^O = \kappa \exp\left[-\frac{\lambda_B \sigma_J^2\left(2^R - 1\right)}{P_c}\right] && (60a)\\ \text{s.t.} \quad & \xi_O^* \geq 1 - \varepsilon, && (60b)\\ & R_s^O \geq R_s^{\min}, && (60c)\\ & 0 \leq q_n \leq 1, \forall n = 1, 2, \cdots, N, && (60d)\\ & 0 < P_c \leq P_{c\max}, && (60e)\\ & 0 < P \leq P_{\max}. && (60f) \end{aligned}$$

Similar to the approach used in the underlay mode, we utilize the BCD algorithm, maintaining the total power $P$ of Lisa, and the amplitude $\boldsymbol{q_n}$ of the reflecting elements matrix on the IRS constant. We further determine the monotonicity of $R_c^O$ with respect to $P_c$, and thus we derive the derivatives of $R_c^O$ with respect to $P_c$ as

$$\frac{\partial R_c^O}{\partial P_c} = \frac{\kappa \lambda_B \sigma_J^2\left(2^R - 1\right)}{P_c^2 \exp\left[\frac{\lambda_B \sigma_J^2 (2^R - 1)}{P_c}\right]} > 0. \quad (61)$$

Hence, $R_c^O$ exhibits a monotonically increasing behavior with respect to $P_c$. Consequently, to optimize the covert rate, Lisa should transmit the covert signal at the maximum permissible transmit power, adhering to both covert transmission requirements and secrecy rate power constraints.

**Proposition 2.** *The objective function given by Equation (60a) is convex for* $0 < P_c < \frac{\alpha}{2}$.

Next, we discuss the covert constraint (60b). We observe from (59) that the covertness requirement (60b) can be reformulated as $P_c A + \sigma_W^2 \leq V^O(\tau)$ for a given $\tau$, where $V^O(\tau)$ represents the value of $(P_c A + \sigma_W^2)$ that satisfies (60b). Then, (60b) can be reformed as the following convex formulation

$$P_c\sigma_{IW}^2 \mathbf{q}^{\boldsymbol{T}} \mathbf{H_{LI}} \mathbf{q} + \sigma_W^2 \leq V^O\left(\tau\right), \quad (62)$$

where $\mathbf{q} = [q_1, q_2, \cdots, q_N]^T$, $q_n$ is the $i$-th element of $\mathbf{q}$. Now, the optimization problem $\boldsymbol{P2.1}$ remains non-convex due to the inclusion of secure rate constraints, as expressed in (60c). Given a pre-set minimum secure rate $R_s^{\min} > 0$, it follows that $R_s^O$ is non-negative. Consequently, we can simplify equation (21) as

$$R_s^O = \log_2\left(1 + \Gamma_T^O\right) - \log_2\left(1 + \Gamma_E^O\right). \quad (63)$$

To address the non-convexity of (60c), we reformulate (63) as follows

$$R_s^O = \nu_1 - \nu_2, \quad (64)$$

where

$$\begin{aligned} \nu_1 &= \log_2\left[\left(P - P_c\right)\left|\mathbf{h_{IT}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2 + \sigma_T^2\right] + \log_2\left(\sigma_E^2\right), \\ \text{and } \nu_2 &= \log_2\left[\left(P - P_c\right)\left|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2 + \sigma_E^2\right] + \log_2\left(\sigma_T^2\right). \end{aligned} \quad (65)$$

By employing the DC method, we approximate $\nu_2$ as $\tilde{\nu}_2$. Then,

$$\begin{aligned} \tilde{\nu}_2\left(P_c\right) =& \nu_2\left(P_c\left(\mu - 1\right)\right) \\ &-\nabla\nu_2\left(P_c\left(\mu - 1\right)\right)\left(P_c - P_c\left(\mu - 1\right)\right), \end{aligned} \quad (66)$$

where $\nabla$ is the gradient operator, $\mu$ is the iteration number, and $\nabla\nu_2\left(P_c\left(\mu - 1\right)\right)$ is calculated as

$$\begin{aligned} &\nabla\nu_2\left(P_c\left(\mu - 1\right)\right) \\ =&\frac{\left|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2}{\ln 2\left[\left(P(\mu - 1) - P_c\right)\left|\mathbf{h_{IE}}\boldsymbol{\Theta}\mathbf{h_{LI}}\right|^2 + \sigma_E^2\right]}. \end{aligned} \quad (67)$$

We approximate (60c) as $\nu_1 - \tilde{\nu}_2 - R_s^{\min} \geq 0$, which is concave. Then, we can express the optimal problem $\boldsymbol{P2.1}$ as the following $\boldsymbol{P2.2}$.

$$\begin{aligned} \boldsymbol{P2.2}: \quad \max_{P_c, P, \boldsymbol{q_n}} \quad & R_c^O = \kappa \exp\left[\frac{-\lambda_B \sigma_J^2\left(2^R - 1\right)}{P_c}\right] && (68a)\\ \text{s.t.} \quad & P_c\sigma_{IW}^2 \mathbf{q}^{\boldsymbol{T}} \mathbf{H_{LI}} \mathbf{q} + \sigma_W^2 \leq V^O\left(\tau\right), && (68b)\\ & \nu_1 - \tilde{\nu}_2 - R_s^{\min} \geq 0, && (68c)\\ & 0 \leq q_n \leq 1, \forall n = 1, 2, \cdots, N, && (68d)\\ & 0 < P_c \leq P_{c\max}, && (68e)\\ & 0 < P \leq P_{\max}. && (68f) \end{aligned}$$

Given that the optimization problem $\mathbf{P2.2}$ is now convex, we utilize CVX to solve this optimization problem.

## VI. Covert Transmission under Hybrid Mode

In this section, we present a novel hybrid mode for Lisa, the signal source, facilitating flexible transmission of both covert and secure signals. The hybrid mode enables Lisa to seamlessly transition between underlay and overlay modes, enhancing covert performance based on specific operational requirements.

### A. Covert Rate Modeling

The covert rate under the hybird mode can be formulated as

$$R_c = \max\left\{R_c^U, R_c^O\right\}. \quad (69)$$

where $R_c^U$ is determined by (29), while $R_c^O$ is determined by (54).

### B. Covert Rate Maximization

We present an optimization problem aiming to maximize the covert rate, taking into account constraints like the covert requirement, secrecy rate, amplitudes, phase shifts of reflecting elements, and limitation on transmit power.

$$\boldsymbol{P3}: \max_{P_c,P,\boldsymbol{\Theta}} \quad R_c \tag{70a}$$
$$\text{s.t.} \quad \xi^* \geq 1-\varepsilon, \tag{70b}$$
$$R_s \geq R_s^{\min}, \tag{70c}$$
$$0 \leq q_n \leq 1, \forall n = 1,2,\cdots,N, \tag{70d}$$
$$0 \leq \theta_n \leq 2\pi, \forall n = 1,2,\cdots,N, \tag{70e}$$
$$0 < P_c \leq P_{c\max}, \tag{70f}$$
$$0 < P \leq P_{\max}, \tag{70g}$$

where (70b) represents the covertness requirement, (70c) is the secure rate requirement, (70d) and (70e) are the constraints for the amplitudes and phase shift of reflecting elements, respectively. (70f) represents the covert transmit power constraint, and (70g) represents the total transmit power constraint.

