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.2019.2908821, IEEE Internet of Things Journal

Secure Beamforming Design in Relay-Assisted Internet of Things

Pingmu Huang, Yunqin Hao, Tiejun Lv, *Senior Member, IEEE*, Jintao Xing, Jie Yang, and P. Takis Mathiopoulos, *Senior Member, IEEE*

***Abstract*—A secure downlink transmission system which is exposed to multiple eavesdroppers and is appropriate for Internet of Things (IoT) applications is considered. A worst case scenario is assumed, in the sense that, in order to enhance their interception ability all eavesdroppers are located close to each other, near the controller and collude to form joint receive beamforming. For such a system, a novel cooperative non-orthogonal multiple access (NOMA) secure transmission scheme for which an IoT device with a stronger channel condition acts as an energy harvesting relay in order to assist a second IoT device operating under weaker channel conditions, is proposed and its performance is analyzed and evaluated. A secrecy sum rate (SSR) maximization problem is formulated and solved under three constraints: i) Transmit power; ii) Successive interference cancellation; iii) Quality of Service. By considering both passive and active eavesdroppers scenarios, two optimization schemes are proposed to improve the overall system SSR. On the one hand, for the passive eavesdropper scenario, an artificial noise-aided secure beamforming scheme is proposed. Since this optimization problem is non-convex, instead of using traditional but highly complex, brute-force two-dimensional search, it is conveniently transformed into a convex one by using an epigraph reformulation. On the other hand, for the active multi-antennas eavesdroppers' scenario, the orthogonal-projection-based beamforming scheme is considered, and by employing the successive convex approximation method, a suboptimal solution is proposed. Furthermore, since for single antenna transmission the orthogonal-projection-based scheme may not be applicable a simple power control scheme is proposed. Various performance evaluation results obtained by means of computer simulations have verified that the proposed schemes outperform other benchmark schemes in terms of SSR performance.**

***Index Terms*—Internet of Things (IoT), secure beamforming, artificial noise (AN), orthogonal projection, secrecy sum rate (SSR).**

I. Introduction

The Internet of Things (IoT) is rapidly evolving as a complex platform connecting a very large number of communication devices, e.g. sensors, controllers and actuators [1]. However, achieving the required ubiquitous connectivity required for such IoT based communication systems becomes a vital and challenging task mainly because of the constraint of scarce bandwidth. In this context, nonorthogonal multiple access (NOMA) is advocated as a promising technique to support pervasive connectivity, so that the spectral efficiency of IoT systems can be significantly enhanced [2]–[6]. The key feature of NOMA is to implement the multiple access (MA) in the power domain while the time/frequency/code resources can simultaneously be shared by all users. Moreover, as compared to orthogonal MA (OMA), NOMA can achieve a better balance between sum rate and user fairness [7]. At the same time, as the wireless broadcast nature of radio propagation makes IoT communications susceptible to eavesdropping attacks, their security aspects need to be very carefully considered when designing such systems. In the past, conventional encryption techniques have been applied to prevent eavesdroppers from recovering the secret messages [8], [9]. However, such encryption-based techniques have inherent difficulties and vulnerabilities dealing with secret key management [1]. Fortunately, physical layer security (PLS) has shown a great deal of potential to more accurately distinguish the signals belonging to the legitimate receiver or the eavesdropper [10]–[12]. Unlike other encryption-based techniques, PLS techniques take advantage of the physical characteristics of wireless medium to ensure information-theoretic security independent of the eavesdropper's computing capabilities [13], [14].

A. Motivation and Contributions

In the past, several PLS techniques based on the OMA secure transmission protocol, including multi-antennas techniques [15], [16], artificial noise (AN) [17]–[23] and cooperative jamming (CJ) [24]–[26] have been proposed. Aiming to further improve the secrecy of the fifth generation (5G) systems, Tian *et al*. [2] combined NOMA with multi-antennas techniques to optimize the secrecy sum rate (SSR) of 5G wireless system for applications where the channel state information (CSI) of eavesdroppers is available. In another approach, Hu *et al*. [1] have combined the AN assisted multi-antennas transmission technique with CJ in order to reduce the effects of the passive non-colluding eavesdroppers for the IoT downlink. However, since many IoT device transmitters have limited radio frequency (RF) power, allocating some power for AN or jamming signal may not be appropriate since this will restrict the coverage range of secure transmissions.

In order to fill this gap, in this paper a novel relay-assisted secure transmission scheme is proposed designed for energy-constrained IoT based communication systems, where one

The financial support of the National Natural Science Foundation of China (NSFC) (Grant No. 61671072) is gratefully acknowledged. (*Corresponding author: Tiejun Lv.*)

P. Huang, Y. Hao, T. Lv, J. Xing and J. Yang are with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China (e-mail: {pmhuang, haoyunqin, lvtiejun, jintaoxing, janeyang}@bupt.edu.cn).

P. T. Mathiopoulos is with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Athens 157 84, Greece (e-mail: mathio@di.uoa.gr).

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.2019.2908821, IEEE Internet of Things Journal

controller emits secret messages to two classes of devices operating in the presence of multiple colluding eavesdroppers. These IoT devices have diversified quality of service (QoS) requirements, and the channel conditions among them are quite different in the sense that the channel operating conditions for D_1 are much better then the channel conditions for D_2. In order to guarantee the confidentiality of data transmission and the QoS requirement of D_2, D_1 acts as an energy harvesting (EH) relay to help D_2. Assuming that the locations of all eavesdroppers are close to the controller, this worst-case positioning scheme will increase the probability of interception of the information signal. For this energy-constraint IoT system, a novel secure cooperative transmission scheme is proposed and its performance is analyzed and evaluated. Assuming that the CSI of the eavesdroppers is available, two operational scenarios are considered, namely the passive eavesdroppers and active eavesdroppers scenarios, for which two optimization. For maximizing the SSR of the IoT system under consideration under transmit power, QoS and successive interference cancellation (SIC) constraints. Within this framework, the primary contributions of this paper are summarized as follows:

- A cooperative simultaneous wireless information and power transfer (SWIPT) secure transmission protocol which takes into account the diversified QoS requirements of different IoT users, is proposed. Unlike secure transmission designs without SWIPT [1], [2], by employing the SWIPT-aided transmission protocol, device 1 forwards the information bearing signal and AN without introducing additional energy consumption.
- For the passive eavesdroppers scenario, an AN-aided secure beamforming scheme which jointly optimizes the transmit beamforming vectors, power splitting (PS) ratio and AN beamforming, is proposed. Since this optimization problem is non-convex, it is conveniently transformed into a convex form through the use of a epigraph reformulation (ER), instead of using the two-dimensional search [27] that requires high computational complexity.
- For the active eavesdroppers scenario, an orthogonal-projection-based secure beamforming design scheme which ensures the confidentiality of data transmission is proposed. As this challenging optimization problem is also non-convex, the NP-hard problem is reformulated into a trackable convex problem. Furthermore, for single antenna transmitters, the orthogonal-projection-based beamforming design problem simplifies to a power allocation problem which should not be solved via the orthogonal projection based method. Instead, a power control scheme is proposed through which via a transformation of the objective function and constraints the non-convex problem can be efficiently handled.

B. Related Previous Research

There has been recently a lot of interest from the information-theoretic point of view, to exploit PLS techniques in order to improve the security of wireless communication systems [21], [23], [24]. For example, considering multiple-input single-output channels (SISO), the cases of both direct transmission and CJ with a helper have been investigated under the assumption that CSI for the wiretap links is imperfect [22]. For multiple-input multiple-output (MIMO) channels, [25] proposed a CJ-aided SSR optimization scheme under the assumption that the power of the system is sufficient. Furthermore, [23], [26] have focused on studying the confidential information transmission of relay systems with the PLS techniques-aided. The secure transmission schemes introduced in these two papers are based on the assumption that available power of the considered relay systems is sufficient. More recently in [21], a robust secure beamforming design for MIMO two-way relaying system based on the AN and physical layer network coding has been introduced. Various performance evaluation results presented in [21] have shown that such beamforming design will further improve the security aspects of the two-way relaying system.

