Joint Information-Theoretic Secrecy and Covert Communication in the Presence of an Untrusted User and Warden

Moslem Forouzesh*, Student Member, IEEE, Paeiz Azmi†, Senior Member, IEEE, Ali Kuhestani, Member, IEEE, and Phee Lep Yeoh‡, Member, IEEE

Abstract—In this article, we investigate joint information-theoretic secrecy and covert communication in a single-input–multioutput (SIMO) system where a transmitter (Alice) is communicating with two legitimate users (Bob and Carol). We consider that an untrusted user and a warden node are also present in the network attempting to attack the secure and covert communications to Bob and Carol, respectively. Specifically, Bob requires secure communications such that his messages from Alice are not detected by the warden. To do so, we consider that Alice transmits Carol’s messages during selected time slots to hide them from the warden while also transmitting Bob’s messages in each time slot contentiously. We formulate an optimization problem with the aim of maximizing the average rate subject to a covert communication requirement and a secure communications constraint. Since the proposed optimization problem is nonconvex, we utilize successive convex approximation to obtain a tractable solution. Moreover, we extend our proposed system model to multiple antenna Alice scenario and find beamforming vectors so that the average sum rate is maximized. Furthermore, we consider practical assumptions that Alice has imperfect knowledge of the warden’s location and imperfect channel state information (CSI) of Bob and Carol. Our numerical examples highlight that the imperfect CSI at Carol has a more detrimental impact on the average rate compared to imperfect CSI at Bob.

Index Terms—Covert communication, imperfect channel state information (CSI), information theoretic secrecy (ITS), power allocation.

I. INTRODUCTION

THE SECURITY and privacy of wireless communications is emerging as a critical consideration for network operators due to the widespread and open nature of wireless transmissions. Generally, the security protections for wireless communications have been implemented based on well-known cryptographic key-based approaches in the higher layers of the network design [1]. This approach is based on assuming specific constraints on the computational capacity of a wireless eavesdropper, such that it cannot discover the secret key assigned to the legitimate users to decrypt the confidential information. Recently, information theoretic secrecy (ITS) has been introduced as a promising technique for securing wireless communication in which no complicated key-exchange procedures are imposed on the network [2]. In the pioneering work [3], Wyner illustrates when the eavesdropper’s channel is a degraded version of the legitimate user’s channel, the transmitter and receiver are able to achieve a positive perfect secrecy rate. Toward this end, several techniques have been proposed to enhance the ITS: Transmit beamforming [4]–[6], antenna selection [7], [8], cooperative techniques [9]–[11], artificial noise aided transmission [12]–[15], and using power-domain nonorthogonal multiple access (PD-NOMA) [16]–[18]. In ITS, the goal is to secure the content of the confidential message from the eavesdropper. However, in other scenarios with privacy considerations, the transmitter and receiver aim to hide the existence of their communications from a warden, which is the so-called covert communication. In the covert communication literature, a warden is a node that tries to detect whether the transmitter has sent an information signal to the receiver or not, in the current time slot. It is worth noting that, when the warden detects the presence of information transmission, it can launch a hostile attack to the network.

In recent years, researchers have investigated covert communication in various wireless communication scenarios, such as IoT applications [19], [20], unmanned aerial vehicle (UAV) networks [21], [22], cooperative relaying networks [23]–[26], device-to-device (D2D) communications in 5G [27], and IEEE 802.11 Wi-Fi networks [28]. In [22], covert communication was considered in the presence of a UAV with location uncertainty of terrestrial nodes. Liu et al. [19], [20] investigated covert communication in an IoT network and showed that the presence of interferences from other devices can be harnessed to support covert communication. Wang et al. [23] investigated covert communication in the presence of an amplify-and-forward relay under the assumption of channel uncertainty. Greedy relaying was investigated in [24] in which the relay
opportunistically transmits its own information to the destination covertly besides retransmitting the source’s message. In [28], a covert jamming attack was investigated which is an inserting attack in IEEE 802.11 wireless LANs. The aim of this attack is to destroy the data and defraud the transmitter by injecting a covert jamming signal [28].

Most previous works have assumed that perfect channel state information (CSI) is accessible. However, in realistic scenarios, it is challenging to acquire the CSI of legitimate nodes without channel estimation error. This is because imperfect events, such as feedback delay, limited training power and duration, and low-rate feedback [10] impact on the channel estimation procedure. To this end, Forouzesh et al. [29] studied covert communications with imperfect knowledge of the warden’s channel distribution while perfect CSI of the legitimate user is still available. The idea of employing an uninformed jammer was proposed in [30], where the source can transmit data covertly to the destination in the presence of an adversary. Recently, Forouzesh et al. [31] studied and compared the performance of ITS and covert communication for a single wiretap channel with the aim of maximizing the secrecy or covert rate.

In this article, we consider the joint ITS and covert communication requirements in a single-input–multioutput (SIMO) network, where two legitimate users (Bob and Carol) request two different security services from the transmitter Alice, which is a novel system model and has not been considered before. Furthermore, two adversary nodes, namely, an untrusted user and a warden node, are present in the network performing ITS and covert communications attacks, respectively. In this system model, Bob needs to receive his message securely, while Carol needs to receive her message covertly. To achieve secrecy, our aim is to prevent the untrusted user from decoding Bob’s message from Alice. Additionally, to achieve covertness, our goal is to avoid the warden from detecting the presence of Carol’s message from Alice. To achieve this, we consider that Alice transmits Carol’s messages during selected time slots to hide them from the warden, while she transmits Bob’s messages in each time slot contentiously. Different from previous works [30], [33], that relied on high powered jammers for interference injection, our proposed joint transmission model applies Bob’s data signal as interference at Willie to support the covert requirements of Carol. Furthermore, Carol’s data signal plays the role of an interfering signal at the untrusted user to support the ITS requirements of Bob. Based on this approach, we formulate an optimization problem with the aim of maximizing the average rate subject to the covertness and secrecy constraints. Since the proposed optimization problem is nonconvex, its solution is intractable. As such, we adopt successive convex approximation to convexify the objective function and obtain a tractable solution. To obtain further insights, we consider a practical scenario, where the CSI of the users and the location of the warden are not perfectly known. Finally, numerical examples and discussions are provided to highlight joint ITS and covert design insights. Specifically, we confirm that the joint secure and covert communications can be successfully achieved by our proposed transmission scheme. Furthermore, we observe that the imperfect CSI of Carol has a more negative impact on the average rate compared to Bob.

Our main contributions are summarized as follows.

1) We propose a new secure communications optimization scenario with the aim of maximizing the average rate subject to covertness and secrecy constraints. We adopt successive convex approximation to obtain a tractable solution.

2) We also consider the practical scenario, where the CSI of the users and the location of the warden are not perfectly known due to the passive warden and channel estimation errors, respectively. We focus on the worst case performance, in which we maximize the average rate for the worst channel and Warden’s location mismatch. We observe that the imperfect CSI of Carol has a more negative impact on the average rate compared to Bob. Furthermore, we consider multiple antennas at Alice and find beamforming vectors that maximize the average rate.

