This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2684221, IEEE Internet of Things Journal

Security-Aware Waveforms for Enhancing Wireless Communications Privacy in Cyber-Physical Systems via Multipath Receptions

Qian Xu, Pinyi Ren, Houbing Song, and Qinghe Du

***Abstract*—Cyber-Physical System (CPS), regarded as the next generation of engineered system, has the capability to interact with the real physical world. Applications of CPS span various fields such as medical monitoring, traffic control, and smart grid. With such widespread applications, privacy assurance is becoming more and more important since what the CPS connects are people and the real world. Any leakage of private information will cause serious consequences. In this paper, we focus on enhancing the secrecy of wireless communications in CPS by use of physical layer security techniques. Specifically, we study an amplify and forward (AF) relay network where all devices are equipped with a single antenna. We propose a privacy-enhanced waveform design approach aided by artificial noise (AN) to enhance the communication secrecy in a wireless environment with multipath receptions. First, we consider the case with perfect eavesdropper's channel state information (CSI). We optimize the AF coefficient for forwarding the information-bearing signal and the AN covariance to maximize the achievable secrecy rate. The optimal solution is obtained by solving a series of semidefinite programs (SDPs). Then, a more practical scenario with imperfect eavesdropper's CSI is studied. We develop a robust waveform design method and obtain the lower bound of the achievable secrecy rate. Numerical results are presented to show the effectiveness of our proposed algorithms.**

***Index Terms*—Cyber-Physical System (CPS), wireless communications, privacy, physical layer security, waveform design, relay transmission.**

I. Introduction

A. Background

Cyber-Physical System (CPS) is an integration of computation, networking, and physical processes. As suggested by its name, CPS is mainly composed of two components, a physical process and a cyber system [1]. The physical elements in CPS are controlled by the cyber system, which consists of a variety of physical objects possessing sensing, computing, and communication capabilities, to do real-time monitoring and processing. CPS is such an intelligent system that it can interact with the real physical world based on the data acquired from the physical world. Applications of CPS span various fields from people's daily lives to a nation's critical infrastructure. They include medical monitoring [2], traffic control, automotive systems, electric power generation and distribution networks, water and gas distribution networks, advanced communication networks [3], etc. There is no doubt that such system will bring us much greater economic and societal benefits than what the information technology (IT) revolution has achieved in the last century.

CPS has aroused great interest in both industry and academia. The US National Science Foundation (NSF) has regarded CPS as a key research area in 2006 [4]. The German federal government proposed the Industrie 4.0 project in 2013 and one of the three key components is CPS [5]. In the academic domain, large number of research efforts have been devoted to the design of CPS [6], [7] and most of them concentrate on providing robust and efficient CPS applications in different environments [8]–[10]. In [8], a multicast routing protocol was proposed for networking decentralized sensors and controllers of CPS to stabilize the voltage of the smart grid. In [9], the authors proposed a novel service scheduling scheme in vehicular CPS by taking human factors into consideration. The authors in [10] investigated the challenges and opportunities for water CPS from four critical aspects. Although major research works are devoted to improving reliability and efficiency of CPS, the security and privacy issues in the CPS [11]–[14] should be addressed first before the widespread deployment of CPS. Compared with the traditional Internet, the security and privacy requirement of CPS is much higher since what the CPS monitors are the real-world physical processes [15]. Any kinds of faults or information leakage will result in serious consequences. For example, for the CPS application in the smart grid, malicious activities will cause power blackouts or socket bombing attacks [1].

B. Related Work

The basic security requirements of CPS include robustness to unpredictable conditions, self-healing capabilities, and appropriate assurances in terms of authentication, integrity, service availability, and non-repudiation of the information flows [16]. However, different kinds of external malicious attacks are threatening the security of CPS, such as denial-of-service (DoS) attack and false-data injection (FDI) attack. Several researches have been conducted to defeat specific attacks

Qian Xu, Pinyi Ren, and Qinghe Du are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, and also with the Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an Jiaotong University, China (e-mails: xq1216@stu.xjtu.edu.cn; pyren@mail.xjtu.edu.cn; duqinghe@mail.xjtu.edu.cn). Houbing Song is with the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, USA (e-mail: h.song@ieee.org).

Corresponding author: Pinyi Ren (email: pyren@mail.xjtu.edu.cn).

The research work reported in this paper is supported by the National Natural Science Foundation of China under the Grant No. 61431011 and the Grant No. 61671371, the National Science and Technology Major Project under Grant No. 2016ZX03001016-005, the Science and Technology Program of Shaanxi Province under the Grant No. 2016KW-032, and the Fundamental Research Funds for the Central Universities.

on specific CPS applications [17]–[19]. Reference [17] studied the real-time detection of DoS attacks in vehicular networks under the random jamming attack and on-off jamming attack. In [18], the optimal FDI attack strategy and the corresponding two defense schemes were proposed. In [19], the authors studied the effect of replay attacks on a control system and proposed a detection method.

Apart from the aforementioned security requirements, privacy or secrecy is also an essential characteristic of a trustworthy CPS. Privacy issues in CPS mainly refer to the leakage of personal sensitive information. The main reason for information leakage is that the CPS highly depends on the communication networks and heterogeneous IT elements [20]. Furthermore, the widely used wireless communications in CPS make the confidential information much more vulnerable to eavesdropping attack. The traditional anti-eavesdropping strategy is based on the cryptographic encryption [21]. However, with the enhancement of eavesdroppers' computing capabilities, the encryption method faces an increasing risk of information leakage. Moreover, the management and distribution of the secret keys often require complex protocols and architectures, which makes the cryptographic method difficult to be applied in the CPS especially the Internet of Things (IoT) with distributed resource-constrained devices [20], [22].

As a contrast, physical layer security (PLS) is a technique which can achieve perfect secrecy without requiring any preshared secret keys. It utilizes the inherent randomness and difference of wireless links to protect the confidential message regardless of eavesdroppers' computation power. Since PLS is agnostic to the system infrastructures, it shows great potential in guaranteeing the secrecy in CPS. The concept of PLS can date back to Wyner's work [23] in 1975. Wyner proposed the well-known wiretap channel model and the idea of secrecy capacity. The work of Wyner was then extended to the broadcast channel with confidential messages [24]. Furthermore, the secrecy capacity in the Gaussian broadcast channel was studied in [25]. Based on the previous theoretical studies of PLS, a series of transmission schemes have been proposed to improve transmission secrecy [26]–[32]. Among these schemes, nodes cooperation and multi-antenna signal processing [33], [34] are the two frequently used techniques. The authors in [29] considered a cooperative network where one node is selected as relay and one node is selected as jammer. They proposed a node selection scheme aiming at minimizing the secrecy outage probability. In [30] and [31], the authors further improved the transmission secrecy by employing multiple cooperative relays to form a virtual antenna array. For the multi-antenna scenarios, various signal processing techniques such as beamforming, precoding, and artificial noise (AN) are employed in the multiple-input single-output (MISO) case or the full-fledged multiple-input multiple-output (MIMO) case [32].

II. Motivation and Contribution

As aforementioned, PLS is a promising technique in handling the privacy problem in CPS due to its independence from secret keys. However, several new issues occur when applying PLS in CPS. First, the transmission protocols should be as simple as possible since most physical elements in CPS are managed in a distributed manner. Hence, the multi-relay-aided coordinated transmissions like [30] and [31] are inapplicable due to the requirement of complex control messages. Second, although multi-antenna techniques such as precoding combined with power allocation [35], [36] can effectively control the direction of the signal beam and manage the interference among users, a massive deployment of multi-antenna devices in CPS is costly, which may block the path to the widespread use of CPS in the industrial production. Consequently, more attention should be paid to the privacy-preserving technique targeting at the single antenna system with simple transmission protocols. Up to now, lots of researches have been done concerning the information secrecy of single-input single-output (SISO) system [37]–[40]. The authors in [37] proposed a fountain-coding-aided secure transmission protocol and the noise aggregation scheme was proposed in [38]. The authors in [39] and authors in [40] improved the transmission secrecy by exploiting the multipath transmission environment.