The optimal problem of (70) can be solved using the following expression

$$R_c^* = \max\left\{\left(R_c^U\right)^*, \left(R_c^O\right)^*\right\}, \tag{71}$$

where $(R_c^U)^*$ and $(R_c^O)^*$ represent the optimal results of the optimization problems $\boldsymbol{P1.2}$ and $\boldsymbol{P2.2}$, respectively.

## VII. Computational Complexity and Convergence Analysis

### A. Computational Complexity

In both underlay and overlay modes, each DC/SCA iteration solves a convex subproblem with decision variables $(P, P_c, \mathbf{q})$, where $\mathbf{q} \in \mathbb{R}^N$ dominates the dimension. Let $n$ be the number of real variables after CVX canonicalization. We have $n = \boldsymbol{\Theta}(N)$, while the number of affine/conic constraints is $m = \boldsymbol{\Theta}(N)$. Using primal–dual interior-point methods, the per-iteration computational cost is cubic in the effective problem size, i.e., $\mathcal{O}((n+m)^3)$. Hence, the worst-case complexity of solving one convex subproblem scales approximately as $\mathcal{O}(N^3)$, up to logarithmic accuracy factors and problem-dependent constants. With $I$ outer BCD iterations and $K$ inner DC/SCA iterations, the overall complexity is

$$\mathcal{O}(IKN^3). \tag{72}$$

### B. Convergence Analysis

The proposed algorithm follows a BCD framework combined with DC/SCA approximations. At each iteration, a convex surrogate problem is solved to optimality using a convex solver. Under standard regularity conditions for SCA/DC methods (e.g., local tightness and first-order consistency of the surrogate functions, bounded feasible set due to power constraints, and continuity of the involved mappings), the objective sequence generated by the algorithm is bounded and admits at least one accumulation point. Moreover, any such accumulation point satisfies the first-order necessary optimality conditions (i.e., it is a stationary point in the BCD sense) of the original non-convex problem.

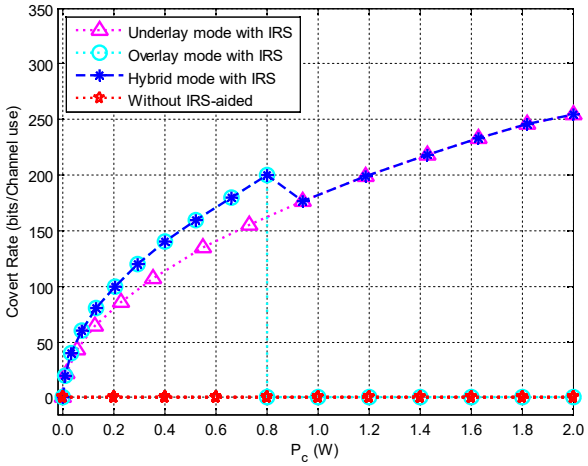


Fig. 2. Covert Rates versus Lisa's Covert Transmit Power, $P_c$

## VIII. Numerical Results and Discussion

In the IRS-aided WCS, numerical results are presented to examine the impact of some crucial parameters on covert transmission performance while satisfying the requirements for secure transmission. Unless specified otherwise, the parameter values can be found in TABLE II.

TABLE II
Parameters

| Parameters | Values |
|---|---|
| Transmit powers of secure and covert signals, ($P_s$, $P_c$) | 1.0 W |
| Covertness requirement ($\varepsilon$) | 0.01 |
| The maximum total transmit power of Lisa, ($P_{\max}$) | 2.0 W |
| Variance noises at Tony and John ($\sigma_T^2$, $\sigma_J^2$) | 0.001 W |
| Variance noises at Warden and Eavesdropper ($\sigma_W^2$, $\sigma_E^2$) | 0.001 W |
| Coefficient of the preset desired rate, $\kappa$ | 1.5 |

Figure 2 shows how Lisa's covert transmit power $P_c$ affects the covert rates across different transmission schemes. The absence of an IRS results in a covert rate of zero, indicating the lack of communication links between Lisa and John necessary for establishing a covert transmission channel. Furthermore, as depicted in Figure 2, under the underlay mode, the covert rate gradually increases with the rise of $P_c$. This is because, under the constraints of covert requirements, an increase in $P_c$ effectively enhances the covert signal strength. However, even with the assistance of the IRS in the overlay mode, the covert transmission requirement cannot be met beyond a certain level of $P_c$. Consequently, the covert rate drops and remains at zero. In the hybrid mode, Lisa selects the covert rate that offers better performance with the aid of the IRS. Therefore, the covert rate for the hybrid mode corresponds to the larger value between the underlay and overlay modes.

Figure 3 illustrates the impact of Lisa's maximum covert transmit power $P_{c\max}$ on the maximum covert rates under different schemes. We observe that, as $P_{c\max}$ increases, the

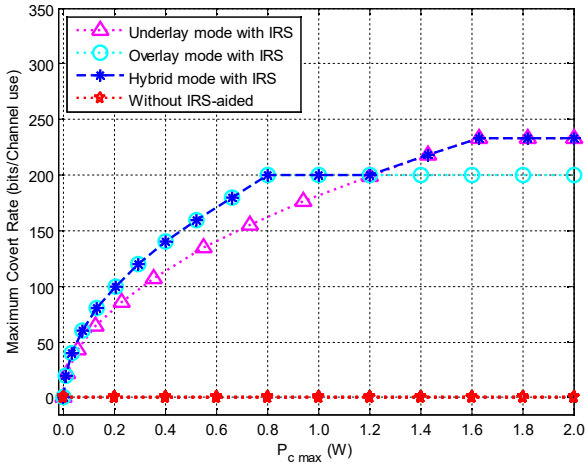


Fig. 3. Maximum Covert Rates versus Lisa's Maximum Covert Transmit Power, $P_{c\max}$