It is underlined that the above mentioned papers ([21]–[26]) investigate various PLS issues encountered in different cooperative wireless communication systems without considering possible energy-limited constraints. Furthermore, these papers have not investigated the security transmission problem in connection with IoT type of wireless communication systems. On this topic, [1], [9], [14], different PLS-based secure transmission schemes have been presented for IoT systems. However these papers have not considered the energy-limited feature of IoT systems when designing the secure transmission beamforming.

To this end, it is necessary to solve the security problem of the energy-constrained IoT systems with EH-assisted. In this paper SWIPT is considered as an EH technique where the IoT transmitter forwards information signal and AN via the harvested energy only. Our work is different from above works in the following aspects: i) [1] investigates the secure transmission problem of IoT system, from an information-theoretic point of view, and only the CJ technique is used so that the coverage range of secure transmissions couldn't be guaranteed; ii) [9] considers a variety of eavesdropping scenarios when designing the secure transmission protocols, but colluding eavesdroppers cases are not explored; iii) [14] considers a secure transmission for IoT under eavesdropper collusion. Although the scheme proposed in [14] is more general than that the schemes presented in [1] and [9], it has not considered secure beamforming design nor the energy-constrained problem. Note in our research here we not only provide secure beamforming designs, but also the energy-constrained problem is considered by combining the PLS technique with SWIPT.

C. Notation and Organization: The remainder of this paper is organized as follows: In Section II, we describe the system model and problem formulation. In Section III, AN-aided transmission beamforming design scheme is presented when eavesdroppers' CSI is unavailable. In Section IV, by taking both the single-antenna and multiple-antenna scenarios into account, two SSR optimization schemes are proposed when the eavesdropper's CSI is available. The performance evaluation results and discussion are provided in Section IV. The conclusions of the paper can be found in Section VI.

Boldface lowercase and uppercase letters denote vectors

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.2019.2908821, IEEE Internet of Things Journal

Table I
PARAMETERS AND THEIR MEANINGS

N_s	Number of Antennas of the Controller
N_i	Number of Antennas of the D_i
N_e	Number of Eavesdroppers
$\mathbf{v}_i$	Transmit Beamforming Vector at Controller S
s_i	Transmitted Symbol for D_i
β	Power Splitting Ratio
τ	Transmission Time Fraction
$\mathbf{w}$	Transmit Beamforming Vector at D_1
$\mathbf{z}$	Artificial Noise Vector
P_s	Total Transmit Power at Controller
P_t	Maximum Power Transmitted at D_1
E	Energy Harvested by D_1
R_i	Achievable Rate for Devices D_i, $i \in \{1,2\}$
R_{sum}	Secrecy Sum Rate for the IoT System
γ_i	Received SINR at D_i
μ	Mean of the Gaussian Noise Distribution
σ^2	Noise Power

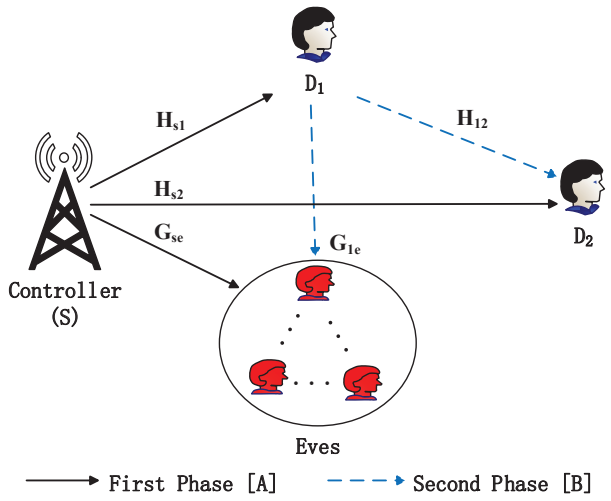

Fig. 1. Model for the secure cooperative IoT based communication system under consideration

and matrices, respectively. The Hermitian transpose, Frobenius norm, and trace of the matrix $\mathbf{A}$ are denoted as $\mathbf{A}^H$, $\|\mathbf{A}\|$, and $\mathrm{Tr}(\mathbf{A})$, respectively, whereas $\mathrm{rank}(\mathbf{A})$ and $|\mathbf{A}|$ stand for the rank and the determinant of the matrix $\mathbf{A}$, respectively. By $\mathbf{A} \succeq \mathbf{0}$ or $\mathbf{A} \succ \mathbf{0}$, it is meant that the matrix $\mathbf{A}$ is positive semidefinite or positive definite, respectively. $\mathbf{I}_M$ is the identity matrix of size $M \times M$. $\mathbb{C}^{\mathbb{N}\times\mathbb{M}}$ denotes an $N \times M$ complex matrix. $\mathrm{diag}\,(\mathbf{A})$ is a diagonal matrix with the entries of matrix $\mathbf{A}$ as its diagonal entries. $[\cdot]^+ \triangleq \max\{0, \cdot\}$. $|\cdot|$ and $\mathbb{E}\{\cdot\}$ denote the absolute value and the statistical expectation, respectively. $\succeq$ represents the property of semidefinite. $\mathcal{CN}\left(\mu, \sigma^2\right)$ denotes the circularly symmetric complex Gaussian distribution with mean μ and variance σ^2. $I\left(.;.\right)$ is the mutual information. Additionally, a list of the most important system parameters and their meaning can be found in Table I.

II. System Model

As illustrated in Fig. 1, an IoT downlink secure communication system consisting of a controller, S, equipped with N_s-antenna and two user devices, $D_i (i \in \{1,2\})$[1] each equipped with N_i antennas is considered. S transmits confidential information to the D_i in the presence of N_e colluding eavesdroppers, Eves[2].

It is also assumed that D_1, which operates under better channel conditions, is used for receiving rather short control signal data. D_2, which operated under weak channel conditions, which is a device which deals with some background tasks, such as downloading multimedia files. As illustrated in Fig. 1, the Eves G_{1e} are located close to each other and all of them are close to S. Clearly, such configuration will lead to higher probabilities of interception for the transmitted information signal.

To ensure the high targeted secrecy rate of D_2, D_1 acts as an EH relay to forward the information-bearing signal to D_2. More specifically, the received signal at D_1 is split into two parts: one for energy harvesting and the other for information decoding so that two stages will be involved in the cooperative NOMA secure transmission. At D_2 the two signals received are combined by a maximal ratio combining (MRC) diversity scheme. It is assumed that all the fading channels shown in Fig. 1 are independent quasi-static fading channels, which remain constant in one time slot but vary independently from one time slot to another. Next the detailed operation of the proposed communication system will be presented.

A. Direct Transmission Phase A: As illustrated in Fig. 1, during the 1^{st} stage of communication, S transmits over the channels H_{s1} and H_{s2} the information signals s_1 and s_2 which, after beamforming, are received by D_1 and D_2 as signals $y_1^{[A]}$ and $y_2^{[A]}$, respectively. These beamformed signals are also intercepted through the G_{se} channel by the Eves, as $y_e^{[A]}$.

