

# 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. 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), physical layer security (PLS), privacy, relay transmission, waveform design, wireless communications.

## I. INTRODUCTION

### A. Background

**CYBER-PHYSICAL** system (CPS) is an integration of computation, networking, and physical processes.

Manuscript received November 30, 2016; revised February 16, 2017; accepted March 3, 2017. Date of publication March 20, 2017; date of current version December 11, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61431011 and Grant 61671371, in part by the National Science and Technology Major Project under Grant 2016ZX03001016-005, in part by the Science and Technology Program of Shaanxi Province under Grant 2016KW-032, and in part by the Fundamental Research Funds for the Central Universities. (Corresponding author: Pinyi Ren.)

Q. Xu, P. Ren, and Q. Du are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with the Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China (e-mail: xq1216@stu.xjtu.edu.cn; pyren@mail.xjtu.edu.cn; duqinghe@mail.xjtu.edu.cn).

H. Song is with the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136 USA (e-mail: h.song@ieee.org).

Digital Object Identifier 10.1109/IIOT.2017.2684221

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 U.S. National Science Foundation 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. Li *et al.* [9] proposed a novel service scheduling scheme in vehicular CPS by taking human factors into consideration. Wang *et al.* [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 nonrepudiation 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 on specific CPS applications [17]–[19]. Lyamin *et al.* [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. Mo and Sinopoli [19] 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 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]. 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 multiantenna signal processing [33], [34] are the two frequently used techniques. Krikidis *et al.* [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. Li *et al.* [30] and [31] further improved the transmission secrecy by employing multiple cooperative relays to form a virtual antenna array. For the multiantenna scenarios, various signal processing techniques such as beamforming, precoding, and artificial noise (AN) are employed in the multiple-input single-output case or the full-fledged multiple-input multiple-output 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 multirelay-aided coordinated transmissions like [30] and [31] are inapplicable due to the requirement of complex control messages. Second, although multiantenna 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 multiantenna 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]. Sun *et al.* [37] proposed a fountain-coding-aided secure transmission protocol and the noise aggregation scheme was proposed in [38]. Li *et al.* [39] and Hussain *et al.* [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 preselected 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 is 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.

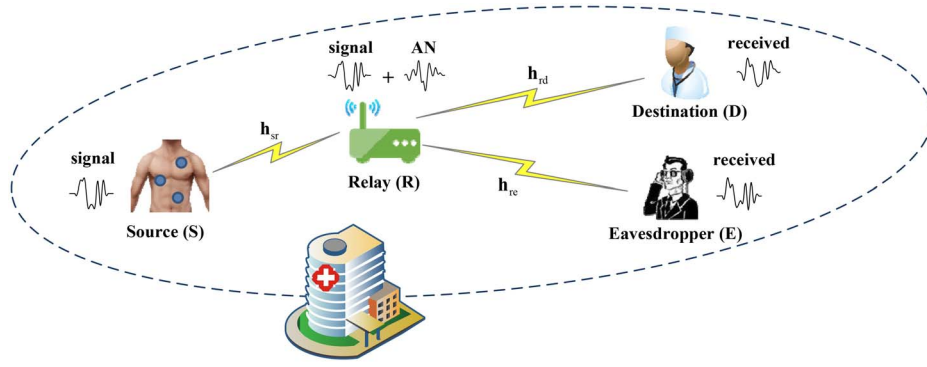


Fig. 1. System model: Source node  $S$  is transmitting a confidential message to the destination node  $D$  with the help of a relay  $R$ . An eavesdropper is trying to intercept the message.

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 legitimate 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, this 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.  $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \Omega)$  means that the random vector  $\mathbf{x}$  follows a complex circular Gaussian distribution with mean  $\boldsymbol{\mu}$  and covariance  $\Omega$ .  $\mathbf{x}(n)$  represents the  $n$ th component of the vector  $\mathbf{x}$ .  $\mathbf{A}^{(i,j)}$  represents the element at the  $i$ th row and  $j$ th column of matrix  $\mathbf{A}$ , and  $\mathbf{A}^{(:,j)}$  represents the  $j$ th column of matrix  $\mathbf{A}$ .  $\mathbf{I}$  denotes an identity matrix.  $\mathbf{A}^T$ ,  $\mathbf{A}^H$ , and  $\text{Tr}(\mathbf{A})$  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,<sup>1</sup> 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 multiantenna 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

$$x_s(t) = \sum_{k=0}^{\infty} \sqrt{E_s} b(k) s(t - kT) \quad (1)$$

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

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

where  $N$  is the number of pulse for one symbol,  $\mathbf{s}(n) \in \mathbb{C}$ ,  $n = 0, 1, \dots, N-1$  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  $\mathbf{h}_{sr} = [h_{sr,1}, \dots, h_{sr,L_r}]^T$  with  $L_r$  resolvable multipaths, the received signal at the relay is