II. SYSTEM MODEL

We consider the system model shown in Fig. 1, which consists of one transmitter (Alice), two legitimate users (Carol and Bob), one untrusted user, and one warden (Willie). This untrusted user and warden scenario may arise in large-scale distributed systems where the trustworthiness and transparency of all users in the network is difficult to guarantee and therefore the transmitter Alice will need to adapt her communications protocol based on the requirements of the legitimate users and potential adversary users identified by the network operator. The distance between Alice and Bob, Alice and Carol, Alice and untrusted user, and Alice and warden are defined as $d_{ab}$, $d_{ac}$, $d_{au}$, and $d_{aw}$, respectively. The channel fading coefficients between Alice and Bob, Alice and Carol, Alice and untrusted user, and Alice and warden are $h_{ab}$, $h_{ac}$, $h_{au}$, and $h_{aw}$, respectively, and these channels have circularly symmetric complex Gaussian distribution with zero mean and unit variance. We assume that all the channel coefficients remain constant within one frame and change independently from one frame to another. Note that a time frame consists of several consecutive time slots.

Alice transmits confidential messages to Carol and Bob, where one user (Bob) requires secure communications to protect against the untrusted user and another user (Carol) requires covert communications to avoid detection by the warden. In this system model, Bob needs to receive his message securely, while Carol needs to receive her message covertly. For secure transmission, our aim is to prevent the untrusted user from
decoding Bob’s message from Alice. Additionally, for covert communication, our goal is to avoid the warden from detecting the presence of Carol’s message from Alice. Hence, Alice employs a joint ITS and covert communication approach to transmit data to Bob and Carol, respectively. In our proposed approach, Alice transmits Carol’s messages according to a predetermined set of indexes for the covert communication time slots, while she transmits Bob’s messages in each data transmission time slot contentiously. In the considered system model, we assume that Alice knows the location and CSI of Bob, Carol, and the untrusted user whereas Alice only knows the location of the warden with no CSI information. This is because we assume the untrusted user is an active user that knows the codebook of the communication network to decode the transmissions from Alice whereas the warden is a passive user that does not participate in any communications [30].

We consider a discrete-time channel with $Q$ time slots, each having a length of $n$ symbols, hence, the transmit signals to Carol and Bob in one time slot are $x_c = [x_1^c, x_2^c, \ldots, x_n^c]$ and $x_b = [x_1^b, x_2^b, \ldots, x_n^b]$, respectively. Note that Alice transmits $x_c$ continuously while she only transmits $x_b$ to Carol during selected covert communication time slots. In the next section, we investigate two main cases: 1) only Carol knows the covert communication time slot indexes and 2) both Carol and Bob know the covert communication time slot indexes.

III. PROPOSED JOINT OPTIMIZATION OF ITS AND COVERT TRANSMISSION RATE

In the covert communication literature, it is typically assumed that the legitimate receivers are aware of Alice’s data transmission strategy. Accordingly, Alice shares a secret of sufficient length between herself and the legitimate receivers to inform them of the covert communication strategy (data transmission time slot index) [23], [32], [33], which is unknown to the warden. In this section, we will first consider that Bob does not know Carol’s covert strategy, i.e., he does not have access to Alice and Carol’s preshared secret encoding strategy. In the following, we analyze the proposed system model based on this assumption.

A. Information Theoretic Security Requirement

The received vector at node $m$ (this node can be Bob, Carol, untrusted user, or warden) is given by

$$y_m = \begin{cases} \sqrt{p_{ab} h_{am} x_b} / d_{am}^{\alpha/2} + n_m, & \Psi_0 \\ \sqrt{p_{ac} h_{am} x_c} / d_{am}^{\alpha/2} + \sqrt{p_{ac} h_{am} x_c} / d_{am}^{\alpha/2} + n_m, & \Psi_1 \end{cases}$$

where $p_{ab}$ and $p_{ac}$ are Alice’s transmit power for Bob and Carol, respectively, $\alpha$ is the path-loss exponent, and $n_m \sim \mathcal{CN}(0, \sigma_m^2 I_n)$ represents the receiver noise at $m$. Here, $I_n$ represents an $n \times n$ identity matrix. Then notation $\Psi_0$ states that Alice does not transmit a covert signal to Carol, while $\Psi_1$ states that Alice transmits to Carol. In the following, we assume the total transmit power is limited by $P$, which is a common assumption in [12]–[14]. Hence, Alice transmits secure and covert messages (to Bob and Carol) with power $p_{ab} = \{p_{ab} \Psi_0 + p_{ac} \Psi_1 \}$ and $p_{ac} = \{0, \Psi_0 \}$, respectively, where $p_{ab} \in [0, 1]$ and $p_{ac} \in [0, 1]$ are the power allocation factor in $\Psi_0$ and $\Psi_1$ slots, respectively. In order to simplify notations, we define $y_a = P|h_{ac}|^2 / d_{ac}^{\alpha/2}, y_b = P|h_{ab}|^2 / d_{ab}^{\alpha/2}, y_c = P|h_{ac}|^2 / d_{ac}^{\alpha/2}, y_w = P|h_{aw}|^2 / d_{aw}^{\alpha/2}, y_u = P|h_{aw}|^2 / d_{aw}^{\alpha/2}$.

The signal-to-noise ratio (SNR) and the signal-to-interference-plus-noise-ratio (SINR) for symbol $\ell$ at the untrusted user and Bob can be written, respectively, as follows:

$$\gamma_\ell^f = \frac{\rho_\ell y_a}{\rho_\ell y_u + 1 - (1 - \rho_\ell) y_u}, \quad \Psi_0$$

$$\gamma_\ell^f = \frac{\rho_\ell y_b}{1 - (1 - \rho_\ell) y_b}, \quad \Psi_1$$

Therefore, the secrecy rate at Bob is given by

$$R_{\text{sec}}^f(\rho) = \log_2 \left( 1 + \gamma_\ell^f - \log_2 \left( 1 + \gamma_\ell^f \right) \right)^+$$

where $[x]^+$ is defined as max$\{x, 0\}$.

B. Covert Communication Requirement

Based on its received signal power, the warden decides whether Alice has sent data to Carol or not. If the warden decides that Alice has sent data to Carol when Alice has not sent any data to Carol, this means that a false alarm (FA) has occurred. Moreover, if the warden decides that Alice has not sent data to Carol when Alice has sent data to Carol, then we say that a missed detection (MD) with Carol when the following inequality is satisfied [30]:

$$\gamma_\ell^f y_u > \gamma_\ell^f y_c$$

Moreover, the optimal decision rule for minimizing the detection error at the warden is written as [30]

$$\frac{Y_u}{n} \leq \theta$$
where \( Y_w = \sum_{\ell=1}^{n} |y_{w,\ell}|^2 \) is the total received power at the warden in each time slot and \( \theta \) is the decision threshold at the warden. Based on (5), we have \( \sum_{\ell=1}^{n} |y_{w,\ell}|^2 |h_{aw}|^2 \sim (\sigma^2_w + \Xi)^2 \chi^2_n/n \) where \( \chi^2_n \) is a chi-squared random variable with \( 2n \) degrees of freedom. Hence, the FA and MD probabilities can be written as
\[
P_{t}^{FA} = \mathbb{P}
\left( \frac{Y_w}{n} > \theta | \Psi_0 \right) = \mathbb{P}
\left( \frac{(\sigma^2_w + \Xi)^2 \chi^2_n}{n} > \theta | \Psi_0 \right)
\] (10)
\[
P_{t}^{MD} = \mathbb{P}
\left( \frac{Y_w}{n} < \theta | \Psi_1 \right) = \mathbb{P}
\left( \frac{(\sigma^2_w + \Xi)^2 \chi^2_n}{n} < \theta | \Psi_1 \right).
\] (11)