D_1 performs EH by employing a SWIPT receiver in order to perform the necessary PS. Noting that the received signals are also corrupted by independent additive white Gaussian noise (AWGN), they can be mathematically expressed as:

$$\mathbf{y}_1^{[A]} = \sqrt{(1-\beta)}\mathbf{H}_{s1}\left(\mathbf{v}_1 s_1 + \mathbf{v}_2 s_2\right) + \mathbf{n}_1^{(1)}, \quad (1a)$$

$$\mathbf{y}_2^{[A]} = \mathbf{H}_{s2}\left(\mathbf{v}_1 s_1 + \mathbf{v}_2 s_2\right) + \mathbf{n}_2^{(1)}, \quad (1b)$$

$$\mathbf{y}_e^{[A]} = \mathbf{G}_{se}\left(\mathbf{v}_1 s_1 + \mathbf{v}_2 s_2\right) + \mathbf{n}_e^{(1)}. \quad (1c)$$

In (1), s_i is the transmitted information symbol for D_i, which has unity energy, i.e. $\mathbb{E}\left\{|s_i|^2\right\} = 1$; $\mathbf{v}_i \in \mathbb{C}^{N_s \times 1}$ is the transmit beamforming vector at S; $\mathbf{H}_{si} \in \mathbb{C}^{N_i \times N_s}$ and $\mathbf{G}_{se} \in \mathbb{C}^{N_e \times N_s}$ are the channel responses from S to D_i and Eves, respectively; $\beta \in [0,1]$ is the PS ratio; $\mathbf{n}_i^{(1)} \sim \mathcal{CN}\left(0, \sigma_i^2 \mathbf{I}_{N_i}\right)$ and $\mathbf{n}_e^{(1)} \sim \mathcal{CN}\left(0, \sigma_e^2 \mathbf{I}_{N_e}\right)$ are the additive white complex Gaussian noise vectors at D_i and Eves, respectively. For simplicity and without any loss of generality, it is assumed that $\sigma_1^2 = \sigma_2^2 = \sigma_e^2 = \sigma^2$. Since the channel conditions for both D_1 and Eves are better than that of D_2,

[1]From now on, and unless otherwise specified, the index i will always takes values from the alphabet {1,2}.

[2]It is noted that, although the proposed system model considers only two devices as a pair of users [28], this pairing can be generalized to multiple users following the methodology we have proposed in [29]. However, this extension is beyond the scope of our current research work and as such will not be considered here.

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.2019.2908821, IEEE Internet of Things Journal

clearly $\|\mathbf{H}_{s2}\|^2 \leq \|\mathbf{H}_{s1}\|^2$, and $\|\mathbf{H}_{s2}\|^2 \leq \|\mathbf{G}_{se}\|^2$. The received signals $y_1^{[A]}$ and $y_2^{[B]}$ are decoded by employing the following SIC principles. For D_1, as it assumed that it operates under good channel conditions, it will first detect the message s_2, which is intended for D_2, and then eliminate it from the combined signal. On the contrary, D_2, as it operates under bad channel conditions, it will not try to eliminate s_1, which is intended for D_1, from the combined signal. Thus, from (1a), the received signal-to-interference-plus-noise-ratio (SINR) at D_1 for detecting s_2 can be mathematically expressed as

$$\mathrm{SINR}_{1,s_2}^{[A]} = \frac{(1-\beta)\|\mathbf{H}_{s1}\mathbf{v}_2\|^2}{(1-\beta)\|\mathbf{H}_{s1}\mathbf{v}_1\|^2 + \sigma^2}, \tag{2}$$

which should be larger than or equal to a predefined threshold so that the QoS constraint at D_1 can be satisfied. Then,for the decoding of s_1 at D, the corresponding received signal-to-noise-ratio (SNR) is given by

$$\mathrm{SNR}_{1,s_1}^{[A]} = \frac{(1-\beta)\|\mathbf{H}_{s1}\mathbf{v}_1\|^2}{\sigma^2}. \tag{3}$$

From (1b), the SINR at D_2 to detect s_2 becomes

$$\mathrm{SINR}_{2,s_2}^{[A]} = \frac{\|\mathbf{H}_{s2}\mathbf{v}_2\|^2}{\|\mathbf{H}_{s2}\mathbf{v}_1\|^2 + \sigma^2}. \tag{4}$$

Furthermore, the energy harvested by D_1 can be formulated as [30]

$$E = \beta\left(\|\mathbf{H}_{s1}\mathbf{v}_1\|^2 + \|\mathbf{H}_{s1}\mathbf{v}_2\|^2\right)\tau, \tag{5}$$

where $\tau = \frac{1}{2}$ is the transmission time fraction for the first phase, and the two phases have the same transmission duration. It is assumed that the energy harvested by D_1 is mainly used for transmitting information and AN. Therefore, the maximum power transmitted at D_1 is given by [31]

$$P_t = \frac{E}{1-\tau} = \beta\left(\|\mathbf{H}_{s1}\mathbf{v}_1\|^2 + \|\mathbf{H}_{s1}\mathbf{v}_2\|^2\right). \tag{6}$$

B. Cooperative Transmission Phase B: During the 2nd phase of transmission, s_2 is beamformed by $\mathbf{w} \in \mathbb{C}^{N_1\times 1}$ and broadcast together with AN to D_2 with the harvested energy. Thus, the signal transmitted by D_1 can be expressed as

$$\mathbf{x} = \mathbf{w}s_2 + \mathbf{z}, \tag{7}$$

where $\mathbf{z}$ is the AN beamforming vector generated by D_1, whose distribution follows $\mathcal{CN}(0, \mathbf{\Sigma})$ with $\mathbf{\Sigma} \succeq \mathbf{0}$. Then, the observations at D_2 and at the Eves can be expressed as

$$\mathbf{y}_2^{[B]} = \mathbf{H}_{12}\mathbf{x} + \mathbf{n}_2^{(2)}, \tag{8a}$$

$$\mathbf{y}_e^{[B]} = \mathbf{G}_{1e}\mathbf{x} + \mathbf{n}_e^{(2)}, \tag{8b}$$

respectively, where $\mathbf{H}_{12} \in \mathbb{C}^{N_2\times N_1}$ and $\mathbf{G}_{1e} \in \mathbb{C}^{N_e\times N_1}$ are the channel responses from D_1 to D_2 and to the Eves, respectively. $\mathbf{n}_2^{(2)} \sim \mathcal{CN}\left(0, \sigma^2\mathbf{I}_{N_2}\right)$ and $\mathbf{n}_e^{(2)} \sim \mathcal{CN}\left(0, \sigma^2\mathbf{I}_{N_e}\right)$ are the additive white complex Gaussian noise vectors at D_2 and Eves, respectively. Consequently, the SINR at D_2 to detect s_2 can be written as

$$\mathrm{SINR}_{2,s_2}^{[B]} = \frac{\|\mathbf{H}_{12}\mathbf{w}\|^2}{\|\mathbf{H}_{12}\mathbf{z}\|^2 + \sigma^2}. \tag{9}$$

Thus, the combined SINR at D_2 becomes

$$\mathrm{SINR}_{2,s_2} = \mathrm{SINR}_{2,s_2}^{[A]} + \mathrm{SINR}_{2,s_2}^{[B]}. \tag{10}$$

As previously noted, s_2 is jointly detected at D_2 from the signals received from S and D_1 by employing MRC diversity reception.

From (1c) and (8b), the received signal of Eves for the two phases can be given by

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{s} + \mathbf{n}_e, \tag{11}$$

where

$$\mathbf{y}_e = \begin{bmatrix} \mathbf{y}_e^{[A]} \\ \mathbf{y}_e^{[B]} \end{bmatrix}, \mathbf{s} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}, \tag{12a}$$

$$\mathbf{H}_e = \begin{bmatrix} \mathbf{G}_{se}\mathbf{v}_1 & \mathbf{G}_{se}\mathbf{v}_2 \\ \mathbf{0}_{N_e\times 1} & \mathbf{G}_{1e}\mathbf{w} \end{bmatrix}, \tag{12b}$$

$$\mathbf{n}_e = \begin{bmatrix} \mathbf{n}_e^{(1)} \\ \mathbf{G}_{1e}\mathbf{z} + \mathbf{n}_e^{(2)} \end{bmatrix}. \tag{12c}$$