$$y_r(t) = h_{sr}(t) * x_s(t) + n_r(t) \quad (3)$$

where  $n_r(t)$  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

$$x_r(t) = \sqrt{A} y_r(t) + z(t) \quad (4)$$

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

$$z(t) = \sum_{m=0}^{M_r-1} \mathbf{z}(m) \psi(t - mT_c) \quad (5)$$

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



where  $M_r = N + L_r - 1$  and  $\mathbf{z} \in \mathbb{C}^{M_r \times 1}$  is the AN vector following  $\mathcal{CN}(\mathbf{0}, \Omega_z)$  distribution.

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

$$y_d(t) = \sqrt{A}h_{rd}(t) * (h_{sr}(t) * x_s(t) + n_r(t)) + h_{rd}(t) * z(t) + n_d(t) \quad (6)$$

and

$$y_e(t) = \sqrt{A}h_{re}(t) * (h_{sr}(t) * x_s(t) + n_r(t)) + h_{re}(t) * z(t) + n_e(t) \quad (7)$$

respectively.

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

$$\mathbf{y}_d(k) = \sqrt{AE_s}b(k)\mathbf{H}_{rd}\mathbf{H}_{sr}\mathbf{s} + \sqrt{A}\mathbf{H}_{rd}\mathbf{n}_r + \mathbf{H}_{rd}\mathbf{z} + \mathbf{n}_d \quad (8)$$

where  $\mathbf{n}_r$  and  $\mathbf{n}_d$  are the additive white Gaussian noise following the  $\mathcal{CN}(\mathbf{0}, \mathbf{I})$  distribution,  $\mathbf{H}_{sr} \in \mathbb{C}^{M_r \times N}$  and  $\mathbf{H}_{rd} \in \mathbb{C}^{M_d \times M_r}$  are the Toeplitz matrices with each column vector being the shifted version of  $\mathbf{h}_{sr}$  and  $\mathbf{h}_{rd}$ , respectively. Note that in (8) we have omitted the intersymbol-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

$$\mathbf{y}_e(k) = \sqrt{AE_s}b(k)\mathbf{H}_{re}\mathbf{H}_{sr}\mathbf{s} + \sqrt{A}\mathbf{H}_{re}\mathbf{n}_r + \mathbf{H}_{re}\mathbf{z} + \mathbf{n}_e \quad (9)$$

where  $\mathbf{H}_{re} \in \mathbb{C}^{M_e \times M_r}$  is the Toeplitz matrices with each column vector being the shifted version of  $\mathbf{h}_{re}$  and  $M_e = M_r + L_e - 1$ .

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  $\mathbf{w} = \mathbf{H}_{rd}\mathbf{H}_{sr}\mathbf{s} / \|\mathbf{H}_{rd}\mathbf{H}_{sr}\mathbf{s}\|$  and the signal-to-interference-plus-noise ratio (SINR) at the destination is given by

$$\gamma_d = \frac{AE_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2}{\mathbf{w}^H (\mathbf{A} \mathbf{H}_{rd} \mathbf{H}_{rd}^H + \mathbf{H}_{rd} \Omega_z \mathbf{H}_{rd}^H + \mathbf{I}) \mathbf{w}}. \quad (10)$$

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

$$\gamma_e = AE_s (\mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s})^H \mathbf{R}_e^{-1} \mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s} \quad (11)$$

with

$$\mathbf{R}_e = \mathbf{A} \mathbf{H}_{re} \mathbf{H}_{re}^H + \mathbf{H}_{re} \Omega_z \mathbf{H}_{re}^H + \mathbf{I}. \quad (12)$$

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

$$C_s = \frac{1}{2} [C_d - C_e]^+ = \frac{1}{2} [\log_2(1 + \gamma_d) - \log_2(1 + \gamma_e)]^+. \quad (13)$$

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  $\Omega_z$ , 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  $\{A, \Omega_z\}$  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 of  $\mathbf{H}_{sr}$  as  $\mathbf{H}_{sr} = \mathbf{U} \Sigma \mathbf{V}^H$  and sets  $\mathbf{s} = \mathbf{v}_1$  where  $\mathbf{v}_1$  is the right singular vector corresponding to the largest singular value of  $\mathbf{H}_{sr}$ .

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  $\Omega_z$  under a total energy constraint. The optimization problem is given by

$$\max_{A, \Omega_z} \frac{1}{2} \{C_d(A, \Omega_z) - C_e(A, \Omega_z)\} \quad (14a)$$

$$\text{s.t.: } \text{Tr}(\mathbf{A}(\mathbf{E}_s \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H + \mathbf{I}) + \Omega_z) \leq E_r \quad (14b)$$

$$\Omega_z \succeq \mathbf{0} \quad (14c)$$

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 1-D search as the outer step and solving an SDP problem in the inner step.