According to the strong law of large numbers (SLLNs), \( \chi^2_n/n \) converges to 1, and based on Lebesgue’s dominated convergence theorem [34] (Ch. 10, p. 231), we can replace \( \chi^2_n/n \) with 1, when \( n \to \infty \). Hence, we can rewrite (10) and (11) as follows:
\[
P_{t}^{FA} = \mathbb{P}(\sigma^2_w + \Xi > \theta | \Psi_0)
\] (12)
\[
P_{t}^{MD} = \mathbb{P}(\sigma^2_w + \Xi < \theta | \Psi_1)
\] (13)

by using distribution of random variable \( \Xi \) as explained in (6), (12), and (13) are calculated as follows:
\[
P_{t}^{FA} = \begin{cases} e^{-\frac{(\theta-\sigma^2_w)}{\Psi_0}}, & \theta - \sigma^2_w \geq 0 \\ 1, & \theta - \sigma^2_w < 0 \end{cases}
\] (14)
\[
P_{t}^{MD} = \begin{cases} 1 - e^{-\frac{(\theta-\sigma^2_w)}{\Psi_1}}, & \theta - \sigma^2_w \geq 0 \\ 0, & \theta - \sigma^2_w < 0 \end{cases}
\] (15)

By exploiting (14) and (15), \( p_{t}^{FA} + p_{t}^{MD} \) can be written as
\[
p_{t}^{FA} + p_{t}^{MD} = \begin{cases} 1 - e^{-\frac{(\theta-\sigma^2_w)}{\Psi_1}} + e^{-\frac{(\theta-\sigma^2_w)}{\Psi_0}}, & \theta - \sigma^2_w \geq 0 \\ 1, & \theta - \sigma^2_w < 0 \end{cases}
\] (16)

It is clear that the warden will select a decision threshold greater than the variance of the received noise, to ensure that the resulting detection error probability will be less than 1.

C. Optimization Formulation

In this section, to evaluate the proposed system model we formulate a novel optimization problem at which the main aim is to maximize the average rate subject to transmit power limitation, quality of service constraints, and the covert communication requirement, i.e., (8). The secrecy rate at Bob is given by
\[
R_{sec}^{F}(\rho_s, \rho_c) = \begin{cases} \log_2\left(1 + \rho_s \gamma_b\right) - \log_2\left(1 + \rho_s \gamma_a\right), & \Psi_0 \\ \log_2\left(1 + \frac{\rho_c \gamma_b}{1 + (1 - \rho_c) \gamma_b}\right), & \Psi_1 \end{cases}
\] (17)

When Alice transmits a secure message and covert message to Bob and Carol, respectively, the sum rate in this time slot is
\[
R = \mathbb{E}_{q}[\hat{R}] = p_q^{(0)} \left[ \log_2\left(1 + \rho_s \gamma_b\right) - \log_2\left(1 + \rho_s \gamma_a\right) \right]^+ + q \left[ \log_2\left(1 + \frac{\rho_c \gamma_b}{1 + (1 - \rho_c) \gamma_b}\right) - \log_2\left(1 + \frac{\rho_c \gamma_a}{1 + (1 - \rho_c) \gamma_a}\right) \right]^+
\] (18)

Since Alice does not transmit data to Carol continuously, we define a Bernoulli random variable \( q \). When the value of this random variable is 0 with probability of \( p_q^{(0)} \), Alice only transmits a secure message to Bob. When its value is one with probability of \( p_q^{(1)} \), Alice transmits both secure and covert messages. As such, the sum rate in each time slot can be expressed as
\[
\hat{R} = \mathbb{E}_{q}[\hat{R}] = p_q^{(0)} \left[ \log_2\left(1 + \rho_s \gamma_b\right) - \log_2\left(1 + \rho_s \gamma_a\right) \right]^+ + q \left[ \log_2\left(1 + \frac{\rho_c \gamma_b}{1 + (1 - \rho_c) \gamma_b}\right) - \log_2\left(1 + \frac{\rho_c \gamma_a}{1 + (1 - \rho_c) \gamma_a}\right) \right]^+
\] (19)

where “not(·)” is a logical operation such that it converts 1 to 0, and 0 to 1. Consequently, the average sum rate of the system model in this network can be obtained as
\[
\hat{R} = \mathbb{E}_{q}[\hat{R}] = p_q^{(0)} \left[ \log_2\left(1 + \rho_s \gamma_b\right) - \log_2\left(1 + \rho_s \gamma_a\right) \right]^+ + q \left[ \log_2\left(1 + \frac{\rho_c \gamma_b}{1 + (1 - \rho_c) \gamma_b}\right) - \log_2\left(1 + \frac{\rho_c \gamma_a}{1 + (1 - \rho_c) \gamma_a}\right) \right]^+
\] (20)

where \( \mathbb{E}_{q}[\cdot] \) is the expectation operator over the random variable \( r \). In order to maximize the average rate subject to the power limitation, covert communication requirement, and secrecy rate constraints, with assumption of the warden’s location is available,\(^1\) we propose the following optimization problem:
\[
\max_{\rho_s, \rho_c} \hat{R}(\rho_s, \rho_c)
\] (21a)
\[
s.t.: \quad 0 \leq \rho_s \leq 1
\] (21b)
\[
0 \leq \rho_c \leq 1
\] (21c)
\[
p_q^{(0)} \left[ \log_2\left(1 + \rho_s \gamma_b\right) - \log_2\left(1 + \rho_s \gamma_a\right) \right]^+ \leq \rho_c
\] (21d)

\(^1\)For the feasibility of this scenario, consider an adversary outpost or vessel in a military scenario for which system nodes can visually observe the location. As such, it is possible that Alice has an imperfect knowledge of the warden’s location due to location estimation error, which we investigate in Section IV-A.
Constraints (21d) and (21e) are the secure and covert communication requirements, respectively. Constraint (21f) is the worst case requirement for the covert communication at Carol.

D. Proposed Optimization Solution

To solve the optimization in (21), we present two lemmas as follows.

**Lemma 1:** The optimal power allocation factor in the $\Psi_0$ slot is equal to one, i.e., $\rho_5 = 1$.

**Proof:** The secrecy rate that is defined in (17) is an increasing function with respect to $\rho_5$ for $y_b > y_a$. Hence, in order to maximize the average rate, Alice should transmit secure data ($x_b$) with the maximum allowable transmit power, i.e., $P$ in the time slot $\Psi_0$, which leads to $\rho_5 = 1$.