From (11), the information sum rate leaked to the Eves can be written as [15]

$$R_e = I\left(s_i; \mathbf{y}_e\right) = \frac{1}{2}\log\left|\mathbf{I}_{N_e} + \mathbf{H}_e\mathbf{H}_e^H\mathbf{Q}_e^{-1}\right| = \frac{1}{2}\log\left(1 + \frac{\mathrm{Tr}\left(\mathbf{G}_{\mathrm{se}}\left(\sum_{\mathrm{i}=1}^{2}\mathbf{v}_i\mathbf{v}_i^{\mathrm{H}}\right)\mathbf{G}_{\mathrm{se}}^{\mathrm{H}} + \mathbf{G}_{1\mathrm{e}}\mathbf{w}\mathbf{w}^{\mathrm{H}}\mathbf{G}_{1\mathrm{e}}^{\mathrm{H}}\right)}{\mathrm{Tr}\left(\mathbf{Q}_e\right)}\right), \tag{13a}$$

where $\mathbf{Q}_e = \mathbf{n}_e\mathbf{n}_e^H = \mathrm{diag}\left(\sigma^2\mathbf{I}_{N_e}, \sigma^2\mathbf{I}_{N_e} + \mathbf{G}_{1e}\mathbf{\Sigma}\mathbf{G}_{1e}^H\right)$, $i \in \{1, 2\}$, and the factor $\frac{1}{2}$ is introduced since the messages are transmitted in two consecutive phases [32]. Note that the minimum-mean-square-error criterion and SIC have been employed by Eves. The achievable rates of D_1 and D_2 are given by

$$R_1 = I\left(s_1; \mathbf{y}_1\right) = \frac{1}{2}\log\left(1 + \mathrm{SNR}_{1,s_1}\right), \tag{14a}$$

$$R_2 = I\left(s_2; \mathbf{y}_2\right) = \frac{1}{2}\log\left(1 + \mathrm{SINR}_{2,s_2}\right), \tag{14b}$$

respectively. As pointed out it [32], it is very difficult to obtain the secrecy capacity region of the downlink wireless systems. Alternative, the rate difference between the legitimate sum rate and the information sum rate leaked to the Eves (i.e., R_e) can be computed as the secure performance measure. In this case, the SSR can be expressed as [2]

$$R_{sum} = \left[\sum_{i=1}^{2} R_i - R_e\right]^+. \tag{15}$$

To improve the security of the downlink for the cooperative communication system under consideration, an SSR maximization problem is formulated. The transmit power constraint at S, the SIC constraint at D_1 and the EH constraint should be satisfied in the SSR maximization problem. The EH constraint is that the achievable power for transmitting information bearing signal and AN is smaller than or equal to the energy harvested by D_1. According to the result given

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.2019.2908821, IEEE Internet of Things Journal

in [7], a higher sum rate can be obtained if S allocates more power for the information-bearing signal s_1. However, such an approach is not applicable in the optimization problem consider here for which the user fairness and high targeted secrecy rate at D_2 should be ensured [7]. With the above in mind, the optimization problem considered in this paper can be formulated as

$$\max_{\mathbf{v}_1,\mathbf{v}_2} \; R_{sum} \tag{16a}$$

$$\text{s.t.} \;\; \mathrm{SINR}_{1,s_2} \geq \gamma, \, \mathrm{SINR}_{2,s_2} \geq \gamma, \tag{16b}$$

$$\|\mathbf{v}_1\|^2 + \|\mathbf{v}_2\|^2 \leq P_s, \|\mathbf{w}\|^2 + \|\mathbf{z}\|^2 \leq P_t, \tag{16c}$$

where P_s is the transmit power constraint at S, $\|\mathbf{w}\|^2$ and $\|\mathbf{z}\|^2$ are the allocated power for information transmission and AN, respectively. Note that (16b) indicates that the received SINR to decode s_2 should be no less than the SINR threshold γ, as (16b) relates to the SIC constraint at D_1 to ensure the necessary QoS decoding performance of D_2.

Next the NP-hard problem of (16) will be solved by optimizing $\mathbf{v}_1, \mathbf{v}_2$, $\mathbf{w}$ as well as β for the cases of passive and active Eves (see Sections III and IV, respectively).

III. AN-aided secure beamforming design (ASBD) for the passive eavesdroppers case

In this section, it is assumed that the passive Eves' CSI is not available at the transmitters D_1 and S. For example this occurs when the eavesdropping nodes in IoT systems are passive or malicious. Since in this case even the location of the Eves is hard to obtain [16], and thus obtaining CSI will be even more difficult, a AN-aided beamforming design scheme is proposed.

Zero-Forcing (ZF) Constraint on AN: Since D_1 has no CSI for the Eves, i.e., D_1 doesn't know $\mathbf{G}_{1e}$, in order to eliminate the interference at D_2, a ZF condition on the AN beamforming is applied [21], [23]. In other words, the AN beamforming is designed so that it steers the signal into the null space of $\mathbf{H}_{12}$, so that $\mathbf{H}_{12}\mathbf{z} = \mathbf{0}$. In this way, D_1 cannot transmit AN to interfere the Eves selectively under the Zero Forcing constraint [33]. Hence, the AN $\mathbf{z}$ is in the form of $\mathbf{z} = \mathbf{H}_{\perp}\mathbf{n}$, where $\mathbf{H}_{\perp} = \mathbf{I}_{N_2} - \mathbf{H}_{12}\left(\mathbf{H}_{12}^H\mathbf{H}_{12}\right)^{-1}\mathbf{H}_{12}^H$ is the projection matrix onto the null space of $\mathbf{H}_{12}$. Note that the components of $\mathbf{n}$ are independent and identically distributed (iid) Gaussian variables, which follow $\mathcal{CN}\left(0, \sigma_z^2\right)$ so that the spatial covariance of AN can be expressed as $\mathbf{\Sigma} = \sigma_z^2\mathbf{H}_{\perp}\mathbf{H}_{\perp}^H \succeq \mathbf{0}$.

The SSR R_{sum} is maximized only when R_e is minimized. Thus, in order to minimize R_e, the power allocated for AN should be made as much as possible, under the EH and SIC constraints at D_1, the transmit power constraint at S and QoS constraint at D_i. According to the semidefinite relaxation (SDR) technique, let $\mathbf{V}_i = \mathbf{v}_i\mathbf{v}_i^H, i \in \{1,2\}, \mathbf{W} = \mathbf{w}\mathbf{w}^H$ and drop rank-one constraints $\mathrm{rank}\left(\mathbf{V}_i\right) = 1$, $\mathrm{rank}\left(\mathbf{W}\right) = 1$. Thus, the secure beamforming problem is reformulated as

$$\max_{\mathbf{V}_i \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0}, \beta} \; \mathrm{Tr}\left(\mathbf{\Sigma}\right) \tag{17a}$$

$$\text{s.t.} \quad \left(1 + \frac{(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^1\right)}{\sigma^2}\right) \geq r_1, \tag{17b}$$

$$\left(1 + \frac{\mathrm{Tr}\left(\mathbf{W}_2^2\right)}{\mathrm{Tr}\left(\mathbf{W}_2^1\right) + \sigma^2} + \frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right) \geq r_2, \tag{17c}$$

$$\frac{(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^2\right)}{\sigma^2 + (1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^1\right)} \geq \gamma, \tag{17d}$$

$$\frac{\mathrm{Tr}\left(\mathbf{W}_2^2\right)}{\mathrm{Tr}\left(\mathbf{W}_2^1\right) + \sigma^2} + \frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2} \geq \gamma, \tag{17e}$$

$$\mathrm{Tr}\left(\mathbf{W}\right) + \mathrm{Tr}\left(\mathbf{\Sigma}\right) \leq \beta \mathrm{Tr}\left(\sum_{i=1}^{2} \mathbf{W}_1^i\right), \tag{17f}$$

$$\mathrm{Tr}\left(\mathbf{V}_1\right) + \mathrm{Tr}\left(\mathbf{V}_2\right) \leq P_s. \tag{17g}$$

where $\mathbf{W}_1^i = \mathbf{H}_{s1}\mathbf{V}_i\mathbf{H}_{s1}^H$, $\mathbf{W}_2^i = \mathbf{H}_{s2}\mathbf{V}_i\mathbf{H}_{s2}^H$, $i \in \{1,2\}$, $\mathbf{W}_{12} = \mathbf{H}_{12}\mathbf{W}\mathbf{H}_{12}^H$, r_i is the predefined threshold of achievable ergodic rate of D_i, and $\frac{1}{2}\log(\cdot)$ is not included in (17b) and (17c) since the logarithmic function is a monotonically increasing function. It is noted that the optimization problem (17) is non-convex due to the non-convex constraints (17b)-(17f). Consequently, these non-convex constraints will be transformed into equivalent convex forms based on the idea of SCA, which can be used to iteratively approximate a non-convex optimization problems by an equivalent convex problem [34].