The problem in (14) is a nonconvex 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

$$\max_{A, \Omega_z, t} \frac{1}{2} \{C_d(A, \Omega_z) - \log_2(t)\} \quad (15a)$$

$$\text{s.t.: } C_e(A, \Omega_z) \leq \log_2(t), \quad (15b)$$

$$\text{Tr}(\mathbf{A}(\mathbf{E}_s \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H + \mathbf{I}) + \Omega_z) \leq E_r \quad (15c)$$

$$\Omega_z \succeq \mathbf{0}. \quad (15d)$$

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  $A$ ,  $\Omega_z$ , and  $t$ . To maximize it we always have

$$\max_{A, \Omega_z, t} C_s \Leftrightarrow \max_t \left( \max_{A, \Omega_z} C_s \right) \quad (16)$$

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

#### A. 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

$$\gamma_d^*(t) \triangleq \max_{A, \Omega_z} \frac{AE_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2}{\mathbf{w}^H (\mathbf{A} \mathbf{H}_{rd} \mathbf{H}_{rd}^H + \mathbf{H}_{rd} \Omega_z \mathbf{H}_{rd}^H + \mathbf{I}) \mathbf{w}} \quad (17a)$$

$$\text{s.t.: } AE_s (\mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s})^H \mathbf{R}_e^{-1} \mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s} \leq t - 1 \quad (17b)$$

$$\text{Tr}(\mathbf{A} (E_s \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H + \mathbf{I}) + \Omega_z) \leq E_r \quad (17c)$$

$$\Omega_z \geq \mathbf{0}. \quad (17d)$$

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:

$$\begin{aligned} AE_s (\mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s})^H \mathbf{R}_e^{-1} \mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s} &\leq t - 1 \\ \Leftrightarrow \frac{t-1}{E_s} - \sqrt{A} (\mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s})^H \mathbf{R}_e^{-1} \sqrt{A} \mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s} &\geq 0 \\ \Leftrightarrow \begin{bmatrix} \frac{t-1}{E_s} & \sqrt{A} (\mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s})^H \\ \sqrt{A} \mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s} & \mathbf{R}_e \end{bmatrix} &\geq \mathbf{0} \\ \Leftrightarrow \mathbf{R}_e - \frac{E_s}{t-1} \mathbf{A} \mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s} (\mathbf{H}_{re} \mathbf{H}_{sr} \mathbf{s})^H &\geq \mathbf{0} \\ \Leftrightarrow \mathbf{H}_{re} \left( \mathbf{A} \mathbf{I} + \Omega_z - \frac{E_s}{t-1} \mathbf{A} \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H \right) \mathbf{H}_{re}^H + \mathbf{I} &\geq \mathbf{0}. \end{aligned} \quad (18)$$

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:

$$\gamma_d^*(t) \triangleq \max_{\bar{A}, \bar{\Omega}_z, \mu} \bar{A} E_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2 \quad (19a)$$

$$\text{s.t.: } \mathbf{w}^H (\bar{A} \mathbf{H}_{rd} \mathbf{H}_{rd}^H + \mathbf{H}_{rd} \bar{\Omega}_z \mathbf{H}_{rd}^H + \mu \mathbf{I}) \mathbf{w} = 1 \quad (19b)$$

$$\mathbf{H}_{re} \left( \bar{A} \mathbf{I} + \bar{\Omega}_z - \frac{E_s}{t-1} \bar{A} \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H \right) \mathbf{H}_{re}^H + \mu \mathbf{I} \geq \mathbf{0} \quad (19c)$$

$$\text{Tr}(\bar{A} (E_s \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H + \mathbf{I}) + \bar{\Omega}_z) \leq \mu E_r \quad (19d)$$

$$\bar{\Omega}_z \geq \mathbf{0}, \mu \geq 0 \quad (19e)$$

where  $\mu$  is an introduced auxiliary variable and the variable transformations are

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

#### Algorithm 1 Optimal Solution to Problem (14) With Perfect Eavesdropper's CSI

**Input:** step size  $\Delta t$ ,  $t_0 = 1 + \Delta t$ ,  $n = 0$ ,  $C_s^{\max} = 0$ ,  $A^* = 0$ ,  $\Omega_z^* = \mathbf{I}$ ;

**Output:**

- 1: **repeat**
- 2:   Solve problem (19) with  $t = t_n$  and obtain  $\gamma_d^*(t_n)$ ,  $A_n$ , and  $\Omega_{z,n}$ ;
- 3:   Calculate  $C_s(t_n) = \frac{1}{2} \log_2(t_n^{-1} + t_n^{-1} \gamma_d^*(t_n))$ ;
- 4:   **if**  $C_s(t_n) > C_s^{\max}$  **then**
- 5:      $C_s^{\max} = C_s(t_n)$ ,  $A^* = A_n$ ,  $\Omega_z^* = \Omega_{z,n}$ ;
- 6:   **end if**
- 7:    $n = n + 1$ ;
- 8:    $t_n = t_{n-1} + \Delta t$ ;
- 9: **until**  $t_n > t_{\max}$ .
- 10: **return** optimal settings  $C_s^{\max}$ ,  $A^*$ ,  $\Omega_z^*$ .