In this paper, we concentrate on the confidential message transmission from a source (e.g., wearable medical device) to a destination (e.g., doctor's smartphone) in a medical CPS. Due to the lack of direct source-destination link, one pre-selected relay is employed to help forward the message. During the transmission, an eavesdropper is attempting to extract this confidential message. We try to enhance the security of this relay network by performing security-aware waveform design. Unlike [39], we consider a more practical scenario where the destination uses the maximum ratio combining (MRC) receiver, the complexity of which is much lower than the minimum mean square error (MMSE) receiver in [39]. What's more, we also study the robust waveform design with imperfect eavesdropper's channel state information (CSI). The main contributions of this paper can be summarized as follows:

1) The secure relay-aided SISO transmission is studied in terms of waveform design for the first time. The relay uses an AN-aided amplify-and-forward (AF) protocol to forward the confidential message.
2) With perfect CSIs of legitimate links and the eavesdropping link, we optimize the AF coefficient for information-bearing signal and the AN covariance to maximize the achievable secrecy rate. The optimal solution is obtained through convex optimization.
3) With imperfect CSI of the eavesdropping link, to make the problem tractable we enlarge the space of estimation error which strengthens the CSI uncertainty constraint. Then we transform the secrecy rate maximization problem into a semidefinite program (SDP) and obtain the optimal robust AF coefficient and AN covariance. Since the uncertainty constraint has been strengthened, the maximum achievable secrecy rate after optimization is actually the lower bound of the original problem.

The rest of this paper is organized as follows. Section III presents the system model and formulates the secrecy rate maximization problem. Section IV solves the optimization problem with the assumption of perfect CSIs of both legit-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2684221, IEEE Internet of Things Journal

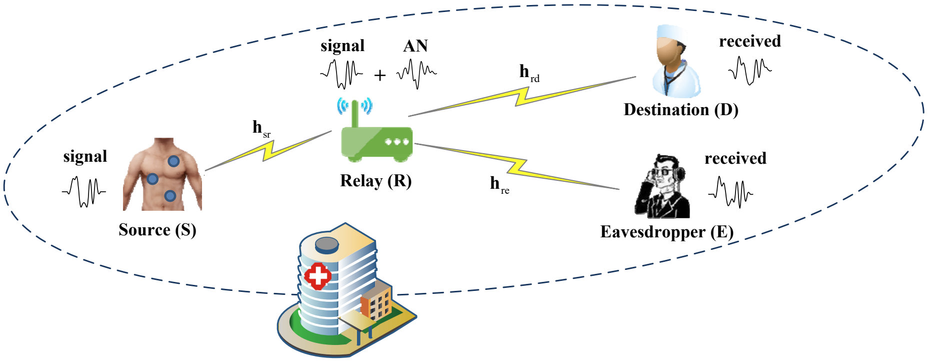


Fig. 1. System model: the source node S is transmitting a confidential message to the destination node D with the help of a relay R. An eavesdropper is trying to intercept the message.

imate links and the eavesdropping link. Section V studies the optimization problem with imperfect CSI of the eavesdropping link. Section VI presents some numerical examples. Finally, the paper concludes with Section VII.

Notations: In this paper, we use bold upper- and lower-case letters to denote matrices and vectors, respectively. We use $\mathbb{C}^{M\times N}$ and $\mathbb{T}^{M\times N}$ to denote the space of $M \times N$ complex matrices and complex Toeplitz matrices, respectively. $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Omega})$ means that the random vector $\mathbf{x}$ follows a complex circular Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Omega}$. $\mathbf{x}(n)$ represents the nth component of the vector $\mathbf{x}$. $\mathbf{A}^{(i,j)}$ represents the element at the ith row and jth column of matrix $\mathbf{A}$, and $\mathbf{A}^{(:,j)}$ represents the jth column of matrix $\mathbf{A}$. $\mathbf{I}$ denotes an identity matrix. $\mathbf{A}^T$, $\mathbf{A}^H$ and $\mathrm{Tr}(\mathbf{A})$ represent the transpose, Hermitian transpose, and trace of a matrix, respectively. $\mathbf{A} \succeq \mathbf{0}$ means that $\mathbf{A}$ is a Hermitian positive semidefinite matrix. $\|\cdot\|$ and $\|\cdot\|_F$ represent the l_2 norm and Frobenius norm, respectively. $x(t) * y(t)$ represents the convolution of continuous signals $x(t)$ and $y(t)$. $y = [x]^+$ means $y = \max\{x, 0\}$.

III. System Model

We consider the privacy issue of the wireless communication part of a medical CPS as illustrated in Fig. 1. The source node S, e.g., wearable medical device, needs to transmit the measurement data of a patient to the destination node, e.g., a doctor's smartphone. Due to the absence of the source-destination link, a relay is employed to help forward the message. Nearby the doctor, there exists an eavesdropper (a registered user without permission to acquire the data) who attempts to intercept the source information. We assume that there is no source-eavesdropper link either[1], since the eavesdropper is close to the destination. All the nodes in the aforementioned network are equipped with a single antenna. Unlike other researches, in this paper we consider the multipath transmission environment. It is expected that about 95% of traffic will be indoor communications [41] and indoor environment possesses richer multipath resources.

With only a single antenna, any multi-antenna processing techniques are not allowed. Thus, the source and the relay attempt to use carefully designed waveform to protect the confidential message. According to [39], the transmitted signal at the source can be written as

$$x_{\mathrm{s}}(t) = \sum_{k=0}^{\infty} \sqrt{E_{\mathrm{s}}} b(k) s(t - kT), \tag{1}$$

where $b(k) \sim \mathcal{CN}(0, 1)$ is the coded confidential symbol, T is the duration time of one symbol, E_{s} represents the total transmit energy for one symbol, and $s(t)$ is the complex continuous waveform with unit energy given by

$$s(t) = \sum_{n=0}^{N-1} \mathbf{s}(n)\psi(t - nT_c), \tag{2}$$

where N is the number of pulse for one symbol, $\mathbf{s}(n) \in \mathbb{C}$, $n = 0, 1, ..., N–1$ are the coefficients to be optimized, and $\psi(t)$ is the pre-given unit energy pulse shaper (e.g., ideal square pulse or raised cosine pulse) with duration $T_c = T/N$. Without loss of generality, we assume $T_c = 1$ in the following analyses.

After the transmission over a multipath channel $\mathbf{h}_{\mathrm{sr}} = [h_{\mathrm{sr},1}, ..., h_{\mathrm{sr},L_{\mathrm{r}}}]^T$ with L_{r} resolvable multipaths, the received signal at the relay is

$$y_{\mathrm{r}}(t) = h_{\mathrm{sr}}(t) * x_{\mathrm{s}}(t) + n_{\mathrm{r}}(t), \tag{3}$$

where $n_{\mathrm{r}}(t)$ is the white Gaussian noise.

The relay adopts the AN-aided AF (AN-AF) protocol to forward the message. That is, besides using some energy to retransmit the received signal as the AF protocol does, the relay also injects randomly generated AN into the transmitted signal. Thus, the transmitted signal at the relay is

$$x_{\mathrm{r}}(t) = \sqrt{A} y_{\mathrm{r}}(t) + z(t), \tag{4}$$

where $\sqrt{A}$ represents the AF coefficient for forwarding $y_{\mathrm{r}}(t)$ and $z(t)$ is the AN signal given by

$$z(t) = \sum_{m=0}^{M_{\mathrm{r}}-1} \mathbf{z}(m)\psi(t - mT_c), \tag{5}$$

where $M_{\mathrm{r}} = N + L_{\mathrm{r}} - 1$ and $\mathbf{z} \in \mathbb{C}^{M_{\mathrm{r}}\times 1}$ is the AN vector following $\mathcal{CN}(\mathbf{0}, \boldsymbol{\Omega}_z)$ distribution.

[1] The focus of our work is introducing the security-enhanced waveform design method in relay networks. Hence, we only consider this simple but widely used scenario like [29], [31]. It is our future work to handle the more complicated settings of eavesdroppers.

The relay-destination link $\mathbf{h}_{\mathrm{rd}} = [h_{\mathrm{rd},1}, ..., h_{\mathrm{rd},L_{\mathrm{d}}}]^T$ and the relay-eavesdropper link $\mathbf{h}_{\mathrm{re}} = [h_{\mathrm{re},1}, ..., h_{\mathrm{re},L_{\mathrm{e}}}]^T$ are assumed to have L_{d} and L_{e} resolvable multipaths, respectively. The received signals at the destination and the eavesdropper are

$$\begin{aligned} & y_{\mathrm{d}}(t) \\ & = \sqrt{A} h_{\mathrm{rd}}(t) * \Big(h_{\mathrm{sr}}(t) * x_{\mathrm{s}}(t) + n_{\mathrm{r}}(t)\Big) + h_{\mathrm{rd}}(t) * z(t) + n_{\mathrm{d}}(t) \end{aligned} \quad (6)$$

and

$$\begin{aligned} & y_{\mathrm{e}}(t) \\ & = \sqrt{A} h_{\mathrm{re}}(t) * \Big(h_{\mathrm{sr}}(t) * x_{\mathrm{s}}(t) + n_{\mathrm{r}}(t)\Big) + h_{\mathrm{re}}(t) * z(t) + n_{\mathrm{e}}(t), \end{aligned} \quad (7)$$

respectively.