Transformation of (17b): Based on the SCA method and the ER, (17b) can be replaced by the following two constraints

$$\theta_1^2 \geq (r_1 - 1)\,\sigma^2, \tag{18a}$$

$$\begin{bmatrix} (1-\beta) & \theta_1 \\ \theta_1 & \mathrm{Tr}(\mathbf{W}_1^1) \end{bmatrix} \succeq \mathbf{0}. \tag{18b}$$

Lemma 1. *For a standard convex function $g(x)$ and a concave function $f(x)$, if the constraint $g(x) \leq f(x)$ exists, then the constraint is convex [35].*

Based upon the following Lemma, it is clear that (18a) is non-convex. Therefore, the first order Taylor expansion (FOTE) can be utilized to approximate (18a) with the following convex function

$$2\theta_1^{(n)}\theta_1 - (\theta_1^{(n)})^2 \geq (r_1 - 1)\,\sigma^2, \tag{19}$$

where $\theta_1^{(n)}$ is the value of variable θ_1 at the n-th iteration, i.e. the superscript (n) denotes the point obtained during the n-th iteration. Note that the constraint (17b) is now replaced by two convex constraints, i.e., the linear matrix inequality constraint (18b) and the convex constraint (19).

Transformation of (17c): Similarly, based on ER and FOTE, the non-convex constraint (17c) can be approximated by the following convex functions

$$2\psi_1^{(n)}\psi_1 - \left(\psi_1^{(n)}\right)^2 \geq D + \sigma^2\left(r_2 - 1\right), \tag{20a}$$

$$\begin{bmatrix} \frac{\mathrm{Tr}(\mathbf{W}_{12})}{\sigma^2} & \psi_1 \\ \psi_1 & \mathrm{Tr}\left(\mathbf{W}_2^1\right) \end{bmatrix} \succeq \mathbf{0}, \tag{20b}$$

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.2019.2908821, IEEE Internet of Things Journal

where $D = \mathrm{Tr}\left(r_2\mathbf{W}_2^1 - \mathbf{W}_2^1 - \mathbf{W}_2^2 - \mathbf{W}_{12}\right)$.

Transformation of (17d): The non-convex constraint (17d) is equivalently formulated as

$$(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^2 - \gamma\mathbf{W}_1^1\right) \geq \gamma\sigma^2. \tag{21}$$

As (21) is still a non-convex constraint, ER and FOTE are employed to yield the following approximate convex constraint

$$2\phi_1^{(n)}\phi_1 - (\phi_1^{(n)})^2 \geq \gamma\sigma^2, \tag{22a}$$

$$\begin{bmatrix} (1-\beta) & \phi_1 \\ \phi_1 & \mathrm{Tr}\left(\mathbf{W}_1^2 - \gamma\mathbf{W}_1^1\right) \end{bmatrix} \succeq \mathbf{0}. \tag{22b}$$

Transformation of (17e): Similarly, the non-convex constraint (17e) is converted to the following convex form

$$2\omega_1^{(n)}\omega_1 - (\omega_1^{(n)})^2 \geq \mathrm{Tr}\left(\gamma\mathbf{W}_2^1 - \mathbf{W}_{12} - \mathbf{W}_2^2\right) + \sigma^2\gamma, \tag{23a}$$

$$\begin{bmatrix} \frac{\mathrm{Tr}(\mathbf{W}_{12})}{\sigma^2} & \omega_1 \\ \omega_1 & \mathrm{Tr}\left(\mathbf{W}_2^1\right) \end{bmatrix} \succeq \mathbf{0}. \tag{23b}$$

Transformation of (17f): In the same manner, the non-convex constraint (17f) can be approximated by

$$2\varphi_1^{(n)}\varphi_1 - (\varphi_1^{(n)})^2 \geq \mathrm{Tr}\left(\mathbf{W}\right) + \mathrm{Tr}\left(\mathbf{\Sigma}\right), \tag{24a}$$

$$\begin{bmatrix} \beta & \varphi_1 \\ \varphi_1 & \mathrm{Tr}\left(\sum_{i=1}^{2}\mathbf{W}_1^i\right) \end{bmatrix} \succeq \mathbf{0}. \tag{24b}$$

Thus, the optimization problem (17) has been recast as

$$\max_{\substack{\mathbf{V}_i,\mathbf{W},\beta,\theta_1,\\ \psi_1,\phi_1,\omega_1,\varphi_1}} \quad \mathrm{Tr}\left(\mathbf{\Sigma}\right) \tag{25a}$$

$$\text{s.t.} \quad (17g),(18b),(19), \tag{25b}$$

$$(20),(22)-(24), \tag{25c}$$

$$\mathbf{V}_i \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0},\, i \in \{1,2\}, \tag{25d}$$

which is a semidefinite programming and its solution $(\mathbf{V}_1^*, \mathbf{V}_2^*, \mathbf{W}^*, \mathbf{\Sigma}^*)$ can be obtained by off-the-shelf optimization solvers, e.g., SeDuMi or Yalmip [36].

The convex problem (25) is solved in an iterative manner starting with the initial values of $\left(\theta_1^{(0)}, \psi_1^{(0)}, \phi_1^{(0)}, \omega_1^{(0)}, \varphi_1^{(0)}\right)$, as presented in Algorithm 1. During each iteration, $\left(\theta_1^{(n)}, \psi_1^{(n)}, \phi_1^{(n)}, \omega_1^{(n)}, \varphi_1^{(n)}\right)$ is updated based on the previously obtained solution until the SSR gap between two successive iterations is less than a predefined accuracy ϵ_1. Moreover, based on Lemma 3.1 of [37], the solution $(\mathbf{V}_1^*, \mathbf{V}_2^*, \mathbf{W}^*)$ yielded by SDR is rank-one. Then the beamforming vectors $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{w}$ are obtained by eigenvalue decomposition of $\mathbf{V}_1, \mathbf{V}_2$ and $\mathbf{W}$, respectively.

Finally, the information rate leaked to Eves can be shown in (26) (in the top of the next page). Substituting (26) into (15) and replacing $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{w})$ with $(\mathbf{v}_1^*, \mathbf{v}_2^*, \mathbf{w}^*)$, the SSR of the IoT system under consideration can be computed.

Algorithm 1 Proposed ASBD Scheme

1: **Input:** Set $n = 0$, $\theta_1^{(0)} = 1$, $\psi_1^{(0)} = 1$, $\phi_1^{(0)} = 1$, $\omega_1^{(0)} = 1$,$\varphi_1^{(0)} = 1$, $\delta = 1$, and $\epsilon_1 = 10^{-4}$.
2: **while** $\delta \geq \epsilon_1$ **do**
a) Solve (25) and update $\left(\theta_1^{(n)}, \psi_1^{(n)}, \phi_1^{(n)}, \omega_1^{(n)}, \varphi_1^{(n)}\right) \leftarrow (\theta_1^*, \psi_1^*, \phi_1^*, \omega_1^*, \varphi_1^*)$,
b) Update $\beta^{(n)}, \mathbf{V}_i^{(n)}, \mathbf{W}^{(n)}$ and $\mathbf{\Sigma}^{(n)}$.
c) Update $\delta = \left|\mathrm{Tr}\left(\mathbf{\Sigma}^{(n)}\right) - \mathrm{Tr}\left(\mathbf{\Sigma}^{(n-1)}\right)\right|$.
d) Set $n \leftarrow n+1$.
3: **end while**
4: **Output:** $\beta^*, \mathbf{V}_i^*, \mathbf{W}^*$ and $\mathbf{\Sigma}^*$.