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].

#### B. Outer Step

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

$$\max_t \frac{1}{2} \log_2(t^{-1} + t^{-1} \gamma_d^*(t)) \quad (20a)$$

$$\text{s.t.: } 1 < t \leq t_{\max} \quad (20b)$$

where  $\gamma_d^*(t)$  has been obtained in the *inner step* for fixed  $t$ . The lower bound of  $t$  is resulted from the fact  $C_e \geq 0$  and  $t \neq 1$  in (19c). The upper bound follows from  $C_s \geq 0$ , the derivation of which is given by

$$\begin{aligned} C_s \geq 0 &\Rightarrow t \leq 1 + \frac{AE_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2}{\mathbf{w}^H (\mathbf{A} \mathbf{H}_{rd} \mathbf{H}_{rd}^H + \mathbf{H}_{rd} \Omega_z \mathbf{H}_{rd}^H + \mathbf{I}) \mathbf{w}} \\ &\leq 1 + \frac{AE_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2}{\mathbf{A} \mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{rd}^H \mathbf{w}} \\ &= 1 + \frac{E_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2}{\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{rd}^H \mathbf{w}} \triangleq t_{\max}. \end{aligned} \quad (21)$$

It should be noted that the constraint (20b) is a necessary but not sufficient condition of  $C_s \geq 0$ . 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  $\gamma_d^*(t)$  and the closed-form solution is unavailable, we use 1-D 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 1-D search.

#### 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  $\mathbf{h}_{re}$  with  $L_e$  resolvable multipaths. Considering the channel uncertainty, we remodel the channel vector as

$$\mathbf{h}_{re} = \hat{\mathbf{h}}_{re} + \Delta\mathbf{h}_{re} \quad (22)$$

and

$$\mathcal{G}_{re} \triangleq \left\{ \Delta\mathbf{h}_{re} \in \mathbb{C}^{L_e \times 1} : \|\Delta\mathbf{h}_{re}\|^2 \leq \varepsilon^2 \right\} \quad (23)$$

where  $\hat{\mathbf{h}}_{re}$  is the estimate of the relay-eavesdropper link and  $\Delta\mathbf{h}_{re}$  is the unknown channel estimation error. The set  $\mathcal{G}_{re}$  defines a continuous space consisting of all possible CSI errors and  $\varepsilon$  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  $\mathbf{h}_{re}$  results in the error of  $\mathbf{H}_{re}$ . To make the subsequent discussion clearer, the relationship between  $\mathbf{h}_{re}$  and  $\mathbf{H}_{re}$  is given explicitly as

$$\mathbf{H}_{re} = \begin{bmatrix} \mathbf{h}_{re} & 0 & \cdots & 0 & 0 \\ 0 & \mathbf{h}_{re} & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & \mathbf{h}_{re} & 0 \\ 0 & 0 & \cdots & 0 & \mathbf{h}_{re} \end{bmatrix} \in \mathbb{C}^{M_e \times M_r}. \quad (24)$$

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

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

$$\mathbf{H}_{re} = \hat{\mathbf{H}}_{re} + \Delta\mathbf{H}_{re} \quad (25)$$

and

$$\begin{aligned} \mathcal{Q}_{re} &\triangleq \left\{ \Delta\mathbf{H}_{re} \in \mathbb{T}^{M_e \times M_r} : \|\Delta\mathbf{H}_{re}\|_F^2 \leq M_r \varepsilon^2 \right\} \\ \Delta\mathbf{H}_{re}^{(:,1)} &= [\Delta\mathbf{h}_{re}^T, \mathbf{0}]^T, \Delta\mathbf{H}_{re}^{(1,j)} = 0 \text{ for } j \neq 1 \end{aligned} \quad (26)$$

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

$$\|\Delta\mathbf{h}_{re}\|^2 \leq \varepsilon^2 \implies \|\Delta\mathbf{H}_{re}\|_F^2 \leq M_r \varepsilon^2. \quad (27)$$

It should be noted that only  $L_e$  elements of  $\Delta\mathbf{H}_{re}$  are independent variables since  $\Delta\mathbf{H}_{re}$  has the same structure as (24). Unfortunately, it is difficult to derive a tractable expression of  $\Delta\mathbf{H}_{re}$  using  $\Delta\mathbf{h}_{re}$ . 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  $\Delta\mathbf{H}_{re}$  and denote the error matrix without structure constraint as  $\tilde{\Delta}\mathbf{H}_{re} \in \mathbb{C}^{M_e \times M_r}$ . That is, all the elements of  $\tilde{\Delta}\mathbf{H}_{re}$  are independent complex variables.