**Lemma 2:** According to Lemma 1, the covert communication requirement is always satisfied.

**Proof:** When $\rho_5 = 1$, we have the following equation:

$$\psi_0 = \frac{P}{p_{\text{av}}^{\text{MD}}} = \psi_1 = \psi$$

by substituting (22) into (16) we have

$$p_{\text{FA}} + p_{\text{MD}} = \begin{cases} 1 - e^{-(\alpha_{\text{FA}}^2 \psi)} + e^{-(\alpha_{\text{MD}}^2 \psi)}, & \theta - \sigma_b^2 \geq 0 \\ 1, & \theta - \sigma_b^2 < 0 \\ 1, & \theta - \sigma_c^2 \geq 0 \\ 1, & \theta - \sigma_c^2 < 0 \end{cases}$$

which satisfies (21f).

The objective function in (21) is nonconcave, therefore, convex optimization methods cannot be directly applied to solve the optimization. Hence, we proceed by applying the epigraph method [35], such that the optimization problem can be rewritten as

$$\max_{\rho_5, \eta} p_q^{(0)}[\log_2(1 + y_b) - \log_2(1 + y_a)] + p_q^{(1)} \eta + p_q^{(1)} \log_2 \left( 1 + \frac{(1 - \rho_5) y_c}{1 + \rho_5 y_c} \right)$$

s.t. (21b), (21c), (21e)

$$\log_2 \left( 1 + \frac{\rho_5 y_b}{1 + (1 - \rho_5) y_b} \right) \leq \eta$$

$$\eta \geq 0.$$  

**Algorithm 1 Iterative Power Allocation Algorithm**

1. **Initialization:** Set $\mu = 0$ (the iteration number) and initialize to $\rho_c(0)$.
2. Set $\mu = \mu + 1$.
3. Solve (29) and set the result to $\rho_c(\mu)$.
4. If $|\rho_c(\mu) - \rho_c(\mu - 1)| \leq \delta$, stop, else go back to step 2.

The optimization problem (24) is still nonconvex due to constraints (21e) and (24c) and the objective function. To tackle this nonconvexity, we employ the successive convex approximation method to approximate the objective function and constraint (21e) to concave functions and constraint (24c) to a convex constraint. First, we consider the objective function as the following:

$$\Xi(\rho_c) = \Phi(\rho_c) - \Gamma(\rho_c)$$

where

$$\Phi(\rho_c) = p_q^{(0)}[\log_2(1 + y_b) - \log_2(1 + y_a)] + p_q^{(1)} \eta + p_q^{(1)} \log_2(1 + y_c)$$

$$\Gamma(\rho_c) = p_q^{(1)} \log_2(1 + \rho_5 y_c).$$

Employing the difference of convex functions (DCs) method, we approximate $\Gamma(\rho_c)$ as

$$\Gamma(\rho_c) \approx \tilde{\Gamma}(\rho_c) = \Gamma(\rho_c(\mu - 1)) + \nabla \Gamma(\rho_c(\mu - 1)) (\rho_c - \rho_c(\mu - 1))$$

where $\nabla$ is the gradient operator, $\mu$ is the iteration number, and $\nabla \Gamma(\rho_c(\mu - 1))$ is calculated as

$$\nabla \Gamma(\rho_c(\mu - 1)) = \frac{p_q^{(1)} \gamma_c}{\ln 2 (1 + \rho_5 (\mu - 1) y_c)}.$$  

Finally, the objective function can be rewritten as $\Phi(\rho_c) - \tilde{\Gamma}(\rho_c)$, which is concave. Similar to the objective function, we can approximate (21e) and (24c) as $T(\rho_c) - \Lambda(\rho_c) \geq 0$ and $\Omega(\rho_c) - \Sigma(\rho_c) \leq 0$, respectively, where $T(\rho_c) = p_q^{(1)} \log_2(1 + y_c) - R_{\text{sec}}^{\min}$, $\Lambda(\rho_c) = p_q^{(1)} \log_2(1 + \rho_5 y_c)$, $\Omega(\rho_c) = \log_2(1 + (1 - \rho_3) y_b) + \log_2(1 + y_a) - \log_2(1 + y_b) + \eta$, and $\Sigma(\rho_c) = \log_2(1 + (1 - \rho_3) y_b) + \log_2(1 + y_a) - \log_2(1 + y_b) + \eta$. Moreover, $\Lambda$ and $\Omega$ can be evaluated similar to (27). Therefore, after applying the DC approximation, (24) can be rewritten as follows:

$$\max_{\rho_5, \eta} \Phi(\rho_c) - \tilde{\Gamma}(\rho_c)$$

s.t. (21b), (21c), (24b), (24d)

$$T(\rho_c) - \Lambda(\rho_c) \geq 0$$

$$\tilde{\Omega}(\rho_c) - \Sigma(\rho_c) \leq 0.$$
as such, the power allocation optimization problem can be expressed as

\[
\max_{\rho_{cs}} p_q^{(1)} \log_2 \left( \frac{1 + (1 - \rho_{cs}) \gamma_c}{1 + \rho_{cs} \gamma_c} \right) \quad (31)
\]
s.t.: (21b), (21c), (21e).

This optimization problem can be solved similar to the optimization problem in (24), which is skipped for brevity.

E. Special Case: Covert Strategy Known to Carol and Bob

In this section, we consider that both Carol and Bob are aware of the covert strategy, i.e., they both have access to Alice’s pre-shared secret encoding strategy. The pre-shared secret encoding enables Bob and Carol to know which time slot will be used by Alice to transmit the covert message. In this scenario, assuming that Carol and Bob share the same transmission bandwidth, we can employ a PD-NOMA multiple access method in which Bob and Carol can perform successive interference cancellation (SIC). By considering SIC, the received SINRs at Bob, Carol, and untrusted user are, respectively, given by

\[
\gamma_{R,SIC} = \frac{\rho_{cs} \gamma_b}{1 + a(1 - \rho_{cs}) \gamma_b}, \quad \Psi_0, \quad \Psi_1
\]

\[
\gamma_{C,SIC} = \frac{(1 - \rho_{cs}) \gamma_c}{1 + (1 - a) \rho_{cs} \gamma_c}, \quad \Psi_0
\]

where \(a\) represents the condition of SIC implementation, i.e., for \(|h_{ab}|^2/d_{ab}^\alpha < |h_{ac}|^2/d_{ac}^\alpha\), we set \(a = 1\) and otherwise, \(a = 0\). In this case, the average rate can be written as

\[
\hat{R}_{SIC} = p_q^{(0)} \left[ \log_2(1 + \rho_{cs} \gamma_b) - \log_2(1 + \rho_{cs} \gamma_b) \right] + p_q^{(1)} \left[ \log_2 \left( \frac{\rho_{cs} \gamma_b}{1 + a(1 - \rho_{cs}) \gamma_b} \right) - \log_2 \left( \frac{\rho_{cs} \gamma_u}{1 + (1 - \rho_{cs}) \gamma_u} \right) \right] + p_q^{(1)} \log_2 \left( 1 + \frac{(1 - \rho_{cs}) \gamma_c}{1 + (1 - a) \rho_{cs} \gamma_c} \right) \quad (34)
\]

Therefore, to maximize the average rate subject to the power limitation, covert requirement, secrecy rate constraints, and PD-NOMA transmission, we propose the following optimization problem:

\[
\max_{\rho_{cs}} \hat{R}_{SIC}(\rho_{cs}, \rho_{cs}) \quad (35a)
\]
s.t.: (21b), (21c), (21d), (21e).