IV. Secure Beamforming Design for the Active Eavesdroppers Case

When active Eves are present, their CSI can be estimated by S and D_1 through leakage from the Eves' receiver radio frequency (RF) frontend [16]. Thus, the AN-aided transmission beamforming design proposed in Section III may not be the best solution because of the presence of active Eves. In light of this, an orthogonal-projection-based transmission beamforming design is proposed for the SSR maximization problem defined in (16). For this scheme it is noted that the number of antennas at D_1 should be more than that of the Eves (i.e., $N_1 > N_e$). For the case when S and D_i have single antennas, a simple power control scheme which optimizes the SSR is also proposed.

A. Multi-Antennas Configuration

The main idea behind the new approach can be explained as follows. Firstly, by using the available CSI of the Eves, a new design for the transmit beamforming $\mathbf{w}$ is proposed, which will deteriorate the quality of the signals received by the Eves due to the addition of AN. This design will be termed as Orthogonal-Projection-Based Secure Beamforming Design (OSBD) for Multi-Antennas Case. On that basis, by letting AN $\mathbf{z} = \mathbf{0}$, the transmitted signal from D_1 during the second phase becomes

$$\mathbf{x} = \mathbf{w}s_2. \tag{27}$$

The observations at D_2 and Eves can be expressed as

$$\mathbf{y}_2^{[B]} = \mathbf{H}_{12}\mathbf{w}s_2 + \mathbf{n}_2^{(2)}, \tag{28a}$$

$$\mathbf{y}_e^{[B]} = \mathbf{G}_{1e}\mathbf{w}s_2 + \mathbf{n}_e^{(2)}, \tag{28b}$$

respectively, where $\mathbf{w}$ lies in the null space of Eves' channel $\mathbf{G}_{1e}$, i.e., $\mathbf{G}_{1e}\mathbf{w} = \mathbf{0}$. Therefore, $\mathbf{w}\mathbf{w}^H = \alpha\left(\frac{\mathbf{I}_{N_1} - \mathbf{Q}_{1e}}{\|\mathbf{I}_{N_1} - \mathbf{Q}_{1e}\|}\right)$ and $\mathbf{Q}_{1e} = \mathbf{G}_{1e}^H(\mathbf{G}_{1e}^H\mathbf{G}_{1e})^{-1}\mathbf{G}_{1e}$, where $\alpha \in [0,1]$ is a scale factor determining the power invested on transmit beamforming. The received SINRs at D_2 and Eves are given by

$$\mathrm{SINR}_{2,s_2} = \frac{\|\mathbf{H}_{s2}\mathbf{v}_2\|^2}{\|\mathbf{H}_{s2}\mathbf{v}_1\|^2 + \sigma^2} + \frac{\|\mathbf{H}_{12}\mathbf{w}\|^2}{\sigma^2}, \tag{29a}$$

$$\mathrm{SINR}_e = \frac{\mathrm{Tr}\left(\mathbf{G}_{\mathrm{se}}\left(\sum_{\mathrm{i}=1}^{2}\mathbf{v}_i\mathbf{v}_i^{\mathrm{H}}\right)\mathbf{G}_{\mathrm{se}}^{\mathrm{H}}\right)}{\mathrm{Tr}\left(\mathbf{\Theta}\right)}, \tag{29b}$$

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.2019.2908821, IEEE Internet of Things Journal

$$R_e = \frac{1}{2}\log\left(1+\frac{\mathrm{Tr}\left(\mathbf{G}_{\mathrm{se}}\left(\sum_{\mathrm{i}=1}^{2}\mathbf{v}_i^{*}\mathbf{v}_i^{*\mathrm{H}}\right)\mathbf{G}_{\mathrm{se}}^{\mathrm{H}}+\mathbf{G}_{1\mathrm{e}}\mathbf{w}^{*}\mathbf{w}^{*\mathrm{H}}\mathbf{G}_{1\mathrm{e}}^{\mathrm{H}}\right)}{\mathrm{Tr}\left(\mathrm{diag}\left(\sigma^2\mathbf{I}_{N_e},\,\sigma^2\mathbf{I}_{N_e}+\mathbf{G}_{1e}\mathbf{\Sigma}^{*}\mathbf{G}_{1e}^{H}\right)\right)}\right). \tag{26}$$

respectively, where $\mathbf{\Theta}=\mathrm{diag}\left(\sigma^2\mathbf{I}_{N_e},\,\sigma^2\mathbf{I}_{N_e}\right)$.

To solve the optimization problem (16), we first let $\mathbf{V}_i=\mathbf{v}_i\mathbf{v}_i^H, i\in\{1,2\}$, $\mathbf{W}=\mathbf{w}\mathbf{w}^H$, and drop rank-one constraints $\mathrm{rank}\left(\mathbf{V}_i\right)=1$, $\mathrm{rank}\left(\mathbf{W}\right)=1$. Then, (16) can be reformulated as (30) (on the top of next page), where $\mathbf{W}_e^i=\mathbf{G}_{se}\mathbf{V}_i\mathbf{G}_{se}^H$, and the non-constraints (17d) and (17e) have been converted to convex forms as previously explained in Section III. It is noted that (30) is non-convex due to the non-convex objective function (30a) and the constraint (30b). However, by using FOTE and ER, (30b) can be approximated by the following convex constraint

$$2\varphi_2^{(n)}\varphi_2-(\varphi_2^{(n)})^2\geq\mathrm{Tr}\left(\mathbf{W}\right), \tag{31a}$$

$$\left[\begin{array}{cc}\beta & \varphi_2\\ \varphi_2 & \mathrm{Tr}\left(\sum_{i=1}^{2}\mathbf{W}_1^i\right)\end{array}\right]\succeq\mathbf{0}. \tag{31b}$$

Since problem (30) is still non-convex its objective function will be transformed into the convex form based on the SCA method. For this, by introducing the slack variables τ, $\mu_i\geq 0, i\in\{1,2\}$, the objective function can be alternatively reformulated as

$$\max_{\tau,\mu_i\geq 0,\beta}\quad\sum_{i=1}^{2}\mu_i-\tau \tag{32a}$$

$$\text{s.t.}\quad\log\left(1+\frac{(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^1\right)}{\mathrm{Tr}\left(\mathbf{\Theta}\right)}\right)\geq\mu_1, \tag{32b}$$

$$\log\left(1+\frac{\mathrm{Tr}\left(\mathbf{W}_2^2\right)}{\sigma^2+\mathrm{Tr}\left(\mathbf{W}_2^1\right)}+\frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right)\geq\mu_2, \tag{32c}$$

$$\log\left(\frac{\mathrm{Tr}\left(\mathbf{\Theta}\right)}{\mathrm{Tr}\left(\mathbf{\Theta}+\sum_{i=1}^{2}\mathbf{W}_e^i\right)}\right)\leq\tau, \tag{32d}$$

where factor $\frac{1}{2}$ in (30) is omitted since it does not affect the monotonicity of (30). Then, the SCA can be implemented over (32). It can be seen that (32b) is equivalent to

$$(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^1\right)\geq\left(e^{\mu_1}-1\right)\mathrm{Tr}\left(\mathbf{\Theta}\right), \tag{33}$$

by the FOTE, (33) is transformed into

$$(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^1\right)\geq(x-1)\,\mathrm{Tr}\left(\mathbf{\Theta}\right), \tag{34}$$

where $x=e^{\mu_1^{(n)}}(\mu_1-\mu_1^{(n)}+1)$ is the FOTE of e^{μ_1} around the point $\mu_1^{(n)}$. According to the ER method, (34) is transformed into the following convex form

$$2\xi^{(n)}\xi-(\xi^{(n)})^2\geq(x-1)\,\mathrm{Tr}\left(\mathbf{\Theta}\right), \tag{35a}$$

$$\left[\begin{array}{cc}1-\beta & \xi\\ \xi & \mathrm{Tr}\left(\mathbf{W}_1^1\right)\end{array}\right]\succeq\mathbf{0}. \tag{35b}$$

(32c) is non-convex and it is not suitable to handle the non-convex problem by adopting the ER method. Therefore, Proposition 1 is introduced to convert (32c) into a convex form.