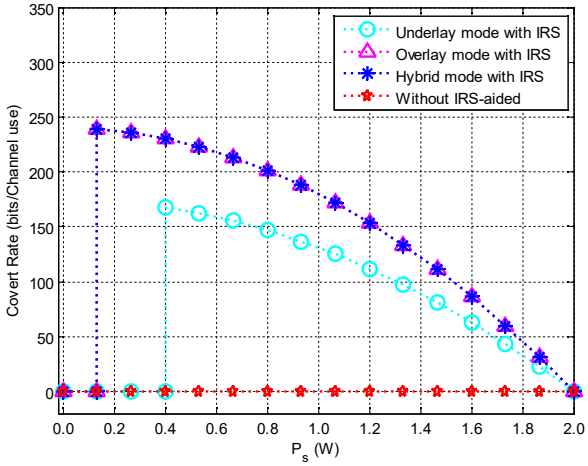


Fig. 4. Covert Rates versus Lisa's Secure Transmit Power, $P_s$

maximum covert rate achieved by the scheme without IRS assistance remains at zero, mirroring the situation depicted in Fig. 2. Meanwhile, the maximum covert rates achieved under both the underlay mode and the overlay mode with IRS assistance gradually increase, reaching their respective optimal values and remaining constant. The interference received by John is smaller under the overlay mode compared to the underlay mode, resulting in a two-fold effect. On one hand, less interference leads to a faster increase in the maximum covert rate of the overlay mode compared to the underlay mode. On the other hand, the absence of protection from interference of the secure signal prevents the covert requirement from being met shortly after $P_{c\max}$ increases. For the hybrid mode assisted by the IRS, its maximum covert rate corresponds to the larger value between the underlay and overlay modes. This results in a graphical representation that initially increases gradually, then remains constant, increases again, and finally stabilizes.

Figure 4 investigates the impact of Lisa's secure transmit power $P_s$ on the covert rates for different transmission schemes. From Fig. 4, we observe that the covert rates

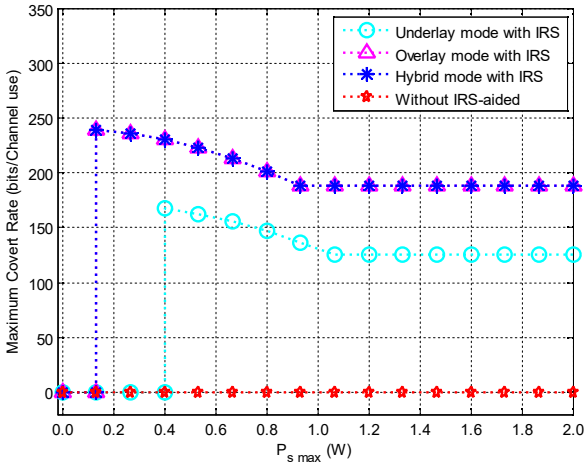


Fig. 5. Maximum Covert Rates versus Lisa's Maximum Secure Transmit Power, $P_{s\max}$

achieved by the IRS-assisted schemes in both the underlay and overlay modes initially remain at zero. Subsequently, they experience a sudden increase, with the covert rate under the overlay mode jumping earlier than that under the underlay mode. This discrepancy arises because, in the overlay mode, the absence of interference from the covert transmission power on the secure transmission channel enables the fulfillment of the minimum required secure rate faster than under the underlay mode. Both rates then decrease with the increase of the secure transmit power $P_s$. This is because, as defined before, the total transmit power of Lisa is expressed as $P = P_s + P_c$. With a fixed value of $P$, an increase in secure transmit power, $P_s$, leads to a decrease in the covert transmit power, $P_c$, consequently resulting in a corresponding decrease in the covert rates. For the hybrid mode, the covert rate corresponds to the larger value between the overlay and underlay modes. Therefore, its covert rate aligns with the data from the overlay mode.

Figure 5 examines how Lisa's secure transmit power $P_{s\max}$ influences the maximum covert rates for various transmission schemes. From Fig. 5, we observe that the maximum covert rates in scenarios assisted by the IRS initially start at zero with the increase of $P_{s\max}$. They then sharply rise to high levels in both underlay and overlay modes before gradually decreasing to their optimal values and maintaining stability thereafter. The reasons behind these phenomena can be attributed to the initial small transmit power of the secure transmission signal, which fails to meet the minimum secure transmission rate requirement for achieving maximum covert rates. Notably, the overlay mode benefits from an unaffected secure transmission channel, allowing it to satisfy the minimum secure rate constraint earlier than the underlay mode with the increase of $P_{s\max}$. Consequently, the overlay mode transitions from zero to a higher value earlier than the underlay mode. Subsequently, for both modes, the gradual increase in $P_{s\max}$ leads to a reduction in $P_{c\max}$, causing a decrease in maximum covert rates to their respective optimized values, which then remain constant. This delicate balance between the secure transmit power $P_{s\max}$ and the covert transmit power $P_{c\max}$ is crucial

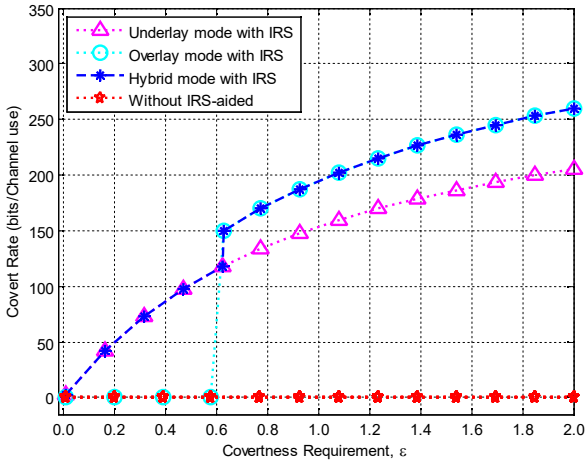


Fig. 6. Covert Rates versus the Covertness Requirement, $\varepsilon$

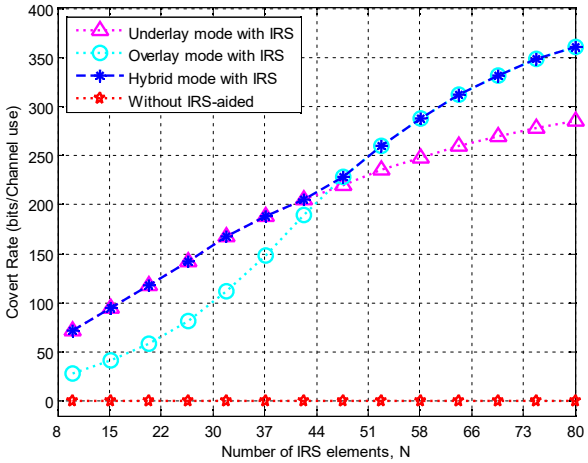


Fig. 7. Covert rate versus the number of IRS elements under different transmission modes.

in shaping the observed phenomena. For the hybrid mode, the maximum covert rate corresponds to the higher value between the overlay and underlay modes. Therefore, it aligns with the numerical value of the maximum covert rate under the overlay mode.