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

$$\mathbf{H}_{re} = \hat{\mathbf{H}}_{re} + \tilde{\Delta}\mathbf{H}_{re} \quad (28)$$

and

$$\tilde{\mathcal{Q}}_{re} \triangleq \left\{ \tilde{\Delta}\mathbf{H}_{re} \in \mathbb{C}^{M_e \times M_r} : \|\tilde{\Delta}\mathbf{H}_{re}\|_F^2 \leq M_r \varepsilon^2 \right\}. \quad (29)$$

In the following analysis, we use channel model (28) and (29) to perform robust waveform design. By using  $\tilde{\Delta}\mathbf{H}_{re}$ , 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

$$\max_{A, \Omega_z, t} \frac{1}{2} \{C_d(A, \Omega_z) - \log_2(t)\} \quad (30a)$$

$$\text{s.t.:} \quad \max_{\tilde{\Delta}\mathbf{H}_{re} \in \tilde{\mathcal{Q}}_{re}} C_e(A, \Omega_z) \leq \log_2(t) \quad (30b)$$

$$(15c) - (15d). \quad (30c)$$

The solution procedure of (30) is similar to the procedure in Section IV. It also has two components: 1) *inner step* and 2) *outer step*. The details are given as follows.

#### A. Inner Step

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

$$\gamma_d^*(t) \triangleq \max_{A, \Omega_z} \frac{AE_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2}{\mathbf{w}^H (\mathbf{A} \mathbf{H}_{rd} \mathbf{H}_{rd}^H + \mathbf{H}_{rd} \Omega_z \mathbf{H}_{rd}^H + \mathbf{I}) \mathbf{w}} \quad (31a)$$

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

$$(15c) - (15d) \quad (31c)$$

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

$$f(\mathbf{X}) \geq 0, \text{ for all } \mathbf{X} \text{ with } \text{Tr}(\mathbf{D} \mathbf{X} \mathbf{X}^H) \leq 1 \quad (32)$$

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

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

Now, we apply Lemma 1 to constraint (31b). For notational simplicity, we define  $g(A, \Omega_z) \triangleq \mathbf{A} \mathbf{I} + \Omega_z - (E_s/t - 1) \mathbf{A} \mathbf{H}_{sr} \mathbf{s} \mathbf{s}^H \mathbf{H}_{sr}^H$ . Plugging (28) into (31b) and doing some mathematical manipulation, we have  $\mathbf{X} = \tilde{\Delta}\mathbf{H}_{re}^H$ ,  $\mathbf{A} = g(A, \Omega_z)$ ,  $\mathbf{B} = g(A, \Omega_z) \hat{\mathbf{H}}_{re}^H$ , and  $\mathbf{C} = \hat{\mathbf{H}}_{re} g(A, \Omega_z) \hat{\mathbf{H}}_{re}^H + \mathbf{I}$ . From (29) we also have  $\mathbf{D} = (M_r \varepsilon^2)^{-1} \mathbf{I}$ . Thus, the constraint (31b)

is transformed into a linear matrix inequality constraint of  $\{A, \Omega_z\}$  as

$$U(A, \Omega_z, \xi) \triangleq \begin{bmatrix} \hat{\mathbf{H}}_{re} g(A, \Omega_z) \hat{\mathbf{H}}_{re}^H + \mathbf{I} & \hat{\mathbf{H}}_{re} g(A, \Omega_z) \\ g(A, \Omega_z) \hat{\mathbf{H}}_{re}^H & g(A, \Omega_z) \end{bmatrix} - \xi \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & -(M_r \varepsilon^2)^{-1} \mathbf{I} \end{bmatrix} \geq \mathbf{0}. \quad (34)$$

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

$$\gamma_d^*(t) \triangleq \max_{\bar{A}, \bar{\Omega}_z, \bar{\xi}, \mu} \bar{A} E_s \|\mathbf{w}^H \mathbf{H}_{rd} \mathbf{H}_{sr} \mathbf{s}\|^2 \quad (35a)$$