In order to solve this optimization problem, we employ the epigraph method [35] and the DC approximation according to Section III-D to convert it to a convex optimization problem. Finally, we can solve the convex optimization by using numerical software such as CVX [36].

IV. PROPOSED OPTIMIZATION WITH IMPERFECT LOCATION AND CHANNEL STATE INFORMATION

In this section, we consider the more practical scenario where Alice has imperfect knowledge of the warden’s location and users’ CSI due to the passive warden and channel estimation errors, respectively.

A. Imperfect Information of Warden’s Location

In a practical system, Alice will need to estimate the distance between herself and the warden, i.e., \(\hat{d}_{aw} = d_{aw} - d_{aw}\) where \(d_{aw}\) is the estimation error. We assume that the distance mismatch lies in a bounded set, i.e., \(\hat{d}_{aw} = [e_{d_{aw}} : |e_{d_{aw}}|^2 \leq \epsilon_d]\), where \(\epsilon_d\) is a known constant. In this case, the summation of the MD and FA probability is given by

\[
p_{t}^{FA} + p_{t}^{MD} = \begin{cases} 1 - e^{\frac{(\theta - \sigma_w^2)^2}{2 \sigma_w^2}} + e^{\frac{(\theta - \gamma_0)}{\gamma_0}}, & \theta - \sigma_w^2 \geq 0 \\ 1, & \theta - \sigma_w^2 < 0 \end{cases} \quad (36)
\]

where \(\gamma_0 = \rho_{cs} \gamma / (\hat{d}_{aw} + e_{d_{aw}})^\alpha\) and \(\gamma_1 = \rho_{cs} \gamma / (\hat{d}_{aw} + e_{d_{aw}})^\alpha\).

In order to maximize the average rate in the imperfect information about warden’s location scenario, we propose the following optimization problem:

\[
\max_{\rho_{cs}, \rho_{cs}} \hat{R}_{SIC}(\rho_{cs}, \rho_{cs}) \quad (37a)
\]
s.t.: (21b), (21c), (21d), (21e).

To solve the optimization problem (37), we present the following lemma.

**Lemma 3:** In our joint ITS and covert system model, the optimal power allocation is the same with both perfect and imperfect information of the warden’s location.
Proof: According to Lemma 1, the optimal power allocation factor in the slot $\Psi_0$ is equal to 1, i.e., $\rho_s = 1$. When $\rho_s = 1$, we have $\psi_0 = P/(d_{au} + e_{dau})^2 = \psi_1 = \psi$, hence, $p_{FA}^{FA} + p_{MD}^{MD}$ can be written as follows:
\[
p_{FA}^{FA} + p_{MD}^{MD} = \begin{cases} 1 - e^{-\frac{(n-\sigma_0^2)}{\nu}} + e^{-\frac{(n-\sigma_0^2)}{\nu}}, & \theta - \sigma_0^2 \geq 0 \\ 1, & \theta - \sigma_0^2 < 0 \end{cases}
\]
(38)
which (39) satisfies (37b).

Finally, to solve (37), we employ epigraph and DC methods similar to Section III-D.

### B. Imperfect CSI Scenario

In practical systems, Alice may also have imperfect CSI of the users due to channel estimation errors. Hence, in this section, we assume Alice has imperfect CSI of Bob, Carol and the untrusted user. Specifically, Alice has an estimated version of channels [36], [37], i.e., $\hat{h}_{ab}$, $\hat{h}_{ac}$, and $\hat{h}_{au}$, and the channel estimation errors are defined as $e_{hab} = h_{hab} - \hat{h}_{hab}$, $e_{hac} = h_{hac} - \hat{h}_{hac}$, and $e_{hua} = h_{hua} - \hat{h}_{hua}$, respectively. Based on the worst-case method, the channel mismatches lie in the bounded set, i.e., $\mathbb{E}_{h_{hab}} = \{e_{hab} : |e_{hab}|^2 \leq \epsilon_b\}$, $\mathbb{E}_{h_{hac}} = \{e_{hac} : |e_{hac}|^2 \leq \epsilon_c\}$, and $\mathbb{E}_{h_{hua}} = \{e_{hua} : |e_{hua}|^2 \leq \epsilon_u\}$, where $\epsilon_b$, $\epsilon_c$, and $\epsilon_u$ are known constants. Therefore, the channel gains from Alice to the users are modeled as follows:
\[
|h_{hab}|^2 = |\hat{h}_{hab} + e_{hab}|^2, |h_{hac}|^2 = |\hat{h}_{hac} + e_{hac}|^2 \tag{40}
\]
\[
|h_{hua}|^2 = |\hat{h}_{hua} + e_{hua}|^2. \tag{41}
\]

In the following, we focus on the worst case performance, in which we maximize the average rate for the worst channel mismatch $e_{hab}$, $e_{hac}$, and $e_{hua}$ in the bounded set $\mathbb{E}_{h_{hab}}$, $\mathbb{E}_{h_{hac}}$, and $\mathbb{E}_{h_{hua}}$, respectively. Hence, the imperfect CSI and imperfect information about the warden's location optimization problem can be formulated as follows:

\[
\max_{\rho_s, \rho_c} \min_{e_{hab}, e_{hac}, e_{hua}} \tilde{R}(\rho_s, \rho_c) \tag{42a}
\]
\[
s.t.: (21b), (21c) \tag{42b}
\]
\[
\begin{align*}
p_q^{(1)} &\left[ \log_2 \left( 1 + \frac{\rho_c \gamma_b}{1 + (1 - \rho_c) \gamma_b} \right) \right] + p_q^{(1)} \left[ \log_2 \left( 1 + \frac{\rho_c \gamma_u}{1 + (1 - \rho_c) \gamma_u} \right) \right] \geq R_{\text{sec}}^{\min} \tag{42d}
\end{align*}
\]
\[
\begin{align*}
&\min_{\theta} \left( p_{MD}^{MD} + p_{FA}^{FA} \right) \geq 1 - \epsilon \tag{42e}
\end{align*}
\]
\[
\begin{align*}
&|e_{hab}|^2 \leq \epsilon_b \tag{42f}
\end{align*}
\]
\[
\begin{align*}
&|e_{hac}|^2 \leq \epsilon_c \tag{42g}
\end{align*}
\]
\[
\begin{align*}
&|e_{hua}|^2 \leq \epsilon_u \tag{42h}
\end{align*}
\]