After the matched filtering by using $\psi(t)$ over an extended signal with $M_{\mathrm{d}} = M_{\mathrm{r}} + L_{\mathrm{d}} - 1$ pulses, the signal vector $\mathbf{y}_{\mathrm{d}}(k) \in \mathbb{C}^{M_{\mathrm{d}} \times 1}$ for symbol $b(k)$ at the destination can be written as

$$\mathbf{y}_{\mathrm{d}}(k) = \sqrt{AE_{\mathrm{s}}} b(k) \mathbf{H}_{\mathrm{rd}} \mathbf{H}_{\mathrm{sr}} \mathbf{s} + \sqrt{A} \mathbf{H}_{\mathrm{rd}} \mathbf{n}_{\mathrm{r}} + \mathbf{H}_{\mathrm{rd}} \mathbf{z} + \mathbf{n}_{\mathrm{d}}, \quad (8)$$

where $\mathbf{n}_{\mathrm{r}}$ and $\mathbf{n}_{\mathrm{d}}$ are the additive white Gaussian noise following the $\mathcal{CN}(\mathbf{0}, \mathbf{I})$ distribution, $\mathbf{H}_{\mathrm{sr}} \in \mathbb{C}^{M_{\mathrm{r}} \times N}$ and $\mathbf{H}_{\mathrm{rd}} \in \mathbb{C}^{M_{\mathrm{d}} \times M_{\mathrm{r}}}$ are the Toeplitz matrixes with each column vector being the shifted version of $\mathbf{h}_{\mathrm{sr}}$ and $\mathbf{h}_{\mathrm{rd}}$, respectively. Note that in (8) we have omitted the inter-symbol-interference (ISI) due to the same assumption in [39] that the number of resolvable multipaths is much less than the number of pulses for one symbol, which means that the application of interest here is the system with high sampling rate and low baud rate.

Similarly, the received signal vector at the eavesdropper is

$$\mathbf{y}_{\mathrm{e}}(k) = \sqrt{AE_{\mathrm{s}}} b(k) \mathbf{H}_{\mathrm{re}} \mathbf{H}_{\mathrm{sr}} \mathbf{s} + \sqrt{A} \mathbf{H}_{\mathrm{re}} \mathbf{n}_{\mathrm{r}} + \mathbf{H}_{\mathrm{re}} \mathbf{z} + \mathbf{n}_{\mathrm{e}}, \quad (9)$$

where $\mathbf{H}_{\mathrm{re}} \in \mathbb{C}^{M_{\mathrm{e}} \times M_{\mathrm{r}}}$ is the Toeplitz matrixes with each column vector being the shifted version of $\mathbf{h}_{\mathrm{re}}$ and $M_{\mathrm{e}} = M_{\mathrm{r}} + L_{\mathrm{e}} - 1$.

For information detection, considering the complexity factor we assume that the destination adopts the MRC receiver which does not need to collect the statistics of the transmitted signal. Thus, the receiving filter is $\mathbf{w} = \mathbf{H}_{\mathrm{rd}} \mathbf{H}_{\mathrm{sr}} \mathbf{s} / \|\mathbf{H}_{\mathrm{rd}} \mathbf{H}_{\mathrm{sr}} \mathbf{s}\|$ and the signal-to-interference-plus-noise ratio (SINR) at the destination is given by

$$\gamma_{\mathrm{d}} = \frac{AE_{\mathrm{s}} \|\mathbf{w}^H \mathbf{H}_{\mathrm{rd}} \mathbf{H}_{\mathrm{sr}} \mathbf{s}\|^2}{\mathbf{w}^H \left(A \mathbf{H}_{\mathrm{rd}} \mathbf{H}_{\mathrm{rd}}^H + \mathbf{H}_{\mathrm{rd}} \mathbf{\Omega}_z \mathbf{H}_{\mathrm{rd}}^H + \mathbf{I}\right) \mathbf{w}}. \quad (10)$$

We consider a worst case for legitimate users that the eavesdropper adopts the MMSE receiver which is the linear maximum SINR filter. Thus, the SINR at the eavesdropper is

$$\gamma_{\mathrm{e}} = AE_{\mathrm{s}} \left(\mathbf{H}_{\mathrm{re}} \mathbf{H}_{\mathrm{sr}} \mathbf{s}\right)^H \mathbf{R}_{\mathrm{e}}^{-1} \mathbf{H}_{\mathrm{re}} \mathbf{H}_{\mathrm{sr}} \mathbf{s} \quad (11)$$

with

$$\mathbf{R}_{\mathrm{e}} = A \mathbf{H}_{\mathrm{re}} \mathbf{H}_{\mathrm{re}}^H + \mathbf{H}_{\mathrm{re}} \mathbf{\Omega}_z \mathbf{H}_{\mathrm{re}}^H + \mathbf{I}. \quad (12)$$

According to [42], the achievable secrecy rate of this relay transmission is

$$C_s = \frac{1}{2} \left[C_{\mathrm{d}} - C_{\mathrm{e}}\right]^+ = \frac{1}{2} \left[\log_2(1+\gamma_{\mathrm{d}}) - \log_2(1+\gamma_{\mathrm{e}})\right]^+. \quad (13)$$

We aim to maximize the secrecy rate by carefully designing the waveforms of the two-hop transmission. The optimal strategy is the joint optimization of $\mathbf{s}$, A, and $\mathbf{\Omega}_z$, which requires the cooperation between source and relay in a centralized manner. A more practical yet suboptimal alternative is the separate optimization of $\mathbf{s}$ at the source and $\{A, \mathbf{\Omega}_z\}$ at the relay in a distributed manner. With the assumption that the source only has the CSI of the source-relay link, to maximize the received signal power at the relay, the source performs the singular value decomposition (SVD) of $\mathbf{H}_{\mathrm{sr}}$ as $\mathbf{H}_{\mathrm{sr}} = \mathbf{U} \mathbf{\Sigma} \mathbf{V}^H$ and sets $\mathbf{s} = \mathbf{v}_1$ where $\mathbf{v}_1$ is the right singular vector corresponding to the largest singular value of $\mathbf{H}_{\mathrm{sr}}$.

With the CSIs of the two adjacent links (i.e., source-relay link and relay-destination link) and perfect or imperfect CSI of the relay-eavesdropper link, the relay attempts to maximize the secrecy rate by optimizing the forwarding coefficient A and AN covariance $\mathbf{\Omega}_z$ under a total energy constraint. The optimization problem is given by

$$\begin{aligned} \max_{A, \mathbf{\Omega}_z} \quad & \frac{1}{2} \Big\{ C_{\mathrm{d}}(A, \mathbf{\Omega}_z) - C_{\mathrm{e}}(A, \mathbf{\Omega}_z) \Big\} && (14\mathrm{a}) \\ \text{s.t.:} \quad & \mathrm{Tr}\Big(A \left(E_{\mathrm{s}} \mathbf{H}_{\mathrm{sr}} \mathbf{s} \mathbf{s}^H \mathbf{H}_{\mathrm{sr}}^H + \mathbf{I} \right) + \mathbf{\Omega}_z \Big) \le E_{\mathrm{r}}, && (14\mathrm{b}) \\ & \mathbf{\Omega}_z \succeq \mathbf{0}, && (14\mathrm{c}) \end{aligned}$$

where E_{r} is the transmit energy budget and constraint (14b) represents the total energy constraint for one symbol at the relay.

It should be noted that although the assumptions described above make legitimate users at a disadvantage, it makes sense for the CPS application due to the lower complexity for legitimate users. Thus, the calculated secrecy rate provides a lower bound for the SISO relay transmission. With more complicated protocols, the secrecy rate can be further improved.

IV. Waveform Design With Perfect CSI

In this section, we consider the case that the relay has the perfect instantaneous CSI of the eavesdropper. The perfect CSI assumption is widely used in the PLS-based transmission protocol design. Moreover, it is not difficult to obtain eavesdropper's CSI if the eavesdropper is a registered legitimate but curious user in a network. We obtain the optimal solution by using a one-dimensional search as the outer step and solving a SDP problem in the inner step.