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

$$(19b), (19d), (19e) \quad (35c)$$

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

### B. Outer Step

After obtaining  $\gamma_d^*(t)$  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  $\Delta \tilde{\mathbf{H}}_{re}$  instead of  $\Delta \mathbf{H}_{re}$ , which makes (30) different from (14). In fact,  $\Delta \mathbf{H}_{re}$ , which has a structure constraint, is a special case of  $\Delta \tilde{\mathbf{H}}_{re}$ . Following this, we have

$$\mathcal{Q}_{re} \subseteq \tilde{\mathcal{Q}}_{re}. \quad (36)$$

In the *inner step* of the solution procedure of (30), constraint (31b) should be satisfied on the whole  $\tilde{\mathcal{Q}}_{re}$ . 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  $\gamma_d^*(t)$  will be lower than the one obtained by using  $\mathcal{Q}_{re}$ . Since the optimal result of *inner step* is a lower bound, the final optimal result after the outer 1-D 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 Sections IV and V also apply to the multieavesdropper case. When there are  $M$  ( $M > 1$ ) eavesdroppers, they can either work in the noncolluding manner or the colluding manner. For the noncolluding 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

$$\mathbf{y}_e(k) = \sqrt{A E_s} b(k) \tilde{\mathbf{H}}_{re} \mathbf{H}_{sr} \mathbf{s} + \sqrt{A} \tilde{\mathbf{H}}_{re} \mathbf{n}_r + \tilde{\mathbf{H}}_{re} \mathbf{z} + \tilde{\mathbf{n}}_e \quad (37)$$

where

$$\mathbf{y}_e(k) = \begin{bmatrix} \mathbf{y}_e^{(1)}(k) \\ \vdots \\ \mathbf{y}_e^{(M)}(k) \end{bmatrix} \quad \tilde{\mathbf{H}}_{re} = \begin{bmatrix} \mathbf{H}_{re}^{(1)} \\ \vdots \\ \mathbf{H}_{re}^{(M)} \end{bmatrix} \quad \tilde{\mathbf{n}}_e = \begin{bmatrix} \mathbf{n}_e^{(1)} \\ \vdots \\ \mathbf{n}_e^{(M)} \end{bmatrix} \quad (38)$$

with the superscript denoting the  $m$ th ( $1 \leq m \leq M$ ) 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.,  $\mathbf{h}_m = d_m^{-\alpha/2} \tilde{\mathbf{h}}_m$ ,  $m \in \{sr, rd, re\}$ , where  $d_m$  is the distance between two communication nodes and  $\alpha$  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 AN, 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  $E_s = E_r = E_0$ . The transmission distances of the source-relay link and relay-destination link are fixed as  $d_{sr} = 3$  m and  $d_{rd} = 5$  m, respectively. The number of multipaths of the source-relay link is fixed as  $L_r = 3$ . The path-loss exponent  $\alpha$  is given as  $\alpha = 2$  unless otherwise specified.

We first present some numerical results for the case with perfect CSI in Figs. 2 and 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  $\mathbf{H}_{rd}$  is a full column rank matrix and there is no null space, employing AN can still improve secrecy rate. What is 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  $d_{re} = 7$  m is larger than the rate for  $d_{re} = 5$  m. This is expected since eavesdropper suffers from severer propagation loss when  $d_{re}$  is larger. From Fig. 2(b) one can see that when the transmit energy is not large enough (e.g., from 15 to 23 dB), 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