Fig. 6 depicts how the covertness requirement $\varepsilon$ affects covert rates under different schemes. Fig. 6 reveals that, when lacking IRS assistance, the covert rate consistently stays at zero as $\varepsilon$ increases. This outcome aligns with the observations made from Fig. 2, Fig. 3, Fig. 4 and Fig. 5 for scenarios without IRS assistance. Another observation is that when $\varepsilon$ increases, the covert rates under the IRS-assisted schemes gradually rise. This phenomenon is attributed to the fact that an increase in $\varepsilon$ indicates a gradual relaxation of the covert requirement, leading to an increment in the covert rate. However, for the overlay mode, the absence of interference from the secure signal has a dual impact. Initially, without the protection of the secure signal, the stringent covert requirement cannot be met, and thus the covert rate is kept at zero. When $\varepsilon$ increases, relaxing the covert requirement, the covert demand under the overlay mode becomes achievable. Additionally, due to the lack of interference from the secure signal, the covert rate in the overlay mode surpasses that under the underlay mode. For the covert rate under the hybrid mode, it takes the larger value between the overlay and underlay modes. Consequently, in the initial stage, its value aligns with that of the underlay mode. However, as the overlay mode satisfies the covert requirement later, the covert rate under the hybrid mode matches that of the overlay mode.

Fig. 7 shows the covert rate versus the number of IRS elements under different transmission modes. As the number of IRS elements increases, the covert rate of all IRS-assisted schemes improves due to the enhanced passive beamforming gain. Although a larger IRS also increases the received signal power at adversarial nodes, such as the warden and the eavesdropper, the IRS phase shifts can be designed to favor the legitimate link while mitigating signal leakage toward these nodes. As a result, a net gain in covert transmission performance is achieved as the IRS size grows. For the underlay mode, the covert rate increases smoothly with the

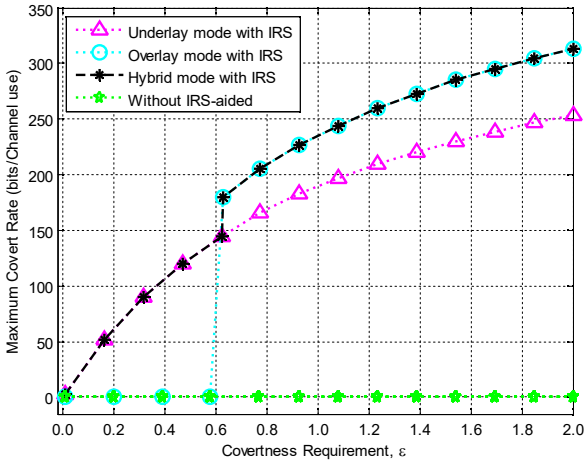


Fig. 8. Maximum Covert Rates versus the Covertness Requirement, $\varepsilon$

number of IRS elements, benefiting from the masking effect of the secure signal. In contrast, the overlay mode yields a lower covert rate in the small-IRS regime due to the stringent covertness constraint, but increases more rapidly as the IRS gain improves, and eventually surpasses the underlay mode. The hybrid mode follows the better of the underlay and overlay modes, coinciding with the underlay mode for small IRS sizes and switching to the overlay mode when it becomes superior. In contrast, without IRS assistance, the covert rate remains zero for all values of the number of IRS elements.

Fig. 8 illustrates how the maximum covert rates vary with the covertness requirement $\varepsilon$ across different modes. the maximum covert rate remains at zero for scenarios without IRS assistance. In scenarios with IRS assistance, the maximum covert rate gradually increases with the rising $\varepsilon$ under the underlay mode. Meanwhile, in the overlay mode, the maximum covert rate initially stays at zero before surpassing the values of the underlay mode and continuing to rise. In the hybrid mode, the covert rate initially aligns with that of the underlay mode. Once the security rate in the overlay mode meets the minimum required threshold, the numerical values of the covert rate become equivalent to those in the overlay

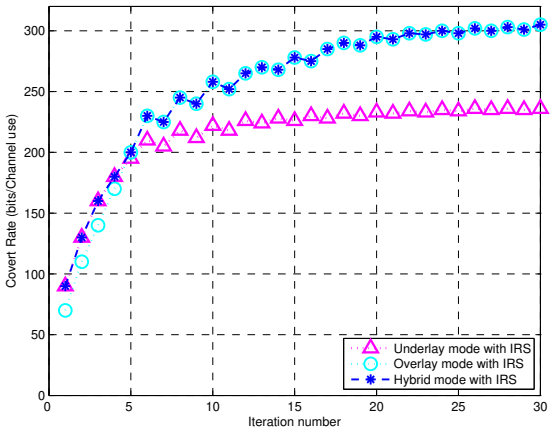


Fig. 9. Convergence behavior of the proposed algorithm under different transmission modes.

mode. These phenomena are consistent with what is observed in Fig. 6.

Fig. 9 shows the convergence behavior of the proposed algorithm. The covert rate increases rapidly at the beginning and stabilizes after about 15–20 iterations. The underlay mode converges to a lower value, while the overlay mode achieves higher performance. The hybrid mode always selects the better one and attains the highest covert rate. The small variations are caused by alternating optimization updates.

## IX. Conclusion

This paper investigated the simultaneous covert and secure transmissions with the support of IRS in a WCS. Specifically, we maximized the covert rate while satisfying secure transmission requirement by a joint optimization of covert transmit power, total transmit power and IRS reflect beamforming under the underlay and overlay modes, respectively. We also proposed a hybrid mode for further enhancing the covert rate performance with the constraint of secure transmission. Extensive numerical results show that the IRS can improve the performance of covert and secure transmissions. Future work will consider extending the proposed framework to scenarios with multiple IRSs, where coordination among different reflecting surfaces needs to be addressed.

## References

[1] Y. Ding, Y. Feng, W. Lu, S. Zheng, N. Zhao, L. Meng, A. Nallanathan, and X. Yang, "Online Edge Learning Offloading and Resource Management for UAV-Assisted MEC Secure Communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 17, no. 1, pp. 54–65, 2023.

[2] X. Zhou, X. Zhou, S. Yan, G. Xia, and F. Shu, "Intelligent Reflecting Surface-Aided Covert Wireless Communications With Finite-Alphabet Inputs," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 4, pp. 6709–6714, 2025.

[3] J. Hu, Q. Lin, S. Yan, X. Zhou, Y. Chen, and F. Shu, "Covert Transmission via Integrated Sensing and Communication Systems," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 3, pp. 4441–4446, 2024.

[4] Y. Feng, L. Xu, Q. Li, S. Yan, H. Wang, and D. W. K. Ng, "Transmit Rate Enhancement for STAR-RIS-Assisted Uplink NOMA," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 5, pp. 7651–7665, 2025.

[5] X. Lu, J. Lei, Y. Shi, and W. Li, "Improved Physical Layer Authentication Scheme Based on Wireless Channel Phase," *IEEE Wireless Communications Letters*, vol. 11, no. 1, pp. 198–202, 2022.

[6] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What Physical Layer Security Can Do for 6G Security," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2023.