Proposition 1. *For any non-negative variables x, y, z, a non-convex expression $xy\leq z$ can be approximated by the following convex constraint*

$$(\eta x)^{\,2}+(y/\eta)^{\,2}\leq 2z. \tag{36}$$

Proof: According to the arithmetic-geometric mean (AGM) inequality, the approximation of the expression $xy\leq z$ can be expressed as

$$2xy\leq(\eta x)^{\,2}+(y/\eta)^{\,2}\leq 2z, \tag{37}$$

where the former inequality holds with equality, if and only if, $\eta=\sqrt{y/x}$. Then the non-convex expression $xy\leq z$ can be replaced by $\frac{(\eta x)^2+(y/\eta)^2}{2}\leq z$. It can be observed that $(\eta x)^{\,2}+(y/\eta)^{\,2}\leq 2z$ is a convex constraint based on Lemma 1, which completes the proof. ■

Firstly, (32c) can be converted to

$$\left(e^{\mu_2}-\frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right)\mathrm{Tr}\left(\mathbf{W}_2^1\right)\leq\Xi, \tag{38}$$

where $\Xi=\mathrm{Tr}\left(\mathbf{W}_2^2+\mathbf{W}_{12}+\mathbf{W}_2^1\right)-e^{\mu_2}+\sigma^2$. Using the FOTE, (38) is then transformed into

$$\left(y-\frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right)\mathrm{Tr}\left(\mathbf{W}_2^1\right)\leq\Xi_1, \tag{39}$$

where $\Xi_1=\mathrm{Tr}\left(\mathbf{W}_2^2+\mathbf{W}_{12}+\mathbf{W}_2^1\right)-y+\sigma^2$, $y=e^{\mu_2^{(n)}}(\mu_2-\mu_2^{(n)}+1)$. Finally, according to the Proposition 1, (39) can be approximated by the following constraint

$$\left(\eta^{(n)}\left(y-\frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right)\right)^2+\left(\mathrm{Tr}\left(\mathbf{W}_2^1\right)/\eta^{(n)}\right)^2\leq 2\Xi_1, \tag{40}$$

where $\eta^{(n)}$ can be updated by

$$\eta^{(n)}=\sqrt{\left(\mathrm{Tr}\left(\mathbf{W}_2^1\right)\right)^{(n-1)}/\left(y-\frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right)^{(n-1)}}. \tag{41}$$

It is clear from Lemma 1 that now (40) is a convex constraint.

Employing FOTE and ER, we transform constraint (32d) as follows

$$2\phi_2^{(n)}\phi_2-(\phi_2^{(n)})^2\geq\mathrm{Tr}\left(\mathbf{\Theta}\right)(1-z), \tag{42a}$$

$$\left[\begin{array}{cc}z & \phi_2\\ \phi_2 & \mathrm{Tr}(\sum_{i=1}^{2}\mathbf{W}_e^i)\end{array}\right]\succeq\mathbf{0}, \tag{42b}$$

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.2019.2908821, IEEE Internet of Things Journal

$$\max_{\mathbf{V}_1\succeq\mathbf{0},\mathbf{V}_2\succeq\mathbf{0},\mathbf{W}\succeq\mathbf{0}} \frac{1}{2}\log\left(\left(1+\frac{(1-\beta)\,\mathrm{Tr}\left(\mathbf{W}_1^1\right)}{\mathrm{Tr}\left(\mathbf{\Theta}\right)}\right)\left(1+\frac{\mathrm{Tr}\left(\mathbf{W}_2^2\right)}{\sigma^2+\mathrm{Tr}\left(\mathbf{W}_2^1\right)}+\frac{\mathrm{Tr}\left(\mathbf{W}_{12}\right)}{\sigma^2}\right)\left(\frac{\mathrm{Tr}\left(\mathbf{\Theta}\right)}{\mathrm{Tr}\left(\mathbf{\Theta}+\sum_{i=1}^{2}\mathbf{W}_e^i\right)}\right)\right) \tag{30a}$$

$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{W})\le P_t, \tag{30b}$$

$$(17d),(17e),\text{ and }(17g), \tag{30c}$$

Algorithm 2 OSBD Scheme with Eves' CSI

1: **Input:** Set $n=0$, $\tau^{(0)}=1$, $\mu_1^{(0)}=1$, $\mu_2^{(0)}=0$, $\varphi_2^{(0)}=1$, $\phi_2^{(0)}=1$, $\xi^{(0)}=1$, $\epsilon=10^{-4}$, and $R_0=\mu_1^{(0)}+\mu_2^{(0)}-\tau^{(0)}$.
2: **Repeat**
a) Solve (43) and obtain $\varphi_2^*,\phi_2^*,\xi^*$ as well as the SSR, i.e., $R=\mu_1^*+\mu_2^*-\tau^*$.
b) Update $\eta^{(n)}$ based on (41).
c) Update $(\tau^{(n)},\mu_1^{(n)},\mu_2^{(n)},\varphi_2^{(n)},\phi_2^{(n)},\xi^{(n)})\leftarrow(\tau^*,\mu_1^*,\mu_2^*,\varphi_2^*,\phi_2^*,\xi^*)$, $R_0\leftarrow R$.
d) Set $n\leftarrow n+1$.
3: **Until** $|R-R_0|^2\le\epsilon$.
4: **Output:** $\beta^*,\mathbf{V}_1^*,\mathbf{V}_2^*$ and $\mathbf{W}$.

where $z=e^{\tau^{(n)}}(\tau-\tau^{(n)}+1)$. At this point, constraint (32d) is replaced by two convex constraints, i.e., the convex constraint (42a) and the linear matrix inequality constraint (42b).

So far, the optimization problem (30) has been reformulated as

$$\max_{\varphi_2,\ \tau,\mu_i,\ \beta,\xi,\phi_2} \quad \sum_{i=1}^{2}\mu_i-\tau \tag{43a}$$

$$\text{s.t.} \quad (17g),(22),(23),(31), \tag{43b}$$

$$(35),(40),\text{ and }(42), \tag{43c}$$

$$\mathbf{V}_i\succeq\mathbf{0},\mu_i\ge0,i\in\{1,2\}. \tag{43d}$$

Consequently, for the active Eves case, the original optimization problem (16) has been transformed into the convex form. Then the solution $(\mathbf{V}_1^*,\mathbf{V}_2^*,\mathbf{W}^*)$ of (16) is obtained by off-the-shelf optimization solver, e.g., SeDuMi and Yalmip. The algorithmic implementation of the proposed OSBD scheme is summarized in Algorithm 2. Note that problem (43) is handled iteratively with the initial value of $(\tau^{(0)},\mu_1^{(0)},\mu_2^{(0)},\varphi_2^{(0)},\phi_2^{(0)},\xi^{(0)})$. For each iteration, $(\tau^{(n)},\mu_1^{(n)},\mu_2^{(n)},\varphi_2^{(n)},\phi_2^{(n)},\xi^{(n)})$ is updated with the solution obtained in the previous iteration until the rate gap between two successive iterations below the predefined accuracy. Moreover, the optimal solution $(\mathbf{V}_1^*,\mathbf{V}_2^*,\mathbf{W}^*)$ yielded by SDR is rank-one, which is described in the following proposition.