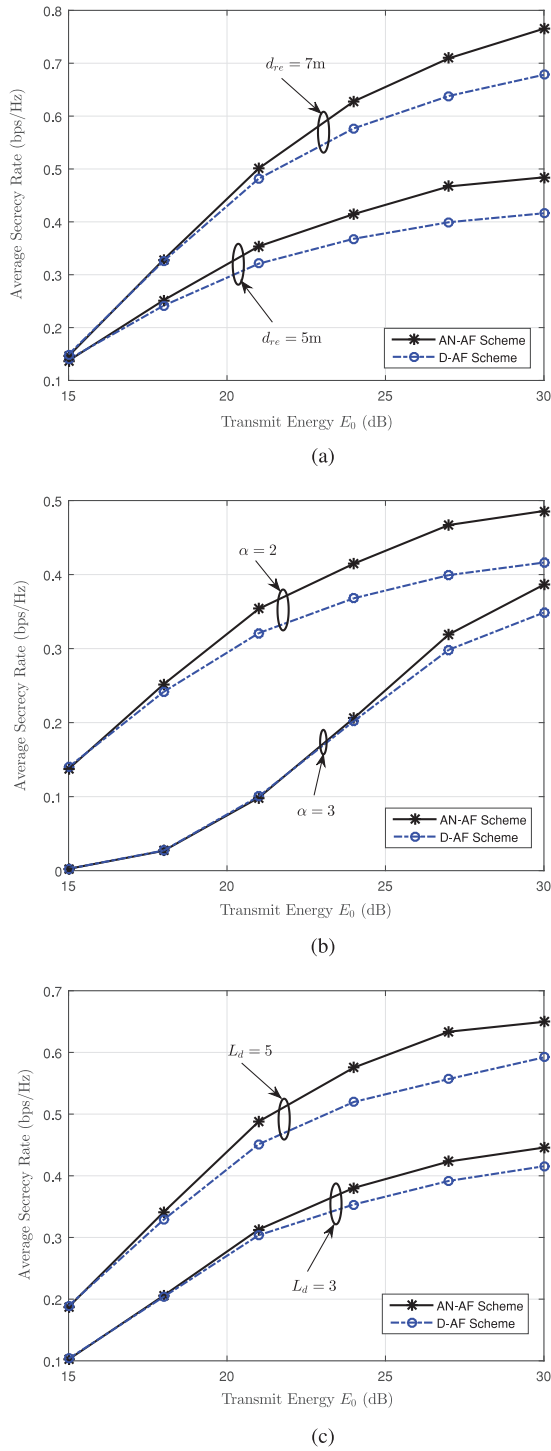


Fig. 2. Perfect CSI: Average secrecy rate as a function of transmit energy with different simulation settings. (a) Different distances between relay and eavesdropper with  $N = 10$  and  $L_d = L_e = 3$ . (b) Different path-loss exponents with  $N = 10$ ,  $d_{re} = d_{rd} = 5$  m, and  $L_d = L_e =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

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 multiantenna system, more paths is equivalent to more receive antennas, which can improve the decoding capability

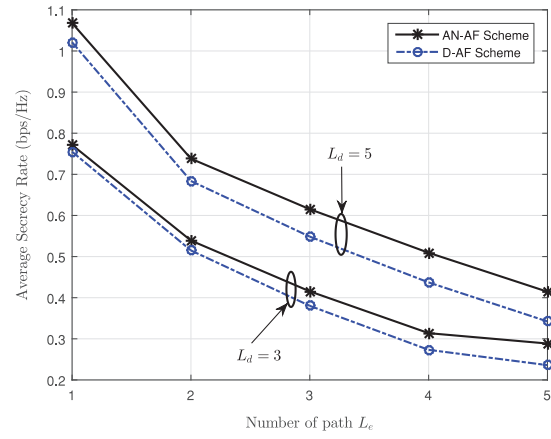


Fig. 3. Perfect CSI: average secrecy rate as a function of the number of relay-eavesdropper link's multipaths for different  $L_d$ . Other simulation settings are  $N = 16$ ,  $E_0 = 27$  dB, and  $d_{re} = d_{rd} = 5$  m.

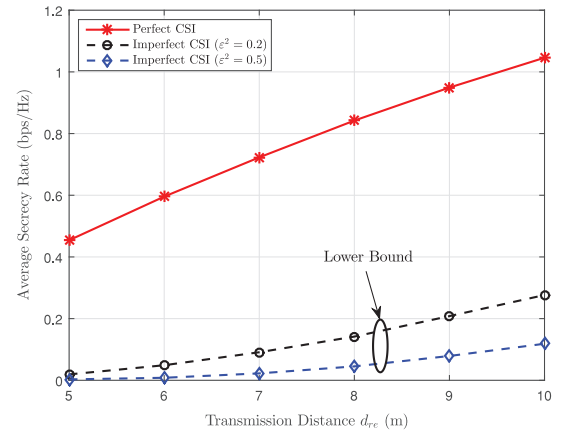


Fig. 4. AN-AF scheme with imperfect CSI: average secrecy rate as a function of the transmission distance of the relay-eavesdropper link. Other simulation settings are  $N = 10$ ,  $E_0 = 30$  dB, and  $L_d = L_e = 3$ .

at the receiver. Hence, when  $L_e$  is fixed, larger  $L_d$  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  $L_d$ . It is observed that the secrecy rate decreases with the increase of  $L_e$ . This is expected since eavesdropper's decoding capability improves with the increase of  $L_e$ , which has been explained in Fig. 2(c). Furthermore, one can see that the performance gap between two schemes is more obvious when either  $L_d$  or  $L_e$  gets larger. That is, the gap increases when the equivalent channel matrix  $\mathbf{H}_{rd}$  or  $\mathbf{H}_{re}$  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 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



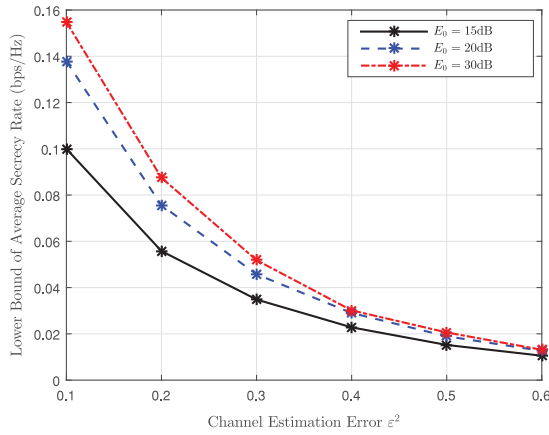


Fig. 5. AN-AF scheme with imperfect CSI: average secrecy rate as a function of channel estimation error for different transmit energy. Other simulation settings are  $N = 10$ ,  $d_{re} = 7$  m, and  $L_d = L_e = 3$ .