[7] E. Illi, M. Qaraqe, S. Althunibat, A. Alhasanat, M. Alsafasfeh, M. de Ree, G. Mantas, J. Rodriguez, W. Aman, and S. Al-Kuwari, "Physical Layer Security for Authentication, Confidentiality, and Malicious Node Detection: A Paradigm Shift in Securing IoT Networks," *IEEE Communications Surveys and Tutorials*, vol. 26, no. 1, pp. 347–388, 2024.

[8] W. Lv, J. Bai, Q. Yan, and H. M. Wang, "RIS-Assisted Green Secure Communications: Active RIS or Passive RIS?" *IEEE Wireless Communications Letters*, vol. 12, no. 2, pp. 237–241, 2023.

[9] M. Zhang, B. Yang, S. Zhao, and L. Ma, "Secrecy Capacity Analysis in D2D-Enabled Cellular Networks Under Power Control," in *2019 International Conference on Networking and Network Applications (NaNA)*, 2019, pp. 81–84.

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

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

[12] T. Cai, J. Zhang, S. Yan, L. Meng, J. Sun, and N. Al-Dhahir, "Resource Allocation for Secure Rate-Splitting Multiple Access with Adaptive Beamforming," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.

[13] J.-Y. Wang, Y.-C. Yu, D.-S. Lu, and D.-P. Su, "Secure Beamforming for MISO Visible Light Communications With ISI and NLoS Components," *IEEE Wireless Communications Letters*, vol. 13, no. 3, pp. 908–912, 2024.

[14] S. Lv, X. Xu, S. Han, and P. Zhang, "RIS-Enhanced Secure Transmission in MTC Networks With Finite Blocklength," *IEEE Transactions on Communications*, vol. 71, no. 6, pp. 3513–3527, 2023.

[15] H. Han, Y. Cao, N. Deng, C. Xing, N. Zhao, Y. Li, and X. Wang, "Secure Transmission for STAR-RIS Aided NOMA Against Internal Eavesdropping," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 11, pp. 15 068–15 073, 2023.

[16] Y. Guo, Y. Liu, Q. Wu, Q. Shi, and Y. Zhao, "Enhanced Secure Communication via Novel Double-Faced Active RIS," *IEEE Transactions on Communications*, vol. 71, no. 6, pp. 3497–3512, 2023.

[17] Y. Xu, T. Zhang, D. Yang, Y. Liu, and M. Tao, "Joint Resource and Trajectory Optimization for Security in UAV-Assisted MEC Systems," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 573–588, 2021.

[18] W. Lu, Y. Ding, Y. Gao, Y. Chen, N. Zhao, Z. Ding, and A. Nallanathan, "Secure NOMA-Based UAV-MEC Network Towards a Flying Eavesdropper," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3364–3376, 2022.

[19] Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, and X. Shen, "UAV-Assisted Physical Layer Security in Multi-Beam Satellite-Enabled Vehicle Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2739–2751, 2022.

[20] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, H. Hu, and F. Gong, "Achieving Reliable and Secure Communications in Wireless-Powered NOMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1978–1983, 2021.

[21] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming Design and Power Allocation for Secure Transmission With NOMA," *IEEE Transactions on Wireless Communications*, vol. 18, no. 5, pp. 2639–2651, 2019.

[22] Y. Yang, B. Yang, S. Shen, Y. She, and T. Taleb, "Covert Rate Study for Full-Duplex D2D Communications Underlaid Cellular Networks," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15 223–15 237, 2023.

[23] Y. Jiang, L. Wang, and H.-H. Chen, "Covert Communications With Randomly Distributed Adversaries in Wireless Energy Harvesting Enabled D2D Underlaying Cellular Networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5401–5415, 2023.

[24] S. Feng, X. Lu, S. Sun, D. Niyato, and E. Hossain, "Securing Large-Scale D2D Networks Using Covert Communication and Friendly Jamming," *IEEE Transactions on Wireless Communications*, vol. 23, no. 1, pp. 592–606, 2024.

[25] J. Li, D. Wu, C. Yue, Y. Yang, M. Wang, and F. Yuan, "Energy-Efficient Transmit Probability-Power Control for Covert D2D Communications With Age of Information Constraints," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 9690–9704, 2022.