The problem in (14) is a non-convex problem since the objective function is the difference between two logarithmic functions, i.e., two concave functions. To tackle this problem, we introduce a slack variable $t > 1$ and transform the problem (14) into an epigraph form as

$$\begin{aligned} \max_{A, \mathbf{\Omega}_z, t} \quad & \frac{1}{2} \Big\{ C_{\mathrm{d}}(A, \mathbf{\Omega}_z) - \log_2(t) \Big\} && (15\mathrm{a}) \\ \text{s.t.:} \quad & C_{\mathrm{e}}(A, \mathbf{\Omega}_z) \le \log_2(t), && (15\mathrm{b}) \\ & \mathrm{Tr}\Big(A \left(E_{\mathrm{s}} \mathbf{H}_{\mathrm{sr}} \mathbf{s} \mathbf{s}^H \mathbf{H}_{\mathrm{sr}}^H + \mathbf{I} \right) + \mathbf{\Omega}_z \Big) \le E_{\mathrm{r}}, && (15\mathrm{c}) \\ & \mathbf{\Omega}_z \succeq \mathbf{0}. && (15\mathrm{d}) \end{aligned}$$

Note that the above new problem is an equivalent form of the original problem. Thus, the optimal solution to problem (15) is also the optimal solution to (14).

Observing problem (15), we find that the objective function is a function of A, $\mathbf{\Omega}_z$, and t. To maximize it we always have

$$\max_{A,\mathbf{\Omega}_z,t}\; C_s \Leftrightarrow \max_{t}\left(\max_{A,\mathbf{\Omega}_z}\; C_s\right), \tag{16}$$

where $C_s \triangleq \frac{1}{2}\Big\{C_{\rm d}(A,\mathbf{\Omega}_z)-\log_2(t)\Big\}$ is the objective function shown in (15a). Thus, the whole optimization procedure can be decomposed into two steps. First, for given t, we optimize $\{A,\mathbf{\Omega}_z\}$ to get the maximum C_s. Then, we optimize t to further improve C_s. The details are given as below.

1) *inner step:*

When t is fixed, after plugging (10) and (11) into (15a) and (15b), respectively, we get an equivalent problem of (15) for a fixed t, which is shown as

$$\begin{aligned}
\gamma_{\rm d}^*(t) \triangleq &\max_{A,\mathbf{\Omega}_z}\; \frac{AE_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2}{\mathbf{w}^H\big(A\mathbf{H}_{\rm rd}\mathbf{H}_{\rm rd}^H+\mathbf{H}_{\rm rd}\mathbf{\Omega}_z\mathbf{H}_{\rm rd}^H+\mathbf{I}\big)\mathbf{w}} && \text{(17a)}\\
&\text{s.t.:}\;\; AE_{\rm s}\left(\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\right)^H\mathbf{R}_{\rm e}^{-1}\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\le t-1, && \text{(17b)}\\
&\qquad\;\; \mathrm{Tr}\Big(A\big(E_{\rm s}\mathbf{H}_{\rm sr}\mathbf{s}\mathbf{s}^H\mathbf{H}_{\rm sr}^H+\mathbf{I}\big)+\mathbf{\Omega}_z\Big)\le E_{\rm r}, && \text{(17c)}\\
&\qquad\;\; \mathbf{\Omega}_z\succeq\mathbf{0}. && \text{(17d)}
\end{aligned}$$

To solve the above problem, we first recast the constraint (17b) as a linear matrix inequality form. According to the Schur's Complement [43], we have the following equivalent transformations

$$\begin{aligned}
&AE_{\rm s}\left(\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\right)^H\mathbf{R}_{\rm e}^{-1}\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\le t-1\\
\Longleftrightarrow\; &\frac{t-1}{E_{\rm s}}-\sqrt{A}\left(\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\right)^H\mathbf{R}_{\rm e}^{-1}\sqrt{A}\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\ge 0\\
\Longleftrightarrow\; &\begin{bmatrix}\frac{t-1}{E_{\rm s}} & \sqrt{A}\left(\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\right)^H\\ \sqrt{A}\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s} & \mathbf{R}_{\rm e}\end{bmatrix}\succeq\mathbf{0}\\
\Longleftrightarrow\; &\mathbf{R}_{\rm e}-\frac{E_{\rm s}}{t-1}A\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\left(\mathbf{H}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s}\right)^H\succeq\mathbf{0}\\
\Longleftrightarrow\; &\mathbf{H}_{\rm re}\left(A\mathbf{I}+\mathbf{\Omega}_z-\frac{E_{\rm s}}{t-1}A\mathbf{H}_{\rm sr}\mathbf{s}\mathbf{s}^H\mathbf{H}_{\rm sr}^H\right)\mathbf{H}_{\rm re}^H+\mathbf{I}\succeq\mathbf{0}
\end{aligned} \tag{18}$$

Replacing (17b) with (18), we find that problem (17) is a quasi-convex problem since the objective function (17a) is a linear-fractional function which is quasi-convex and the constraints are all convex. Using Charnes-Cooper transformation [44] we obtain the following equivalent problem

$$\begin{aligned}
\gamma_{\rm d}^*(t) \triangleq &\max_{\bar{A},\bar{\mathbf{\Omega}}_z,\mu}\; \bar{A}E_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2 && \text{(19a)}\\
&\text{s.t.:}\;\; \mathbf{w}^H\big(\bar{A}\mathbf{H}_{\rm rd}\mathbf{H}_{\rm rd}^H+\mathbf{H}_{\rm rd}\bar{\mathbf{\Omega}}_z\mathbf{H}_{\rm rd}^H+\mu\mathbf{I}\big)\mathbf{w}=1, && \text{(19b)}\\
&\qquad\;\; \mathbf{H}_{\rm re}\Big(\bar{A}\mathbf{I}+\bar{\mathbf{\Omega}}_z-\frac{E_{\rm s}}{t-1}\bar{A}\mathbf{H}_{\rm sr}\mathbf{s}\mathbf{s}^H\mathbf{H}_{\rm sr}^H\Big)\mathbf{H}_{\rm re}^H+\mu\mathbf{I}\succeq\mathbf{0}, && \text{(19c)}\\
&\qquad\;\; \mathrm{Tr}\Big(\bar{A}\big(E_{\rm s}\mathbf{H}_{\rm sr}\mathbf{s}\mathbf{s}^H\mathbf{H}_{\rm sr}^H+\mathbf{I}\big)+\bar{\mathbf{\Omega}}_z\Big)\le \mu E_{\rm r}, && \text{(19d)}\\
&\qquad\;\; \bar{\mathbf{\Omega}}_z\succeq\mathbf{0},\quad \mu\ge 0, && \text{(19e)}
\end{aligned}$$

where μ is an introduced auxiliary variable and the variable transformations are

$$\bar{A}=\mu A, \bar{\mathbf{\Omega}}_z=\mu\mathbf{\Omega}_z.$$

The problem (19) is a standard SDP problem with linear equality and linear matrix inequalities constraints. We can get the optimal numerical solution by using some convex optimization toolboxes, such as `CVX` [45].

2) *outer step:*

Based on (16) and (17), the problem (15) is equivalent to

$$\begin{aligned}
&\max_{t}\;\; \frac{1}{2}\log_2\left(t^{-1}+t^{-1}\gamma_{\rm d}^*(t)\right) && \text{(20a)}\\
&\text{s.t.:}\;\; 1<t\le t_{\max}, && \text{(20b)}
\end{aligned}$$

where $\gamma_{\rm d}^*(t)$ has been obtained in the *inner step* for fixed t. The lower bound of t is resulted from the fact $C_{\rm e}\ge 0$ and $t\ne 1$ in (19c). The upper bound follows from $C_s\ge 0$, the derivation of which is given by

$$\begin{aligned}
C_s \ge& 0\\
\Longrightarrow t\le& 1+\frac{AE_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2}{\mathbf{w}^H\left(A\mathbf{H}_{\rm rd}\mathbf{H}_{\rm rd}^H+\mathbf{H}_{\rm rd}\mathbf{\Omega}_z\mathbf{H}_{\rm rd}^H+\mathbf{I}\right)\mathbf{w}}\\
\le& 1+\frac{AE_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2}{A\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm rd}^H\mathbf{w}}\\
=& 1+\frac{E_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2}{\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm rd}^H\mathbf{w}}\triangleq t_{\max}.
\end{aligned} \tag{21}$$

It should be noted that the constraint (20b) is a necessary but not sufficient condition of $C_s\ge 0$. We use it to narrow the feasible range of t.

Problem (20) is a single-variable optimization problem. However, since we only have the numerical result of $\gamma_{\rm d}^*(t)$ and the closed-form solution is unavailable, we use one-dimensional search [46] on interval $(1,t_{\max}]$ to find the optimal solution.

We now summarize the whole solving procedure of problem (14) with perfect eavesdropper's CSI in Algorithm 1. Note that in Algorithm 1 the exhaustive line search with a given step size is adopted as an example of the one-dimensional search.