in Fig. 4, the average secrecy rates of the imperfect-CSI situation are much smaller than those of perfect-CSI situation. The larger the  $\varepsilon^2$  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  $d_{re}$ . 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  $\varepsilon^2$ , 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  $\varepsilon^2$  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 dashed-dotted line. This implies that when the transmit energy is high enough, the further enhancement of energy can not improve secrecy rate significantly.

## VII. CONCLUSION

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 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 an SISO relay network with multipath receptions. Specifically, we proposed an AN-AF strategy which required the relay to forward the source message and inject AN 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 1-D 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. Comput. Sci. Appl. (ICCSA)*, Salvador, Brazil, Jun. 2012, pp. 146–150.
- [2] Q. Du *et al.*, "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 Netw.*, vol. 29, no. 4, pp. 62–67, Jul./Aug. 2015.
- [4] W. Wolf, "News briefs," *Computer*, vol. 40, no. 11, pp. 104–105, Nov. 2007.
- [5] H. Kagermann, W. Wahlster, and J. Helbig, "Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative Industrie 4.0," Final Rep. Industrie 4.0 Working Group, Fed. Ministry Educ. Res., Frankfurt, Germany, Apr. 2013.
- [6] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, *Cyber-Physical Systems: Foundations, Principles and Applications*. Boston, MA, USA: 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 *et al.*, "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 *et al.*, "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 Res.*, 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 Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Montreal, QC, Canada, Jun. 2009, pp. 49–57.
- [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 Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–10.
- [15] H. Song, G. A. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems*. Chichester, U.K.: 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. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 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 *et al.*, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, 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./Oct. 2009, pp. 911–918.
- [20] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Netw.*, vol. 30, no. 2, pp. 62–66, Mar./Apr. 2016.

- [21] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE Internet Things 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 *et al.*, "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. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 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.*, to be published.
- [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. Syst., Man, Cybern. C, Appl. Rev.*, 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. Informat.*, 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 Appl.*, vol. 75, no. 9, pp. 5345–5357, 2016.
- [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, pp. 1–5.
- [41] M. Paolini. (2011). *Beyond Data Caps: An Analysis of the Uneven Growth in Data Traffic*. [Online]. Available: <http://www.senzafileconsulting.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, U.K.: Cambridge Univ. Press, 2004.
- [44] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logistics Quart.*, vol. 9, nos. 3–4, pp. 181–186, Dec. 1962.
- [45] M. Grant and S. Boyd. (Apr. 2011). *CVX: MATLAB Software for Disciplined Convex Programming*. [Online]. Available: <http://cvxr.com/cvx>
- [46] D. P. Bertsekas, *Nonlinear Programming*, 2nd ed. Belmont, MA, USA: Athena Sci., 1999.
- [47] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. Optim.*, vol. 14, no. 4, pp. 1140–1162, 2004.
- [48] H.-M. 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. Forens. Security*, vol. 9, no. 8, pp. 1240–1250, Aug. 2014.



**Qian Xu** received the B.S. degree from Xi'an Jiaotong University, Xi'an, China, in 2014, where she is currently pursuing the Ph.D. degree at the Department of Information and Communications Engineering.

Her current research interests include wireless physical-layer security, device-to-device communications, and cooperative relaying networks.



**Pinyi Ren** received the B.S., M.S., and Ph.D. degrees from Xi'an Jiaotong University, Xi'an, China.

He is currently a Professor with the Information and Communications Engineering Department, Xi'an Jiaotong University. His current research interests include cognitive radio networks, MIMO systems, game theory in wireless communications, wireless relay, routing, and signal detection.



**Houbing Song** received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012.

Since 2012, he has been an Assistant Professor with the Department of Electrical and Computer Engineering, West Virginia University Institute of Technology, Montgomery, WV, USA. His current research interests include optical communications, wireless communications and networking, vehicular networking, smart grid communications, and cyber-physical systems.



**Qinghe Du** received the B.S. and M.S. degrees from Xi'an Jiaotong University, Xi'an, China, and the Ph.D. degree from Texas A&M University, College Station, TX, USA.

He is currently an Assistant Professor with the Information and Communications Engineering Department, Xi'an Jiaotong University. His current research interests include mobile wireless communications and networking with an emphasis on mobile multicast, statistical QoS provisioning, and cognitive radio networks.