### C. Proposed Optimization Solution

In order to solve (42), we perform the following two steps: 1) solving the inner minimization and obtain $e_{hab}^*, e_{hac}^*$, and $e_{hua}^*$ and 2) solving the maximization problem according to Section III-D. The inner minimization is formulated as follows:
\[
\min_{e_{hab}^*, e_{hac}^*, e_{hua}^*} \tilde{R}(\rho_s, \rho_c) \tag{43a}
\]
s.t.: (42c), (42d), (42f) - (42h).
\[
\begin{align*}
&|e_{hab}^*|^2 + |e_{hac}^*|^2 + |e_{hua}^*|^2 \leq \left| h_{hab} \right|^2 + \left| e_{hab} \right|^2 \tag{44}
\end{align*}
\]
Likewise, we have this inequality for $h_{hac}$ and $h_{hua}$. By employing these inequalities, we can write the lower bound of the objective function as
\[
\tilde{R}(\rho_s, \rho_c) \geq \tilde{R}(\rho_s, \rho_c) \tag{45}
\]
where
\[
\begin{align*}
\gamma_c^b &\equiv \frac{P|h_{hac}|^2 - \epsilon_c}{d_{ac}^2 \sigma_c^2} \leq \gamma_c \equiv \frac{P|h_{hac}|^2}{d_{ac}^2 \sigma_c^2} \tag{46a}
\end{align*}
\]
\[
\begin{align*}
\gamma_c^u &\equiv \frac{P|h_{hua}|^2 - \epsilon_u}{d_{au}^2 \sigma_u^2} \leq \gamma_u \equiv \frac{P|h_{hua}|^2}{d_{au}^2 \sigma_u^2} \tag{46b}
\end{align*}
\]
\[
\begin{align*}
\gamma_c &\equiv \frac{P|h_{hua}|^2}{d_{au}^2 \gamma_u} \leq \gamma_c \equiv \frac{P|h_{hua}|^2}{d_{au}^2 \gamma_u} \tag{46c}
\end{align*}
\]
Finally, the optimization problem (42) can be rewritten as
\[
\max_{\rho_s, \rho_c} \tilde{R}(\rho_s, \rho_c) \tag{46a}
\]
s.t.: (21b), (21c)
\[
\begin{align*}
p_q^{(1)} &\left[ \log_2 \left( 1 + \frac{\rho_c \gamma_b}{1 + (1 - \rho_c) \gamma_b} \right) \right] + p_q^{(1)} \left[ \log_2 \left( 1 + \frac{\rho_c \gamma_u}{1 + (1 - \rho_c) \gamma_u} \right) \right] \geq R_{\text{sec}}^{\min} \tag{46d}
\end{align*}
\]
\[
\begin{align*}
&|e_{hab} |^2 \leq \epsilon_b \tag{46f}
\end{align*}
\]
\[
\begin{align*}
&|e_{hac} |^2 \leq \epsilon_c \tag{46g}
\end{align*}
\]
\[
\begin{align*}
&|e_{hua} |^2 \leq \epsilon_u \tag{46h}
\end{align*}
\]
Since (46) is in the same form as (21), we can employ epigraph method [35] and DC approximation similar to Section III-D to convert (46) to a convex problem that can be solved using CVX.
V. MULTIPLE ANTENNA ALICE AND BEAMFORMING OPTIMIZATION

In this section, we extend our proposed system model to consider the multiple antenna Alice scenario in which Alice is equipped with \( N_a \) antennas. In this case, Alice can employ beamforming and thus, the average achievable rate is increased. When Alice has \( N_a \) antennas, in slot \( \Psi_0 \), she transmits secure data toward Bob by employing maximum-ratio transmission (MRT) beamforming [13], [14]. While in slot \( \Psi_1 \), she transmits covert data to Carol and secure data to Bob by optimizing the beamforming vectors. Therefore, in this situation, the \( \ell \)th received signal at node \( m \) is given by Therefore, in this situation, the \( \ell \)th received signal at node \( m \) is given by

\[ y_m^\ell = \begin{cases} d_{am}^\alpha/\sqrt{\lambda} \mathbf{h}_m^H \mathbf{w}_{bs} x^\ell_b + n_m^m, & \Psi_0 \\ d_{am}^\alpha + d_{am}^\alpha \mathbf{w}_{ac} \mathbf{w}_{bc}^H + n_m^m, & \Psi_1 \end{cases} \]

where \( \mathbf{h}_{am} \sim \mathcal{CN}(0, \mathbf{I}_{N_a \times 1}) \), \( \mathbf{C}_{am} \) represents the complex Gaussian channel vector from Alice to node \( m \), \( \theta \) is the zero matrix, \( \mathbf{C}_{am} \) is the positive-definite channel covariance matrix between Alice and node \( m \), and \( (.)^H \) is the Hermitian operator. Moreover, \( \mathbf{w}_{bs} \in \mathbb{C}^{N_b \times 1} \) and \( \mathbf{w}_{bc} \in \mathbb{C}^{N_a \times 1} \) are the beamforming vectors for transmission of the secure message in \( \Psi_0 \), the secure message in \( \Psi_1 \), and the covert message in \( \Psi_1 \), respectively. It is worth noting that, since in slot \( \Psi_0 \), Alice only transmits the secure data to Bob, she is able to consider the weight vector \( \mathbf{w}_{bs} = \mathbf{h}_{ab} / \| \mathbf{h}_{ab} \| \), which is the MRT beamformer at Alice toward Bob. The conditional distribution of each symbol of the received signal at the warden given \( h_{aw} \), i.e., \( y_m^\ell | h_{aw} \), is \( y_m^\ell | h_{aw} \sim \mathcal{CN}(0, \sigma_{am}^2 + \mathbf{I}) \) [30], where \( \mathbb{Z} = \left\{ d_{am}^\alpha \mathbf{w}_{sb}^H \mathbf{h}_{aw}, d_{am}^\alpha \| \mathbf{w}_{sb} \| \| \mathbf{h}_{aw} \|, d_{am}^\alpha \| \mathbf{w}_{sb} \| \| \mathbf{h}_{aw} \| \right\} \) [25]. Hence, the PDF of \( \mathbb{Z} \) is

\[ f_\psi(\mathbb{Z}) = \begin{cases} \frac{1}{\psi_0^\ell} e^{-\frac{\psi_0^\ell}{\psi_0}}, & \Psi_0 \\ \frac{1}{\psi_1^\ell} e^{-\frac{\psi_1^\ell}{\psi_1}}, & \Psi_1 \end{cases} \]

where \( \psi_0 = d_{am}^\alpha \mathbf{w}_{sb}^H \mathbf{C}_{aw} \mathbf{w}_{bs} \) and \( \psi_1 = d_{am}^\alpha \mathbf{w}_{sb}^H \mathbf{C}_{aw} \mathbf{w}_{bc} \). It is assumed that the antenna separation is sufficient such that the covariance matrices are diagonal; hence

\[ \psi_0 = \operatorname{Tr} \left( d_{am}^\alpha \mathbf{w}_{sb}^H \mathbf{C}_{aw} \mathbf{w}_{sb} \right) = d_{am}^\alpha \mathbf{w}_{sb}^H \mathbf{C}_{aw} \mathbf{w}_{sb} \]

Finally, by invoking (48), \( p_t^{FA} + p_t^{MD} \) can be written as

\[ p_t^{FA} + p_t^{MD} = \left\{ \begin{array}{ll} 1 - e^{-\frac{(\theta_{ab}^2 - \theta)}{2\sigma_{aw}^2}}, & \theta - \sigma_{aw}^2 \geq 0 \\ 1, & \theta - \sigma_{aw}^2 < 0 \end{array} \right. \] (50)