Algorithm 1 Optimal solution to problem (14) with perfect eavesdropper's CSI.

```
Input: step size $\Delta t$, $t_0 = 1+\Delta t$, $n = 0$, $C_s^{\max} = 0$, $A^* = 0$,
       $\mathbf{\Omega}_z^* = \mathbf{I}$;
Output:
repeat
    Solve problem (19) with $t = t_n$ and obtain $\gamma_{\rm d}^*(t_n)$, $A_n$,
    and $\mathbf{\Omega}_{z,n}$;
    Calculate $C_s(t_n) = \frac{1}{2}\log_2\left(t_n^{-1} + t_n^{-1}\gamma_{\rm d}^*(t_n)\right)$;
    if $C_s(t_n) > C_s^{\max}$ then
        $C_s^{\max} = C_s(t_n), A^* = A_n, \mathbf{\Omega}_z^* = \mathbf{\Omega}_{z,n}$;
    end if
    $n = n + 1$;
    $t_n = t_{n-1} + \Delta t$;
until $t_n > t_{\max}$.
return optimal settings $C_s^{\max}, A^*, \mathbf{\Omega}_z^*$.
```

V. Robust Waveform Design

In the previous section, we discuss the secrecy rate maximization problem with the assumption of perfect eavesdropper's CSI. However, it is difficult to obtain a passive eavesdropper's CSI in practice. Even for the case where the eavesdropper is a registered user in the network, we can only obtain its CSI occasionally when it has communication requirement. Consequently, the CSI may be outdated for the design of transmission strategy. In this section, we use a deterministic model to characterize the channel uncertainty (channel estimation error) of the relay-eavesdropper link and perform a robust secure waveform design.

Recall that the relay-eavesdropper link is a multipath channel $\mathbf{h}_{\rm re}$ with $L_{\rm e}$ resolvable multipaths. Considering the channel uncertainty, we remodel the channel vector as

$$\mathbf{h}_{\rm re} = \hat{\mathbf{h}}_{\rm re} + \Delta\mathbf{h}_{\rm re}, \quad \text{and} \tag{22}$$

$$\mathcal{G}_{\rm re} \triangleq \left\{\Delta\mathbf{h}_{\rm re} \in \mathbb{C}^{L_{\rm e}\times 1} : \|\Delta\mathbf{h}_{\rm re}\|^2 \leq \varepsilon^2\right\}, \tag{23}$$

where $\hat{\mathbf{h}}_{\rm re}$ is the estimate of the relay-eavesdropper link and $\Delta\mathbf{h}_{\rm re}$ is the unknown channel estimation error. The set $\mathcal{G}_{\rm re}$ defines a continuous space consisting of all possible CSI errors and ε represents the maximum value of the norm of the channel estimation error.

With channel uncertainty, robust waveform design is needed to maximize the worst-case secrecy rate under all possible CSI errors. The estimation error of $\mathbf{h}_{\rm re}$ results in the error of $\mathbf{H}_{\rm re}$. To make the subsequent discussion clearer, the relationship between $\mathbf{h}_{\rm re}$ and $\mathbf{H}_{\rm re}$ is given explicitly as

$$\mathbf{H}_{\rm re} = \begin{bmatrix} \mathbf{h}_{\rm re} & 0 & \cdots & 0 & 0 \\ 0 & \mathbf{h}_{\rm re} & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & \mathbf{h}_{\rm re} & 0 \\ 0 & 0 & \cdots & 0 & \mathbf{h}_{\rm re} \end{bmatrix} \in \mathbb{C}^{M_{\rm e}\times M_{\rm r}}. \tag{24}$$

We can see that $\mathbf{h}_{\rm re}$ occurs $M_{\rm r}$ times in $\mathbf{H}_{\rm re}$ and other elements are all zero.

Plugging (22) into (24), we can decompose $\mathbf{H}_{\rm re}$ into

$$\mathbf{H}_{\rm re} = \hat{\mathbf{H}}_{\rm re} + \Delta\mathbf{H}_{\rm re}, \quad \text{and} \tag{25}$$

$$\begin{aligned}\mathcal{Q}_{\rm re} \triangleq \big\{&\Delta\mathbf{H}_{\rm re} \in \mathbb{T}^{M_{\rm e}\times M_{\rm r}} : \|\Delta\mathbf{H}_{\rm re}\|_F^2 \leq M_{\rm r}\varepsilon^2, \\ &\Delta\mathbf{H}_{\rm re}^{(:,1)} = [\Delta\mathbf{h}_{\rm re}^T, \mathbf{0}]^T, \Delta\mathbf{H}_{\rm re}^{(1,j)} = 0 \text{ for } j \neq 1\big\},\end{aligned} \tag{26}$$

where $\hat{\mathbf{H}}_{\rm re}$ is the estimation value and $\Delta\mathbf{H}_{\rm re}$ denotes the error of estimation. The maximum value of error in (26) follows from

$$\|\Delta\mathbf{h}_{\rm re}\|^2 \leq \varepsilon^2 \Longrightarrow \|\Delta\mathbf{H}_{\rm re}\|_F^2 \leq M_{\rm r}\varepsilon^2. \tag{27}$$

It should be noted that only $L_{\rm e}$ elements of $\Delta\mathbf{H}_{\rm re}$ are independent variables since $\Delta\mathbf{H}_{\rm re}$ has the same structure as (24). Unfortunately, it is difficult to derive a tractable expression of $\Delta\mathbf{H}_{\rm re}$ using $\Delta\mathbf{h}_{\rm re}$. Hence, it is intractable for convex optimization if we use (26) directly in the robust waveform design. To tackle this problem, we relax the constraint on the structure of $\Delta\mathbf{H}_{\rm re}$ and denote the error matrix without structure constraint as $\Delta\tilde{\mathbf{H}}_{\rm re} \in \mathbb{C}^{M_{\rm e}\times M_{\rm r}}$. That is, all the elements of $\Delta\tilde{\mathbf{H}}_{\rm re}$ are independent complex variables.

Using $\Delta\tilde{\mathbf{H}}_{\rm re}$ instead of $\Delta\mathbf{H}_{\rm re}$, we remodel the equivalent channel matrix as

$$\mathbf{H}_{\rm re} = \hat{\mathbf{H}}_{\rm re} + \Delta\tilde{\mathbf{H}}_{\rm re}, \quad \text{and} \tag{28}$$

$$\tilde{\mathcal{Q}}_{\rm re} \triangleq \left\{\Delta\tilde{\mathbf{H}}_{\rm re} \in \mathbb{C}^{M_{\rm e}\times M_{\rm r}} : \|\Delta\tilde{\mathbf{H}}_{\rm re}\|_F^2 \leq M_{\rm r}\varepsilon^2\right\}. \tag{29}$$

In the following analysis, we use channel model (28) and (29) to perform robust waveform design. By using $\Delta\tilde{\mathbf{H}}_{\rm re}$, we actually enlarge the channel uncertainty space and the obtained secrecy rate below is a lower bound of the real achievable secrecy rate. The detailed explanation refers to Proposition 1.

With channel estimation error, using the same method in (15), we can transform the optimization problem (14) with imperfect eavesdropper's CSI into an epigraph form as

$$\max_{A,\mathbf{\Omega}_z,t} \quad \frac{1}{2}\Big\{C_{\rm d}(A,\mathbf{\Omega}_z) - \log_2(t)\Big\} \tag{30a}$$

$$\text{s.t.:} \quad \max_{\Delta\tilde{\mathbf{H}}_{\rm re}\in\tilde{\mathcal{Q}}_{\rm re}} C_{\rm e}(A,\mathbf{\Omega}_z) \leq \log_2(t), \tag{30b}$$

$$\text{(15c)} - \text{(15d)}. \tag{30c}$$

The solution procedure of (30) is similar to the procedure in Section IV. It also has two components: *inner step* and *outer step*. The details are given as follows.

1) *inner step:*

When t is fixed, after performing steps (17) and (18), we can derive the optimization object of the inner step as

$$\gamma_{\rm d}^*(t) \triangleq \max_{A,\mathbf{\Omega}_z} \frac{AE_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2}{\mathbf{w}^H\big(A\mathbf{H}_{\rm rd}\mathbf{H}_{\rm rd}^H + \mathbf{H}_{\rm rd}\mathbf{\Omega}_z\mathbf{H}_{\rm rd}^H + \mathbf{I}\big)\mathbf{w}} \tag{31a}$$

$$\text{s.t.:} \quad \max_{\Delta\tilde{\mathbf{H}}_{\rm re}\in\tilde{\mathcal{Q}}_{\rm re}} \mathbf{H}_{\rm re}\left(A\mathbf{I} + \mathbf{\Omega}_z - \frac{E_{\rm s}}{t-1}A\mathbf{H}_{\rm sr}\mathbf{s}\mathbf{s}^H\mathbf{H}_{\rm sr}^H\right)\mathbf{H}_{\rm re}^H + \mathbf{I} \succeq \mathbf{0}, \tag{31b}$$

$$\text{(15c)} - \text{(15d)}, \tag{31c}$$

Constraint (31b) actually includes an infinite number of constraints. We introduce Lemma 1 to convert them into a linear matrix inequality.