[26] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert Communication in Relay-Assisted IoT Systems," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6313–6323, 2021.
[27] C. Gao, B. Yang, D. Zheng, X. Jiang, and T. Taleb, "Cooperative Jamming and Relay Selection for Covert Communications in Wireless Relay Systems," *IEEE Transactions on Communications*, vol. 72, no. 2, pp. 1020–1032, 2024.
[28] R. Sun, B. Yang, S. Ma, Y. Shen, and X. Jiang, "Covert Rate Maximization in Wireless Full-Duplex Relaying Systems With Power Control," *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6198–6212, 2021.
[29] R. Xu, D. Guo, B. Zhang, and G. Ding, "Finite Blocklength Covert Communications in Interweave Cognitive Radio Networks," *IEEE Communications Letters*, vol. 26, no. 9, pp. 1989–1993, 2022.
[30] J. Shi, Z. Dai, Z. Li, Z. Tie, and R. Chen, "User Scheduling Design for Covert Communication in Cooperative Cognitive Radio System," *IEEE Sensors Journal*, vol. 23, no. 5, pp. 5459–5469, 2023.
[31] Z. Li, R. Chen, J. Shi, L. Yang, and S. Ma, "A Game-Theoretic Approach to Achieve Covert Communication in Cognitive Radio Systems," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 10, pp. 13 011–13 023, 2023.
[32] H. Huang, A. V. Savkin, and W. Ni, "Online UAV Trajectory Planning for Covert Video Surveillance of Mobile Targets," *IEEE Transactions on Automation Science and Engineering*, vol. 19, no. 2, pp. 735–746, 2022.
[33] X. Lu, W. Yang, S. Yan, Z. Li, and D. W. K. Ng, "Covertness and Timeliness of Data Collection in UAV-Aided Wireless-Powered IoT," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12 573–12 587, 2022.
[34] M. Tatar Mamaghani and Y. Hong, "Aerial Intelligent Reflecting Surface-Enabled Terahertz Covert Communications in Beyond-5G Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 19 012–19 033, 2022.
[35] X. Zhou, S. Yan, Q. Wu, F. Shu, and D. W. K. Ng, "Intelligent Reflecting Surface (IRS)-Aided Covert Wireless Communications With Delay Constraint," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 532–547, 2022.
[36] S. Ma, Y. Zhang, H. Li, J. Sun, J. Shi, H. Zhang, C. Shen, and S. Li, "Covert Beamforming Design for Intelligent-Reflecting-Surface-Assisted IoT Networks," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5489–5501, 2022.
[37] C. Wang, X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, and D. Niyato, "Covert Communication Assisted by UAV-IRS," *IEEE Transactions on Communications*, vol. 71, no. 1, pp. 357–369, 2023.
[38] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint Information-Theoretic Secrecy and Covert Communication in the Presence of an Untrusted User and Warden," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7170–7181, 2021.
[39] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 17–30, 2023.
[40] R. Sun, B. Yang, J. Jiao, Y. Zuo, Y. Shen, X. Jiang, and W. Yang, "Joint Secure and Covert Communication Study in Two-hop Relaying Systems," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 2023, pp. 1–7.
[41] H.-M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and Covert Communications Against UAV Surveillance via Multi-Hop Networks," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 389–401, 2020.
[42] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert Communication and Secure Transmission Over Untrusted Relaying Networks in the Presence of Multiple Wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020.
[43] M. Forouzesh, F. Samsami Khodadad, P. Azmi, A. Kuhestani, and H. Ahmadi, "Simultaneous Secure and Covert Transmissions Against Two Attacks Under Practical Assumptions," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10 160–10 171, 2023.
[44] C. Wang, Z. Li, H. Zhang, D. W. K. Ng, and N. Al-Dhahir, "Achieving Covertness and Security in Broadcast Channels With Finite Blocklength," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7624–7640, 2022.
[45] P. Liu, Z. Li, J. Si, N. Al-Dhahir, and Y. Gao, "Joint Information-Theoretic Secrecy and Covertness for UAV-Assisted Wireless Transmission With Finite Blocklength," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 187–10 199, 2023.
[46] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep Reinforcement Learning-Based Intelligent Reflecting Surface for Secure Wireless Communications," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 375–388, 2021.
[47] H. Hashida, Y. Kawamoto, and N. Kato, "Selective Reflection Control: Distributed IRS-Aided Communication With Partial Channel State Information," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 11 949–11 958, 2022.
[48] H. Albinsaid, K. Singh, A. Bansal, S. Biswas, C.-P. Li, and Z. J. Haas, "Multiple Antenna Selection and Successive Signal Detection for SM-Based IRS-Aided Communication," *IEEE Signal Processing Letters*, vol. 28, pp. 813–817, 2021.
[49] L. Xiao, S. Hong, S. Xu, H. Yang, and X. Ji, "IRS-Aided Energy-Efficient Secure WBAN Transmission Based on Deep Reinforcement Learning," *IEEE Transactions on Communications*, vol. 70, no. 6, pp. 4162–4174, 2022.
[50] J. Zhang, W. Wang, J. Tang, N. Zhao, K.-K. Wong, and X. Wang, "Robust Secure Transmission for IRS-Aided NOMA Networks With Hybrid Beamforming," *IEEE Transactions on Wireless Communications*, vol. 23, no. 4, pp. 3086–3101, 2024.
[51] R. Sun, B. Yang, Y. Shen, X. Jiang, and T. Taleb, "On Joint Covert and Secure Communications in D2D-Enabled Cellular Systems," *IEEE Transactions on Mobile Computing*, vol. 24, no. 12, pp. 12 918–12 934, 2025.
[52] X. Yu, Y. Zhou, S. Yan, Y. Rui, X. Dang, C. Yuen, and M. Guizani, "Covert Performance of STAR-RIS Aided THz Communication System With RSMA and Phase Errors," *IEEE Journal on Selected Areas in Communications*, vol. 44, pp. 1944–1959, 2026.
[53] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving Covert Wireless Communications Using a Full-Duplex Receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.
[54] M. Grant and S. Boyd, "CVX: Matlab Software for Disciplined Convex Programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.
[55] ——, "Graph Implementations for Nonsmooth Convex Programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110.

**Yihuai Yang** received her B.E. degree in Communication Engineering from Kunming University of Science and Technology and M.S. degree in Communication and Information System from Yunnan University, China in 2001, and 2006, respectively. She is a professor with the School of Information Engineering, Kunming University, Yunnan, China. She is a member of the Yunnan Key Laboratory of Intelligent Logistics Equipment and Systems, China. Her research interests include next-generation wireless systems, integrated sensing and communication, vehicular networks, edge computing, and deep reinforcement learning.

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

**Shikai Shen** received his B.S. and M.S. Degrees from Yunnan Normal University in 1984 and from Yunnan University in 2003, respectively. He is currently a Professor with the School of Electronic Information and Automation, Dianchi College, Kunming, China, the School of Information Engineering, Kunming University, Kunming, China, and also with the Yunnan Key Laboratory of Intelligent Logistics Equipment and Systems, Kunming, China. He is also a Senior Member of the China Computer Federation. His research interests include wireless sensor networks, network coding, the Internet of Things, etc.

**Yumei She** received the B.S. degree from Minzu University of China, Peking, China, in 1985. She is currently a Professor with the School of Mathematics and Computer Science, Yunnan Minzu University, Kunming, China. Her research interests include natural language processing and wireless sensor networks. Prof. She is a member of the China Computer Federation. His research interests include wireless sensor networks, network coding, the Internet of Things, etc.

**Xiaohong Jiang** received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1989, 1992, and 1999 respectively. He is currently a Full Professor with the School of Systems Information Science, Future University Hakodate, Japan. Before joining Future University, he was an Associate Professor with Tohoku University, from February 2005 to March 2010. His research interests include computer communications networks, mainly wireless networks and optical networks, network security, and routers/switches design. He has published over 300 technical papers at premium international journals and conferences, which include over 70 papers published in top IEEE journals and conferences, such as IEEE/ ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, and IEEE INFOCOM.

**Tarik Taleb** received the B.E. degree with distinction in Information Engineering and the M.Sc. and Ph.D. degrees in Information Sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Full Professor at Ruhr University Bochum (RUB), Germany, where he leads research activities on next-generation mobile and distributed systems. Prior to joining RUB, he was a Professor at the University of Oulu, Finland (2018–2023), and an Associate Professor at Aalto University, Finland (2014–2021). Earlier in his career, he served as a Senior Researcher and 3GPP Standards Expert at NEC Europe Ltd., Heidelberg, Germany, where he contributed to the evolution of mobile network architectures and standardization activities. Before joining NEC, he was an Assistant Professor at the Graduate School of Information Sciences, Tohoku University, Japan, working in a research laboratory fully funded by KDDI. He also held a Research Fellowship at the Intelligent Cosmos Research Institute, Japan, from 2005 to 2006. Prof. Taleb is widely recognized for his pioneering contributions to mobile network softwarization, network slicing, cloud-edge continuum management, and autonomous networking. His current research interests include autonomous network and service management, edge-cloud continuum systems, network softwarization and slicing, software-defined security, and AI-native communication networks.

## APPENDIX

### A. Proof of Lemma 1

*Proof:* We note that

$$\sqrt{P_c}\left(\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}\right)=\sqrt{P_c}\left(\sum_{n=1}^{N}h_{IW_n}\theta_n h_{LI_n}\right), \tag{73}$$

where $h_{IW_n}$ and $h_{LI_n}$ are the $n$-th element of the wireless channel $\mathbf{h}_{IW}$ and $\mathbf{h}_{LI}$, respectively.