The average rate in this case can be written as

\[ \tilde{R} = E_q \left[ \hat{R} \right] = p_q^{(0)} \left[ \log_2 \left( 1 + \frac{d_{ab}^\alpha \| \mathbf{w}_{sb} \| \| \mathbf{h}_{aw} \|^2}{2\sigma_b^2} \right) \right]^{+} \]

In order to maximize the average rate subject to the power limitation, covert communication requirement, and secrecy rate constraints, we propose the following optimization problem:

\[ \max_{\mathbf{w}_{bc}, \mathbf{w}_{ab}} \tilde{R}(\mathbf{w}_c, \mathbf{w}_b, \rho_{ab}) \]

s.t.: \( \operatorname{Tr}(\mathbf{w}_b \mathbf{w}_b^H) + \operatorname{Tr}(\mathbf{w}_c \mathbf{w}_c^H) = P \)

\[ p_q^{(0)} \left[ \log_2 \left( 1 + \frac{d_{ab}^\alpha \| \mathbf{w}_{sb} \| \| \mathbf{h}_{aw} \|^2}{2\sigma_b^2} \right) \right]^{+} \]

Finally, by employing the semidefinite relaxation (SDR) [40] and epigraph methods [35], (52) can be rewritten as follows:

\[ \max_{\mathbf{w}_c, \mathbf{w}_b, \eta} \tilde{R}(\mathbf{w}_c, \mathbf{w}_b, \eta) \]

s.t.: \( \operatorname{Tr}(\mathbf{w}_b) + \operatorname{Tr}(\mathbf{w}_c) = P \)
Table I

| Parameter       | Value     |
|-----------------|-----------|
| 1−ε            | 0.9       |
| d_{au}         | 5 meters (m) |
| d_{ac}         | 5 m       |
| α              | 4         |
| $P_{min}$      | 0.5 bps/Hz |
| $P_{min}$      | 0.1 bps/Hz |
| $P_{q_{1}}$    | 0.5       |

between Alice and Carol. The distance parameters are listed in Table I.

In the numerical results, the considered simulation requirement typically assumes a low data rate user. If both higher minimum data rate compared to Carol since the covert solution. In the simulations, we assume that Bob requires a higher minimum data rate transmission, further security strategies such as beamforming [39] may be employed at Alice. In the numerical results, the considered simulation parameters are listed in Table I.

Fig. 2 illustrates the average rate versus the distance between Alice and Carol. The figure shows that the distance of the received noise power at Carol on the average rate is increasing. Moreover, this figure shows the impact of the average rate increases. When the distance between Alice and Carol is increased, Alice cannot proportionately increase the transmit power $P_{ac}$ due to the covert communication requirement to minimize detection by the warden. Moreover, since Alice transmits data with total available power, i.e., $P$ in the secrecy slots $\Psi_0$, decreasing the distance between Alice and Bob $d_{ab}$ has less effect on the average rate. Since we apply the DC method to approximate the optimization problem (24) to a convex one, it is necessary to compare our proposed solution with the optimal solution by employing the exhaustive search method and finding the optimality gap. As seen in Fig. 2, the optimality gap is approximately 5% which highlights the efficiency of our proposed analysis.

Fig. 3 shows the average rate versus the total transmit power. As seen in this figure, by increasing total transmit power, the average rate increases. Moreover, this figure shows the impact of the received noise power at Carol on the average rate is higher than the impact of the received noise power at Bob on the average rate. Similar to Fig. 2, we see that the covert requirement has a higher impact on the average rate compared to the distance between Alice and Bob. For example, by decreasing $d_{ac}$ from 3 to 1 m the average rate increases on average approximately 39%, while by decreasing $d_{ab}$ from 3 to 1 m the average rate increases on average approximately 37%. When the distance between Alice and Carol is increased, Alice cannot proportionately increase the transmit power $P_{ac}$, due to the covert communication requirement to minimize detection by the warden. Moreover, since Alice transmits data with total available power, i.e., $P$ in the secrecy slots $\Psi_0$, decreasing the distance between Alice and Bob $d_{ab}$ has less effect on the average rate. Since we apply the DC method to approximate the optimization problem (24) to a convex one, it is necessary to compare our proposed solution with the optimal solution by employing the exhaustive search method and finding the optimality gap. As seen in Fig. 2, the optimality gap is approximately 5% which highlights the efficiency of our proposed analysis.

VI. NUMERICAL RESULTS

In this section, we present numerical results to evaluate the performance of our proposed system model and optimization solution. In the simulations, we assume that Bob requires a higher minimum data rate compared to Carol since the covert requirement typically assumes a low data rate user. If both Bob and Carol require high data rate transmissions, further security strategies such as beamforming [39] may be employed at Alice. In the numerical results, the considered simulation parameters are listed in Table I.

Fig. 2 illustrates the average rate versus the distance between Alice and Carol. The figure shows that the distance...
highlight the sensitivity of Carol’s channel estimation error on the achievable rate. Moreover, note that the imperfect CSI scenario (in all three cases) provides lower $\rho_{cs}$. This means that the covert transmit power decreases when the secrecy transmit power increases.

Fig. 5 plots the average rate versus the distance between Alice and Carol. Moreover, this figure evaluates the impact of SIC implementation on the average rate for the special case when both Carol and Bob know the covert strategy. As seen in this figure, when Carol and Bob know which time slot will be used for the covert message and perform SIC, the average rate is increased by approximately 5%. As such, the figure shows that there is a fundamental tradeoff between the cost of Bob’s access to Alice’s preshared secret and increase in the average rate.

In Fig. 6, we evaluate the effect of data transmission probability for Carol ($p_q^{(1)}$) on the achievable rate. As seen, by increasing $p_q^{(1)}$, the average secrecy rate decreases. This is because, by increasing $p_q^{(1)}$, the selected time slots for transmitting the covert message to Carol increases, which leads to more interference at Bob and consequently, the average secrecy rate is decreased. Hence, for high values of $p_q^{(1)}$ (approximately 0.6 and above), Alice reduces the covert signal power to be able to satisfy the secure communication rate requirements ($R_{sec}$). Consequently, we observe the average covert rate is a decreasing function with respect to $p_q^{(1)}$ for high values of $p_q^{(1)}$.

In Fig. 7, the average rate versus the number of Alice antennas is plotted. This figure evaluates the impact of employing the beamforming technique on the average rate. The figure also illustrates the superiority of our proposed beamforming compared to the random antenna selection technique. In random antenna selection, Alice selects an antenna among $N_a$ available
antennas randomly. As observed, the proposed beamforming technique achieves a secrecy performance that is 30% higher than random antenna selection.

VII. CONCLUSION

This article investigates joint ITS and covert communican in a SIMO network, where a source communicates with two legitimate users in the presence of one untrusted user and a warden. While one of the users requests secure communication, the other user needs covert communication. For this system model, we presented an optimization problem with the aim of maximizing the average rate subject to a covert communication requirement and an ITS rate constraint. To solve the problem, the successive convex approximation method was adopted to convexify the optimization. We then considered a practical system where the location of the warden and the CSIs of users are imperfectly known. Moreover, we extended our proposed system model to multiple antenna Alice scenario and found beamforming vectors so that maximize average rate. Our numerical examples reveal the impact of network topology and the joint ITS and covert design on the average rate.