Lemma 1 (Robust QMI [47]): If $\mathbf{D} \succeq \mathbf{0}$, let $f(\mathbf{X}) = \mathbf{X}^H\mathbf{A}\mathbf{X} + \mathbf{B}^H\mathbf{X} + \mathbf{X}^H\mathbf{B} + \mathbf{C}$. We have

$$f(\mathbf{X}) \succeq \mathbf{0}, \quad \text{for all } \mathbf{X} \text{ with } \operatorname{Tr}\left(\mathbf{D}\mathbf{X}\mathbf{X}^H\right) \leq 1 \tag{32}$$

holds if and only if there exists $\xi \geq 0$ such that the following inequality holds

$$\begin{bmatrix} \mathbf{C} & \mathbf{B}^H \\ \mathbf{B} & \mathbf{A} \end{bmatrix} - \xi \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & -\mathbf{D} \end{bmatrix} \succeq \mathbf{0}. \tag{33}$$

Now, we apply Lemma 1 to constraint (31b). For notational simplicity, we define $g(A,\mathbf{\Omega}_z) \triangleq A\mathbf{I} + \mathbf{\Omega}_z - \frac{E_{\rm s}}{t-1}A\mathbf{H}_{\rm sr}\mathbf{s}\mathbf{s}^H\mathbf{H}_{\rm sr}^H$. Plugging (28) into (31b) and doing some mathematical manipulation, we have $\mathbf{X} = \Delta\tilde{\mathbf{H}}_{\rm re}^H$, $\mathbf{A} = g(A,\mathbf{\Omega}_z)$, $\mathbf{B} = g(A,\mathbf{\Omega}_z)\hat{\mathbf{H}}_{\rm re}^H$, and $\mathbf{C} = \hat{\mathbf{H}}_{\rm re}g(A,\mathbf{\Omega}_z)\hat{\mathbf{H}}_{\rm re}^H + \mathbf{I}$. From (29) we also have $\mathbf{D} = (M_{\rm r}\varepsilon^2)^{-1}\mathbf{I}$. Thus, the constraint (31b) is transformed into a linear matrix inequality constraint of $\{A,\mathbf{\Omega}_z\}$ as

$$\begin{aligned}U(A,\mathbf{\Omega}_z,\xi) \triangleq &\begin{bmatrix} \hat{\mathbf{H}}_{\rm re}g(A,\mathbf{\Omega}_z)\hat{\mathbf{H}}_{\rm re}^H + \mathbf{I} & \hat{\mathbf{H}}_{\rm re}g(A,\mathbf{\Omega}_z) \\ g(A,\mathbf{\Omega}_z)\hat{\mathbf{H}}_{\rm re}^H & g(A,\mathbf{\Omega}_z) \end{bmatrix} \\ &-\xi \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & -(M_{\rm r}\varepsilon^2)^{-1}\mathbf{I} \end{bmatrix} \succeq \mathbf{0}.\end{aligned} \tag{34}$$

Using Charnes-Cooper transformation again, we obtain the final optimization problem of the *inner step* as

$$\gamma_{\rm d}^*(t) \triangleq \max_{\bar{A},\bar{\mathbf{\Omega}}_z,\bar{\xi},\mu} \bar{A}E_{\rm s}\|\mathbf{w}^H\mathbf{H}_{\rm rd}\mathbf{H}_{\rm sr}\mathbf{s}\|^2 \tag{35a}$$

$$\text{s.t.:} \quad U(\bar{A},\bar{\mathbf{\Omega}}_z,\bar{\xi}) \succeq \mathbf{0}, \tag{35b}$$

$$\text{(19b), (19d), (19e),} \tag{35c}$$

where $\bar{\xi} = \mu\xi$. This problem is in a SDP form and can be easily handled by standard convex program solvers.

2) *outer step:* After obtaining $\gamma_{\rm d}^{*}(t)$ for fixed t, the rest procedure is the same as the *outer step* described in Section IV. We omit the details here.

Proposition 1: The optimal result of problem (30), i.e., maximum secrecy rate, is actually a lower bound of the real optimal result of the original problem (14) with imperfect eavesdropper's CSI.

Proof: In (30), we use $\Delta\tilde{\mathbf{H}}_{\rm re}$ instead of $\Delta\mathbf{H}_{\rm re}$, which makes (30) different from (14). In fact, $\Delta\mathbf{H}_{\rm re}$, which has a structure constraint, is a special case of $\Delta\tilde{\mathbf{H}}_{\rm re}$. Following this, we have

$$\mathcal{Q}_{\rm re} \subseteq \tilde{\mathcal{Q}}_{\rm re}. \tag{36}$$

In the *inner step* of the solution procedure of (30), constraint (31b) should be satisfied on the whole $\tilde{\mathcal{Q}}_{\rm re}$. According to (36), we actually impose a constraint on a set with more elements, which will increase the number of constraints. Hence, the feasible set is narrowed and the calculated $\gamma_{\rm d}^{*}(t)$ will be lower than the one obtained by using $\mathcal{Q}_{\rm re}$. Since the optimal result of *inner step* is a lower bound, the final optimal result after the outer one-dimensional search is also a lower bound of the real maximum secrecy rate of problem (14). ■

The above discussions mainly concentrate on the single-eavesdropper case. It is worth noting that the methods in Section IV and Section V also apply to the multi-eavesdropper case. When there are M $(M > 1)$ eavesdroppers, they can either work in the non-colluding manner or the colluding manner. For the non-colluding eavesdroppers, they work independently to intercept the confidential message. Thus, the eavesdropper's decoding capability is determined by the strongest eavesdropper with the highest SINR. Following this, the single constraint shown in (19c) and (35b) is now increased to M constraints, respectively, and each added constraint has the same form as the original one in (19c) and (35b), respectively. The rest of the two optimization methods remain unchanged. For the colluding eavesdroppers, they can combine their received signals to achieve a better performance. Similar to [48], we can write the combined signals in a matrix form as

$$\mathbf{y}_{\rm e}(k) = \sqrt{AE_{\rm s}}b(k)\tilde{\mathbf{H}}_{\rm re}\mathbf{H}_{\rm sr}\mathbf{s} + \sqrt{A}\tilde{\mathbf{H}}_{\rm re}\mathbf{n}_{\rm r} + \tilde{\mathbf{H}}_{\rm re}\mathbf{z} + \tilde{\mathbf{n}}_{\rm e}, \tag{37}$$

where

$$\mathbf{y}_{\rm e}(k) = \begin{bmatrix} \mathbf{y}_{\rm e}^{(1)}(k) \\ \vdots \\ \mathbf{y}_{\rm e}^{(M)}(k) \end{bmatrix}, \tilde{\mathbf{H}}_{\rm re} = \begin{bmatrix} \mathbf{H}_{\rm re}^{(1)} \\ \vdots \\ \mathbf{H}_{\rm re}^{(M)} \end{bmatrix}, \tilde{\mathbf{n}}_{\rm e} = \begin{bmatrix} \mathbf{n}_{\rm e}^{(1)} \\ \vdots \\ \mathbf{n}_{\rm e}^{(M)} \end{bmatrix} \tag{38}$$

with the superscript denoting the mth $(1 \leq m \leq M)$ eavesdropper. Replacing (9) with (37), the subsequent optimization processes are the same as the ones for the single-eavesdropper case.