Due to the unavailability of knowledge regarding $\mathbf{h}_{IW}$ and $\mathbf{h}_{LI}$ at Warden, only the statistical information of $h_{IW_n}\sim\mathcal{CN}(0,\sigma_{IW}^2)$ and $h_{LI_n}\sim\mathcal{CN}(0,\sigma_{LI}^2)$ are accessible, where $\sigma_{IW}^2$ and $\sigma_{LI}^2$ represent the variances of the noise on the channels $h_{IW_n}$ and $h_{LI_n}$, respectively. Consequently, $(\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI})\sim\mathcal{CN}(0,A)$, where $A=\sigma_{IW}^2\left(\sum_{n=1}^{N}q_n^2|h_{LI_n}|^2\right)$. As a result, $|\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2$ follows an exponential distribution with parameter $\lambda_A$. Building on this observation and referencing equation (6), the false alarm rate under the underlay mode can be expressed as

$$\begin{aligned}P_{FA}^{U}&=P(\mathcal{D}_1|\mathcal{H}_0)\\&=P(T^U>\gamma^U|\mathcal{H}_0)\\&=P\left(|\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2>\frac{\gamma^U-\sigma_W^2}{P_s}\right)\\&=1-P\left(|\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2\le\frac{\gamma^U-\sigma_W^2}{P_s}\right)\\&=\begin{cases}1, & \gamma^U<\sigma_W^2,\\ 1-\displaystyle\int_0^{\frac{\gamma^U-\sigma_W^2}{P_s}}\lambda_A\exp(-\lambda_A x)\,dx, & \sigma_W^2\le\gamma^U\le\phi_1,\\ 0, & \gamma^U>\phi_1,\end{cases}\end{aligned} \tag{74}$$

and

$$\begin{aligned}P_{MD}^{U}&=P(\mathcal{D}_0|\mathcal{H}_1)\\&=P(T^U<\gamma^U|\mathcal{H}_1)\\&=P\left(|\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2P_c+|\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2P_s+\sigma_W^2<\gamma^U\right)\\&=\begin{cases}0, & \gamma^U<\phi_1,\\ \displaystyle\int_0^{\frac{\gamma^U-\sigma_W^2}{P_c+P_s}}\lambda_A\exp(-\lambda_A x)\,dx, & \phi_1\le\gamma^U\le\phi_2,\\ 1, & \gamma^U>\phi_2,\end{cases}\end{aligned} \tag{75}$$

which completes the proof of Lemma 1. ∎

### B. Proof of Lemma 2

*Proof:* Based on the binary hypothesis testing adopted by Warden, and according to equation (12), the false alarm rate under the overlay mode can be expressed as

$$\begin{aligned}P_{FA}^{O}&=P(\mathcal{D}_1|\mathcal{H}_0)\\&=P(T^O>\gamma^O|\mathcal{H}_0)\\&=\begin{cases}1, & \gamma^O<\sigma_W^2,\\ 0, & \gamma^O\ge\sigma_W^2,\end{cases}\end{aligned} \tag{76}$$

$$\begin{aligned}P_{MD}^{O}&=P(\mathcal{D}_0|\mathcal{H}_1)\\&=P(T^O<\gamma^O|\mathcal{H}_1)\\&=P\left(|\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2P_c+\sigma_W^2<\gamma^O\right)\\&=\begin{cases}0, & \gamma^O<\sigma_W^2,\\ \displaystyle\int_0^{\frac{\gamma^O-\sigma_W^2}{P_c}}\lambda_A\exp(-\lambda_A x)\,dx, & \sigma_W^2\le\gamma^O\le\phi_1,\\ 1, & \gamma^O>\phi_1,\end{cases}\end{aligned} \tag{77}$$

which completes the proof of Lemma 2. ∎

### C. Proof of Lemma 3

*Proof:* Due to the unavailability of knowledge regarding $\mathbf{h}_{IJ}$ and $\mathbf{h}_{LI}$ at Lisa, she only knows the statistical information of $h_{IJ_n}\sim\mathcal{CN}(0,\sigma_{IJ}^2)$ and $h_{LI_n}\sim\mathcal{CN}(0,\sigma_{LI}^2)$. As such, $(\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI})\sim\mathcal{CN}(0,B)$, where $B=\sigma_{IJ}^2\left(\sum_{n=1}^{N}q_n^2|h_{LI_n}|^2\right)$. Here, $\sigma_{IJ}^2$ and $\sigma_{LI}^2$ are noise variances of the channels $h_{IJ_n}$ and $h_{LI_n}$, respectively. As a result, $|\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI}|^2$ follows an exponential distribution with parameter $\lambda_B$.

Based on the definition of transmission outage probability, it follows that

$$\begin{aligned}\delta_J^U&=P\big[\log_2(1+\Gamma_J^U)<R\big]\\&=P\big(\Gamma_J^U<2^R-1\big)\\&=P\left(\frac{P_c|\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI}|^2}{P_s|\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI}|^2+\sigma_J^2}<2^R-1\right)\\&=\int_0^{\frac{\sigma_J^2(2^R-1)}{P_c+P_s-2^RP_s}}\lambda_B\exp(-\lambda_B x)\,dx\\&=1-\exp\left[-\frac{\lambda_B\sigma_J^2(2^R-1)}{P_c+P_s-2^RP_s}\right],\end{aligned} \tag{78}$$

which completes the proof of Lemma 3. ∎

### D. Proof of Lemma 4

*Proof:* Given the definition of transmission outage probability, it can be inferred that

$$\begin{aligned}\delta_J^O&=P\big[\log_2(1+\Gamma_J^O)<R\big]\\&=P\big(\Gamma_J^O<2^R-1\big)\\&=P\left(\frac{P_c|\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI}|^2}{\sigma_J^2}<2^R-1\right)\\&=P\left(|\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI}|^2<\frac{\sigma_J^2(2^R-1)}{P_c}\right)\\&=\int_0^{\frac{\sigma_J^2(2^R-1)}{P_c}}f_{|\mathbf{h}_{IJ}\mathbf{\Theta}\mathbf{h}_{LI}|^2}(x)\,dx\\&=\int_0^{\frac{\sigma_J^2(2^R-1)}{P_c}}\lambda_B\exp(-\lambda_B x)\,dx\\&=1-\exp\left[-\frac{\lambda_B\sigma_J^2(2^R-1)}{P_c}\right],\end{aligned} \tag{79}$$

which completes the proof of Lemma 4. ∎

### E. Proof of Theorem 1

*Proof:* Following equations (2), (15), and (16), Warden's total detection error rate can be expressed as

$$\xi^U = \begin{cases} \exp\left[\lambda_A \dfrac{\sigma_W^2 - \gamma^U}{P_s}\right], & \sigma_W^2 \le \gamma^U < \phi_1, \\ 1 - \exp\left[\lambda_A \left(\dfrac{\sigma_W^2 - \gamma^U}{P_c + P_s}\right)\right], & \phi_1 \le \gamma^U < \phi_2, \\ 1, & \text{otherwise}, \end{cases} \tag{80}$$

where $\phi_1 = |\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2 P_s + \sigma_W^2$, and

$$\phi_2 = |\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2 P_c + |\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2 P_s + \sigma_W^2.$$