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.
[2] N. Yang, L. Wang, G. Geraci, M. Elksahlshian, J. Yuan, and M. D. Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.
[3] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1367, Oct. 1975.
[4] A. Khisti and G. Wornell, “Secure transmission with multiple antennas—Part II: The MISO/MIMO wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[5] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part I: The MISO/MIMO wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[6] T. Lv, H. Gao, and S. Yang, “Secrecy transmit beamforming for heterogeneous networks,” IEEE J. Sel. Areas Commun., vol. 33, no. 6, pp. 1154–1170, Jun. 2015.
[7] N. Yang, P. L. Yehoh, M. Elkashian, R. Schober, and I. B. Collings, “Transmit antenna selection for security enhancement in MIMO wiretap channels,” IEEE Trans. Commun., vol. 61, no. 1, pp. 144–154, Jan. 2013.
[8] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, Jun. 2012.
[9] H. M. Wang, F. Liu, and M. Yang, “Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems,” IEEE Trans. Veh. Technol., vol. 64, no. 10, pp. 4893–4898, Oct. 2015.
[10] M. Forouzesh, P. Azmi, and N. Mokari, “Reduce impact of false detection of adversary states on the secure cooperative network,” in Proc. Int. Symp. Telecommun. (IST), Tehran, Iran, Mar. 2016, pp. 261–265.
[11] T. Lv, Y. Yin, Y. Lu, S. Yang, E. Liu, and S. Clapworthy, “Physical detection of misbehavior in relay systems with unreliable channel state information,” IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1517–1530, Jul. 2018.
[12] L. Wang, M. Elkashian, and J. Huang, “Secure transmission with optimal power allocation in untrusted relay networks,” IEEE Wireless Commun. Lett., vol. 3, no. 3, pp. 289–292, Jun. 2014.
[13] A. Kuhestani, A. Mohammadi, and M. Mohammadi, “Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers,” IEEE Trans. Inf. Forensics Security, vol. 13, pp. 341–355, 2018.
[14] A. Kuhestani, A. Mohammadi, K. K. Wong, P. L. Yehoh, M. Moradikia, and M. R. Khandaker, “Optimal power allocation by imperfect hardware analysis in untrusted relaying networks,” IEEE Trans. Wireless Commun., vol. 17, no. 7, pp. 4302–4314, Jul. 2018.
[15] M. Letafati, A. Kuhestani, and H. Behrozhi, “Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2856–2868, 2020.
[16] Y. Zhang, H. Wang, Q. Yang, and Z. Ding, “Secrecy sum rate maximization in non-orthogonal multiple access,” IEEE Commun. Lett., vol. 20, no. 5, pp. 930–933, May 2016.
[17] Y. Liu, Z. Qin, M. Elkashian, Y. Gao, and L. Hanzo, “Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks,” IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[18] M. Forouzesh, P. Azmi, N. Mokari, K. K. Wong, and H. Pishro-Nik, “Robust physical layer security for power domain non-orthogonal multiple access-based HetNets and HUDNs: SIC avoidance at eavesdroppers,” IEEE Access, vol. 7, pp. 107879–107896, 2019.
[19] Z. Liu, J. Liu, Y. Zeng, and J. Ma, “Covert wireless communication in IoT network: From AWGN channel to THz band,” IEEE Internet Things J., vol. 7, no. 4, pp. 3378–3388, Apr. 2020.
[20] Z. Liu, J. Liu, Y. Zeng, and J. Ma, “Covert wireless communications in IoT systems: Hiding information in interference,” IEEE Wireless Commun., vol. 25, no. 6, pp. 46–52, Dec. 2018.
[21] H. Wang, Y. Zhang, X. Zhang, and Z. Li, “Secrecy and covert communications against UAV surveillance via multi-hop networks,” IEEE Trans. Commun., vol. 68, no. 1, pp. 389–401, Jan. 2020.
[22] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, “Joint optimization of a UAV’s trajectory and transmit power for covert communications,” IEEE Trans. Signal Process., vol. 67, no. 16, pp. 4276–4290, Aug. 2019.
[23] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, “Covert communication with the help of relay and channel uncertainty,” IEEE Wireless Commun. Lett., vol. 8, no. 1, pp. 317–320, Feb. 2019.
[24] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, “Covert communication achieved by a greedy relay in wireless networks,” IEEE Trans. Wireless Commun., vol. 17, no. 7, pp. 4766–4779, Jul. 2018, doi: 10.1109/TWC.2018.2831217.
[25] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yehoh, “Covert communication and security transmission over untrusted relaying networks in the presence of multiple warden,” IEEE Trans. Commun., vol. 68, no. 6, pp. 3737–3749, Jun. 2020, doi: 10.1109/TCOMM.2020.2978206.
[26] M. Forouzesh, P. Azmi, and A. Kuhestani, “Covert transmission with covert requirement in untrusted relaying networks,” in Proc. 9th Int. Symp. Telecommun. (IST), Tehran, Iran, Dec. 2018, pp. 670–675.
[27] Y. Jiang, L. Wang, and H. Chen, “Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission,” IEEE Trans. Veh. Technol., vol. 69, no. 3, pp. 2980–2992, Mar. 2020, doi: 10.1109/TVT.2019.2966358.
[28] W. Kim, J. Park, J. Jo, and H. Lim, “Covert jamming using fake ACK frame injection on IEEE 802.11 wireless LANs,” IEEE Wireless Commun. Lett., vol. 8, no. 5, pp. 1502–1505, Oct. 2019.
Moslem Forouzesh (Student Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2016 and 2020, respectively. His current research interests include nonorthogonal multiple access, radio resource allocation in wireless networks, physical-layer security, and covert communication.

Paeiz Azmi (Senior Member, IEEE) was born in Tehran, Iran, in April 1974. He received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Sharif University of Technology, Tehran, in 1996, 1998, and 2002, respectively. From 1999 to 2001, he was with the Advanced Communication Science Research Laboratory, Iran Telecommunication Research Center, Tehran, where he was with the Signal Processing Research Group, from 2002 to 2005. Since September 2002, he has been with the Electrical and Computer Engineering Department, Tarbiat Modares University, Tehran, where he became an Associate Professor, in January 2006, and is currently a Full Professor. His current research interests include modulation and coding techniques, digital signal processing, wireless communications, radio resource allocation, molecular communications, and estimation and detection theories.

Ali Kuhestani (Member, IEEE) received the Ph.D. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2017. From 2018 to 2019, he was a Postdoctoral Researcher with the Department of Electrical Engineering, Sharif University of Technology, Tehran. He has authored and coauthored more than 20 journals in prestigious publication avenues (e.g., the IEEE and IET) and more than ten papers in major conference proceedings. His research interests include physical-layer security of wireless communications, Internet of Things, millimeter-wave communication, massive MIMO system, and space-time coding.

Dr. Kuhestani was a recipient of the Iran’s National Elites Foundation Award for outstanding students in 2017. He was a reviewer of the IEEE transactions/journals and conferences.