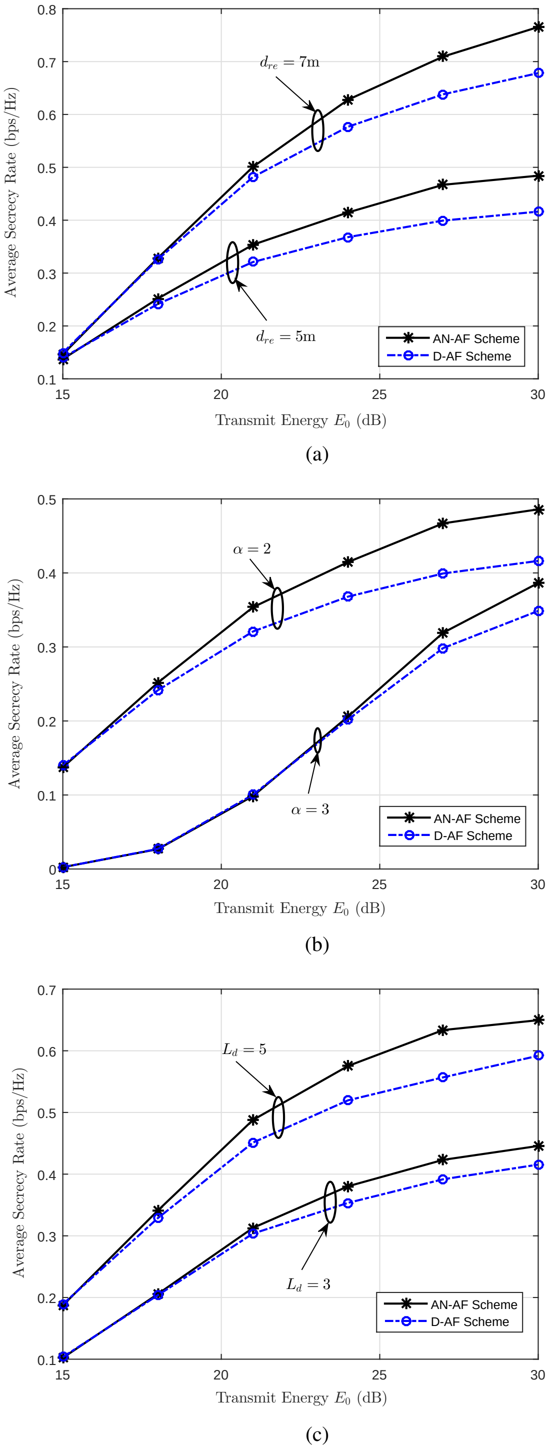
VI. Numerical Results

In this section, we present numerical results to show the average secrecy rates for different system parameters with different assumptions of CSI accuracy. In the simulations, the multipath channels are assumed to undergo a path loss combined with a small-scale fading, i.e., $\mathbf{h}_m = d_m^{-\alpha/2}\tilde{\mathbf{h}}_m, m \in \{{\rm sr}, {\rm rd}, {\rm re}\}$, where d_m is the distance between two communication nodes and α is the path-loss exponent. For $\tilde{\mathbf{h}}_m$, we assume that each element of $\tilde{\mathbf{h}}_m$ follows an independent and identical complex Gaussian distribution with zero mean and unit variance like [39]. We introduce a baseline scheme called Direct AF (D-AF) scheme. For the D-AF scheme, except that it does not use artificial noise, others are the same as the AN-AF scheme. All the following results are obtained by averaging over 1000 randomly generated small-scale channel realizations. Moreover, in the simulations below, we set $E_{\rm s} = E_{\rm r} = E_0$. The transmission distances of the source-relay link and relay-destination link are fixed as $d_{\rm sr} = 3{\rm m}$ and $d_{\rm rd} = 5{\rm m}$, respectively. The number of multipaths of the source-relay link is fixed as $L_{\rm r} = 3$. The path-loss exponent α is given as $\alpha = 2$ unless otherwise specified.

We first present some numerical results for the case with perfect CSI in Fig. 2 and Fig. 3. In Fig. 2, we plot the average secrecy rate versus transmit energy for different simulation settings. From the three figures, we can see that the AN-AF scheme outperforms the D-AF scheme and the advantage becomes more and more obvious with the increase of transmit energy. This implies that even though the AN will cause interference to the destination due to the fact that $\mathbf{H}_{\rm rd}$ is a full column rank matrix and there is no null space, employing AN can still improve secrecy rate. What's more, with more available transmit energy, we can add more AN to the information-bearing waveform, which brings more benefits to the legitimate receiver. From Fig. 2(a) one can see that the secrecy rate for $d_{\rm re} = 7{\rm m}$ is larger than the rate for $d_{\rm re} = 5{\rm m}$. This is expected since eavesdropper suffers from severer propagation loss when $d_{\rm re}$ is larger. From Fig. 2(b) one can see that when the transmit energy is not large enough (e.g., from 15dB to 23dB), the secrecy rate for $\alpha = 3$ is significantly less than the rate for $\alpha = 2$ and the performances of the two schemes are nearly the same for $\alpha = 3$. This is because when the path loss is severe, most energy is used to compensate for the large-scale fading, which limits the ability of the AN-AF scheme. In Fig. 2(c), in order to guarantee that the length of waveform is much larger than the number of multipath, we enhance N to 16. One can see that the secrecy rate is higher if the relay-destination link has more paths. In fact, similar to the multi-antenna system, more paths is equivalent to more receive antennas, which can improve the decoding capability at the receiver. Hence, when $L_{\rm e}$ is fixed, larger $L_{\rm d}$ puts the relay-destination link in a more superior position compared with the relay-eavesdropper link.

Fig. 3 shows the average secrecy rate versus the number of relay-eavesdropper link's multipaths for different $L_{\rm d}$. It is observed that the secrecy rate decreases with the increase of $L_{\rm e}$. This is expected since eavesdropper's decoding capability improves with the increase of $L_{\rm e}$, which has been explained in Fig. 2(c). Furthermore, one can see that the performance gap between two schemes is more obvious when either $L_{\rm d}$ or $L_{\rm e}$ gets larger. That is, the gap increases when the equivalent channel matrix $\mathbf{H}_{\rm rd}$ or $\mathbf{H}_{\rm re}$ has more degrees of freedom.

We then study the impact of imperfect CSI on the average secrecy rate. As discussed in Section V, the obtained secrecy



(a)

(b)

(c)

Fig. 2. Perfect CSI: Average secrecy rate as a function of transmit energy with different simulation settings. (a) Different distances between relay and eavesdropper with $N = 10$ and $L_{\rm d} = L_{\rm e} = 3$. (b) Different path-loss exponents with $N = 10$, $d_{\rm re} = d_{\rm rd} = 5$m, and $L_{\rm d} = L_{\rm e} = 3$. (c) Different number of relay-destination link's multipaths with $N = 16$, $d_{\rm re} = d_{\rm rd} = 5$m, and $L_{\rm e} = 3$.

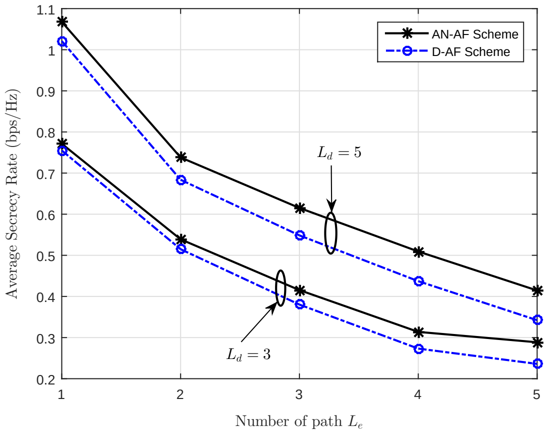


Fig. 3. Perfect CSI: Average secrecy rate as a function of the number of relay-eavesdropper link's multipaths for different $L_{\rm d}$. Other simulation settings are $N = 16$, $E_0 = 27$dB, and $d_{\rm re} = d_{\rm rd} = 5$m.

rate is a lower bound of the real achievable rate when the CSI is imperfect. Since we do not know the specific gap between the lower bound and the real value, it is unfair to compare the performances between two schemes. Hence, in the following simulations, we only show the results of AN-AF scheme.

Fig. 4 depicts the average secrecy rate as a function of the transmission distance between relay and eavesdropper. The solid line represents the result with perfect CSI and the two dashed lines represent the imperfect-CSI case. As illustrated in Fig. 4, the average secrecy rates of the imperfect-CSI situation are much smaller than those of perfect-CSI situation. The larger the ε^2 is, the lower the secrecy rate will be. It is worth noting that the two dashed lines are only the lower bounds while the red line is the accurate rate. Therefore, secrecy rate does suffer from the estimation error of CSI but the real gap will be smaller than the one presented in Fig. 4. Moreover, one can see that the secrecy rate increases with the enhance of $d_{\rm re}$. This corresponds with the result shown in Fig. 2(a).

Fig. 5 plots the average secrecy rate versus the channel estimation error for different transmit energy. It is observed that with the increase of channel estimation error ε^2, the lower bound of the average secrecy rate decreases. This is consistent with the result in Fig. 4. It is also observed that the secrecy rate improves a lot with the increase of transmit energy when the estimation error is between 0.1 and 0.3. However, when ε^2 is larger than 0.4, the rate improvement is less significant. This implies that there is no need to improve transmit energy when the estimation error is large. Moreover, one can see that the gap between the solid line and the dashed line is much bigger than the gap between the dashed line and the dash-dot line. This implies that when the transmit energy is high enough, the further enhancement of energy can not improve secrecy rate significantly.