- ***Case I***: For $\gamma^U < \sigma_W^2$ and $\gamma^U > \phi_2$, $\xi^U = 1$, representing the worst-case scenario for Warden. Therefore, Warden does not set the optimal threshold $\gamma_U^*$ in these regions.
- ***Case II***: For $\sigma_W^2 \le \gamma^U < \phi_1$, to determine the monotonicity of $\xi^U$, we calculate the first derivative of $\xi^U$ with respect to $\gamma^U$ and obtain

$$\frac{\partial \xi^U}{\partial \gamma^U} = -\frac{\lambda_A}{P_s} \exp\left[\lambda_A \frac{\sigma_W^2 - \gamma^U}{P_s}\right] < 0. \tag{81}$$

  Thus, $\xi^U$ is a continuously decreasing function of $\gamma^U$, implying that Warden will set $\phi_1$ as the optimal threshold $\gamma_U^*$ to minimize his total detection error rate $\xi^U$. Therefore,

$$\xi_U^* = \exp\left(-\lambda_A |\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2\right). \tag{82}$$

- ***Case III***: For $\phi_1 \le \gamma^U < \phi_2$, employing the same method, we also calculate the first derivative of $\xi^U$ with respect to $\gamma^U$ and get

$$\frac{\partial \xi^U}{\partial \gamma^U} = \frac{\lambda_A}{P_c + P_s} \exp\left[\lambda_A \left(\frac{\sigma_W^2 - \gamma^U}{P_c + P_s}\right)\right] > 0. \tag{83}$$

  Then, we know that $\xi^U$ is a continuously increasing function of $\gamma^U$. Thus, Warden also sets $\phi_1$ as the optimal threshold to minimize $\xi^U$ in this case. Therefore,

$$\xi_U^* = 1 - \exp\left(-\frac{\lambda_A |\mathbf{h}_{IW}\mathbf{\Theta}\mathbf{h}_{LI}|^2}{P_c + P_s}\right). \tag{84}$$

Consequently, $\xi_U^*$ corresponds to the minimum value between equations (82) and (84), thereby concluding the proof of Theorem 1. ∎

### F. Proof of Theorem 2

*Proof:* Building upon equations (2), (17), and (18), we can derive the overall detection error rate $\xi^O$ observed by Warden as

$$\xi^O = \begin{cases} 1 - \exp\left[\lambda_A \left(\dfrac{\sigma_W^2 - \gamma^O}{P_c}\right)\right], & \sigma_W^2 \le \gamma^O \le \phi_1, \\ 1, & \text{otherwise}. \end{cases} \tag{85}$$

We first notice that Warden will not set the optimal detection threshold $\gamma_O^*$ in the range where $\xi^O = 1$. Next, to evaluate the monotonic behavior of $\xi^O$ within the range of $\sigma_W^2 \le \gamma^O \le \phi_1$, we calculate the first derivative of $\xi^O$ with respect to $\gamma^O$ and get

$$\frac{\partial \xi^O}{\partial \gamma^O} = \frac{\lambda_A}{P_c} \exp\left[\lambda_A \left(\frac{\sigma_W^2 - \gamma^O}{P_c}\right)\right] > 0. \tag{86}$$

Therefore, the overall error rate $\xi^O$ is a monotonically increasing function of $\gamma^O$. Warden will choose $\sigma_W^2$ as the optimal threshold $\gamma_O^*$ to minimize $\xi^O$. By substituting $\gamma_O^* = \sigma_W^2$ into equation (85), we obtain equation (45), thus concluding the proof of Theorem 2. ∎

### G. Proof of Proposition 1

*Proof:* To analyze the convexity of the objective function in (35a), we rewrite it as

$$R_c^U(P_c, P_s) = \kappa \cdot \exp\left(-\frac{\alpha}{P_c - \beta P_s}\right), \tag{87}$$

where $\alpha = \lambda_B \sigma_J^2 (2^R - 1) > 0$ and $\beta = 2^R - 1 > 0$ are constants, and $\kappa > 0$ is a positive scaling constant.

Let us define an intermediate function $z(P_c, P_s) = P_c - \beta P_s$. Then, define

$$g(P_c, P_s) = -\frac{\alpha}{z(P_c, P_s)} = -\alpha \cdot \frac{1}{P_c - \beta P_s}. \tag{88}$$

The function $z(P_c, P_s)$ is affine and therefore convex. Since $z > 0$, the function $h(z) = -\alpha/z$ is concave on this domain. Thus, $g(P_c, P_s) = h(z(P_c, P_s))$ is the composition of a concave function with an affine mapping, and is therefore concave.

Now, consider the full objective function:

$$R_c^U(P_c, P_s) = \kappa \cdot \exp(g(P_c, P_s)). \tag{89}$$

Since $\exp(x)$ is a convex and non-decreasing function, and $g(P_c, P_s)$ is concave, the composition $f(g(P_c, P_s)) = \exp(g(P_c, P_s))$ is convex by the composition rule for convex functions. Therefore, $R_c^U(P_c, P_s)$ is a convex function over the domain $P_c - \beta P_s > 0$. This concludes the proof of Proposition 1. ∎

### H. Proof of Proposition 2

*Proof:* Let $\alpha = \lambda_B \sigma_J^2 (2^R - 1) > 0$. Then the objective function becomes

$$R_c^O(P_c) = \kappa \exp\left(-\frac{\alpha}{P_c}\right), \quad P_c > 0. \tag{90}$$

Its second derivative is

$$\begin{aligned} \frac{d^2 R_c^O}{dP_c^2} &= \kappa \exp\left(-\frac{\alpha}{P_c}\right)\left(\frac{\alpha^2}{P_c^4} - \frac{2\alpha}{P_c^3}\right) \\ &= \kappa \exp\left(-\frac{\alpha}{P_c}\right) \cdot \frac{\alpha}{P_c^4}(\alpha - 2P_c) \end{aligned} \tag{91}$$

Since $\kappa > 0$, $\alpha > 0$, and $P_c > 0$, the sign of the second derivative depends on $\alpha - 2P_c$. Thus,

$$P_c < \frac{\alpha}{2}. \tag{92}$$

Therefore, $R_c^O(P_c)$ is convex for $0 < P_c < \alpha/2$. This concludes the proof of Proposition 2. ∎