VII. Conclusions

Although CPS is expected to produce enormous economic benefits, it is vulnerable to many kinds of malicious attacks due to the employment of communication networks. Among

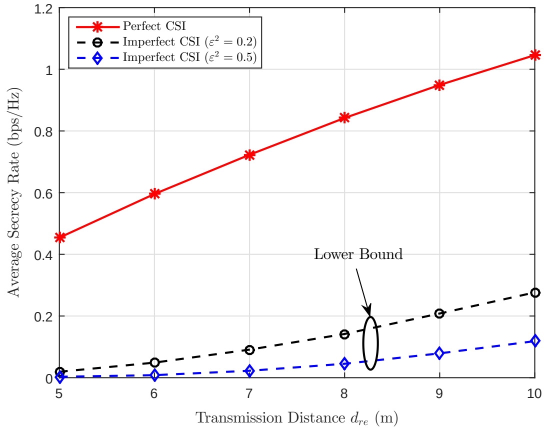


Fig. 4. AN-AF scheme with imperfect CSI: Average secrecy rate as a function of the transmission distance of the relay-eavesdropper link. Other simulation settings are $N = 10$, $E_0 = 30$dB, and $L_{\mathrm{d}} = L_{\mathrm{e}} = 3$.

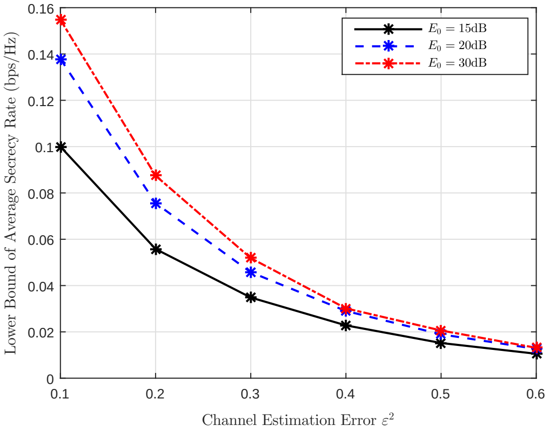


Fig. 5. AN-AF scheme with imperfect CSI: Average secrecy rate as a function of channel estimation error for different transmit energy. Other simulation settings are $N = 10$, $d_{\mathrm{re}} = 7$m, and $L_{\mathrm{d}} = L_{\mathrm{e}} = 3$.

these attacks, privacy is becoming a very critical issue since what the CPS connects is the real physical world and thus any information leakage will cause serious consequences. We studied the privacy-enhanced waveform design method for a SISO relay network with multipath receptions. Specifically, we proposed an AN-AF strategy which required the relay to forward the source message and inject artificial noise at the same time. We first studied the case with perfect eavesdropper's CSI. The AF coefficient for forwarding information-bearing signal and the AN covariance were optimized to maximize the achievable secrecy rate. We obtained the optimal solution by using a one-dimensional search and solving a series of SDPs. Then, we considered a more practical scenario where there exists channel estimation error for eavesdropper's CSI. To tackle this problem, we enlarged the estimation error space and then obtained the lower bound of the achievable secrecy rate. Numerical examples were presented to show the performances of the proposed schemes under different simulation environments. Simulation results demonstrate that although the injected AN will cause interference to the legitimate user, it is still helpful for increasing secrecy rate.

References

[1] Q. Shafi, "Cyber physical systems security: A brief survey," in *Proc. Computational Science and Its Applications (ICCSA)*, Jun. 2012, pp. 146–150.

[2] Q. Du, W. Zhao, W. Li, X. Zhang, B. Sun, H. Song, P. Ren, L. Sun, and Y. Wang, "Massive access control aided by knowledge-extraction for co-existing periodic and random services over wireless clinical networks," *J. Med. Syst.*, vol. 40, no. 7, pp. 1–8, Jul. 2016.

[3] Z. Su, Q. Xu, H. Zhu, and Y. Wang, "A novel design for content delivery over software defined mobile social networks," *IEEE Network*, vol. 29, no. 4, pp. 62–67, Jul. 2015.

[4] W. Wolf, "News briefs," *Computer*, vol. 40, no. 11, pp. 104–105, Nov. 2007.

[5] H. Kagermann, W. Wahlster, and J. Helbig, "Secure the future of German manufacturing industry: Recommendations for implementing the strategic initiative Industrie 4.0," Final report of the Industrie 4.0 Working Group, Frankfurt, Tech. Rep., Apr. 2013.

[6] H. Song, D. Rawat, S. Jeschke, and C. Brecher, *Cyber-Physical Systems: Foundations, Principles and Applications*. Boston, MA: Academic Press, 2016.

[7] S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Cham, Switzerland: Springer, 2017.

[8] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1097–1107, Jul. 2012.

[9] X. Li, C. Qiao, X. Yu, A. Wagh, R. Sudhaakar, and S. Addepalli, "Toward effective service scheduling for human drivers in vehicular cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1775–1789, Sep. 2012.

[10] Z. Wang, H. Song, D. W. Watkins, K. G. Ong, P. Xue, Q. Yang, and X. Shi, "Cyber-physical systems for water sustainability: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 216–222, May 2015.

[11] S. Li, T. Tryfonas, G. Russell, and P. Andriotis, "Risk assessment for mobile systems through a multilayered hierarchical Bayesian network," *IEEE Trans. Cybern.*, vol. 46, no. 8, pp. 1749–1759, Aug. 2016.

[12] S. Li, T. Tryfonas, and H. Li, "The Internet of things: A security point of view," *Internet Research*, vol. 26, no. 2, pp. 337–359, 2016.

[13] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "CAP: A context-aware privacy protection system for location-based services," in *Proc. IEEE International Conference on Distributed Computing Systems (ICDCS)*, Jun. 2009.

[14] W. Yu, H. Xu, H. Zhang, D. Griffith, and N. Golmie, "Ultra-dense networks: Survey of state of the art and future directions," in *Proc. IEEE International Conference on Computer Communication and Networks (ICCCN)*, Aug. 2016.

[15] H. Song, G. A. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems*. Chichester, UK: Wiley, 2017.

[16] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 3, pp. 1294–1312, Aug. 2015.

[17] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[18] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: modeling and countermeasures," *IEEE Transactions on Parallel and Distributed System*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[19] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. Allerton Conf. Commun., Control, Comput.*, Monticello, IL,USA, Sep. 2009, pp. 911–918.

[20] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, Mar. 2016.

[21] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE IoT J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014.

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

[23] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[24] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[25] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[26] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66–72, Mar. 2014.

[27] L. Sun, Q. Du, P. Ren, and Y. Wang, "Two birds with one stone: towards secure and interference-free D2D transmissions via constellation rotation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8767–8774, Oct. 2016.

[28] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840 – 2853, Jun. 2016.

[29] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[30] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[31] Q. Li, Y. Yang, W. K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[32] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[33] W. Xu, Y. Cui, H. Zhang, G. Y. Li, and X. You, "Robust beamforming with partial channel state information for energy efficient networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2920–2935, Dec. 2015.

[34] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2016.

[35] D. C. Popescu, D. B. Rawat, O. Popescu, and M. Saquib, "Game-theoretic approach to joint transmitter adaptation and power control in wireless systems," *IEEE Trans. Systems, Man, and Cybernetics–Part B*, vol. 40, no. 3, pp. 675–682, Jun. 2010.

[36] D. B. Rawat and D. C. Popescu, "Precoder adaptation and power control for cognitive radios in dynamic spectrum access environments," *IET Commun.*, vol. 6, no. 8, pp. 836–844, May 2012.

[37] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Trans. Ind. Inf.*, vol. 12, no. 1, pp. 291–300, Feb. 2016.

[38] M. Hussain, Q. Du, L. Sun, and P. Ren, "Security enhancement for video transmission via noise aggregation in immersive systems," *Multimedia Tools and Applications*, pp. 1–13, Sep. 2015.

[39] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

[40] M. Hussain, Q. Du, L. Sun, and P. Ren, "Security protection over wireless fading channels by exploiting frequency selectivity," in *Proc. IEEE WCSP*, Yangzhou, China, Oct. 2016.

[41] M. Paolini. (2011) Beyond data caps: An analysis of the uneven growth in data traffic. [Online]. Available: http://www.senzafiliconsulting.com.

[42] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channels," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[43] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge Univ. Press, 2004.

[44] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logist.Quart.*, vol. 9, pp. 181–186, Dec. 1962.

[45] M. Grant and S. Boyd. (2011, Apr.) CVX: Matlab software for disciplined convex programming. http://cvxr.com/cvx.

[46] D. P. Bertsekas, *Nonlinear Programming (2nd edition)*. Belmont, MA, USA: Athena Scientific, 1999.

[47] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. Optimiz.*, vol. 14, no. 4, pp. 1140–1162, 2004.

[48] H. Wang, F. Liu, and X. G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 8, pp. 1240–1250, Aug. 2014.