Proposition 2. *If problem (43) is feasible, the beamforming vectors* $\mathbf{v}_1$, $\mathbf{v}_2$ *and* $\mathbf{w}$ *can be exactly obtained by eigenvalue decomposition of* $\mathbf{V}_1^*,\mathbf{V}_2^*$ *and* $\mathbf{W}^*$*, since* $\mathbf{V}_1^*,\mathbf{V}_2^*$ *and* $\mathbf{W}^*$ *are rank-one.*

Proof: The transmit beamforming vectors are jointly optimized through the OSBD scheme. According to the rank reduction procedure of the semidefinite programming given in Lemma 3.1 of [37], $\mathbf{V}_1^*$, $\mathbf{V}_2^*$ and $\mathbf{W}^*$ satisfy the following inequality

$$\mathrm{rank}^2(\mathbf{V}_1^*)+\mathrm{rank}^2(\mathbf{V}_2^*)+\mathrm{rank}^2(\mathbf{W}^*)\le3. \tag{44}$$

Since from (17d) and (32b) it is observed that problem (43) is not feasible if $\mathbf{V}_1^*=\mathbf{0}$ or $\mathbf{V}_2^*=\mathbf{0}$, then, $\mathrm{rank}(\mathbf{V}_1^*)=\mathrm{rank}(\mathbf{V}_2^*)=1$, and also $\mathrm{rank}(\mathbf{W}^*)\le1$. Since $\alpha>0$, $\mathrm{rank}(\mathbf{W}^*)\ne0$, then clearly there exits a $\mathbf{W}^*$ which satisfies $\mathrm{rank}(\mathbf{W}^*)=1$ and concludes the proof. ■

B. Single-Antenna Configuration

In applications where devices are equipped with a single antenna, the secure beamforming design problem analyzed in the previous subsection, simplifies to a power allocation problem. As there will be no diversity gain and in order to maximize the SSR and at the same time avoiding the AN interference to D_2, all the energy harvested by D_1 is used for information transmission. In other words, since the transmitted signal from D_1 during the second phase is represented as $x=\sqrt{P_t}s_2$, the EH constraint from (16) can be removed. Then, under the constraints of the transmit power at S and the QoS requirement at D_i, the SSR is optimized. By conveniently introducing power allocation factors ρ_1 and ρ_2 as replacement of the beamforming vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, respectively, the optimization problem is reformulated as

$$\max_{\beta,\rho_1,\rho_2} \log\left(1+P_s\left(1-\beta\right)h_1\right)-\log\left(1+\frac{\left\|\mathbf{g}_{se}\right\|^2P_s+P_s\beta h_1\left\|\mathbf{g}_{1e}\right\|^2}{2\sigma^2}\right) \tag{45a}$$

$$\text{s.t.} \quad P_s\left(1-\beta\right)h_1\rho_1\ge\gamma_1, \tag{45b}$$

$$\frac{PH_s\left(1-\beta\right)h_1\rho_2}{1+P_s\left(1-\beta\right)h_1\rho_1}\ge\gamma_2, \tag{45c}$$

$$\frac{P_sh_2\rho_2}{1+P_sh_2\rho_1}+P_s\beta h_{12}h_1\ge\gamma_2, \tag{45d}$$

$$\rho_1+\rho_2=1,\rho_1,\rho_2\in[0,1], \tag{45e}$$

where h_1,h_2 and h_{12} are normalized main channel gains; $\mathbf{g}_{se}$ and $\mathbf{g}_{1e}$ are wiretap channels; γ_i, is target SINR of D_i; (45b) and (45d) are QoS constraints of D_i; And (45c) ensuring that D_1 can satisfactorily perform SIC. As this optimization problem (45) is a bilevel programming problem, with the outer level variable being β, it will be transformed into the convex one.

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.2019.2908821, IEEE Internet of Things Journal

Following [6], it can be shown that at least one inequality constraint in (45) is satisfied with equality at the optimal solution when problem (45) is feasible. Otherwise, the optimization variables can be changed to increase the SSR until one of the constraints holds with equality.

For convenience of the analysis' presentation, let us consider that the inequality constraint (45b) holds with equality at the optimal solution so that

$$\rho_1 = \frac{\gamma_1}{P_s\left(1-\beta\right)h_1}, \rho_2 = \frac{P_s\left(1-\beta\right)h_1-\gamma_1}{P_s\left(1-\beta\right)h_1}. \tag{46}$$

It is noted that the variables ρ_1 and ρ_2 are expressed as a function of β. Substituting (46) into (45c) and (45d), constraints (45c) and (45d) are rewritten as

$$P_s\left(1-\beta\right)h_1 \geq \gamma_1+\gamma_2+\gamma_1\gamma_2, \tag{47a}$$
$$P_s h_1^2 h_{12}\beta^2 \leq \xi+\zeta, \tag{47b}$$

respectively, where $\xi = P_s h_1 h_2 - \gamma_2 h_1 - \gamma_1\gamma_2 h_2, \zeta = \beta\left(\gamma_2 h_1 - P_s h_1 h_2 + P_s h_1 h_2 h_{12}\gamma_1 + P_s h_1^2 h_{12}\right)$. Since the optimization, problem (45) due to is still non-convex, a slack variable u is introduced to non-convex objective approximate the second term in (45a) by FOTE. In this way, the non-convex optimization problem (45) can be reformulated as

$$\max_{\beta,\upsilon} \ \log\left(1+P_s\left(1-\beta\right)h_1\right)-\upsilon \tag{48a}$$
$$\text{s.t. } 1+\frac{\left\|\mathbf{g}_{se}\right\|^2 P_s + P_s\beta h_1\left\|\mathbf{g}_{1e}\right\|^2}{2\sigma^2} \leq z, \tag{48b}$$
$$(47a)\text{ and }(47b), \tag{48c}$$

where $z = e^{\upsilon^{(n)}}\left(\upsilon-\upsilon^{(n)}+1\right)$. Since the optimization problem stated in (48) is now in convex form, its optimal solution can be readily obtained by the handy solver, e.g., SeDuMi or Yalmip. Note that if (45c) or (45d) hold with equality, a similar methodology can be followed to obtain an equivalent convex optimization problem. However, due to space limitations, the detailed procedure will not be presented here.

V. Performance Evaluation Results and Discussion

In this section, the SSR performance of the previously described cooperative relay-aided secure IoT communication systems will be presented. The various performance evaluation results have been obtained by extensive computer simulation experiments. It is assumed that the two legitimate users and N_e eavesdroppers are deployed within a 8-meter×8-meter network, while S is located at the edge with coordinate $(0,4)$. $h_{Li} = 10^{-3}d_i^{-\alpha_i}, (i=1,2)$ and $h_{Le} = 10^{-3}d_e^{-\alpha_e}$ represent the large-scale path losses, where $d_i, (i=1,2)$ and d_e are the distances from S to D_i and Eves, respectively, $\alpha_1 = 2, \alpha_2 = 4$ and $\alpha_e = 2$ are the corresponding path loss exponents. The downlink channels $\mathbf{H}_{s1}, \mathbf{H}_{12}, \mathbf{G}_{se}$ and $\mathbf{G}_{1e}$ operate in the presence of Rician fading, as follows

$$\mathbf{H} = \sqrt{\frac{\Gamma}{1+\Gamma}}\mathbf{H}^{LoS} + \sqrt{\frac{1}{1+\Gamma}}\mathbf{H}^{NLoS}, \tag{49}$$

where $\mathbf{H}^{LoS}$ is the LOS deterministic component, $\mathbf{H}^{NLoS}$ is modeled as the small-scale Rayleigh fading following $\mathcal{CN}(0,1)$, and unless otherwise stated, with Rician factor $\Gamma = 4$. The distribution of $\mathbf{H}_{s2}$ follows $\mathcal{CN}(0,1)$. Matlab is used as a simulation tool, and Yalmip is employed as an optimization solver. All the SSR curves are generated by averaging 500 independent channel realizations.

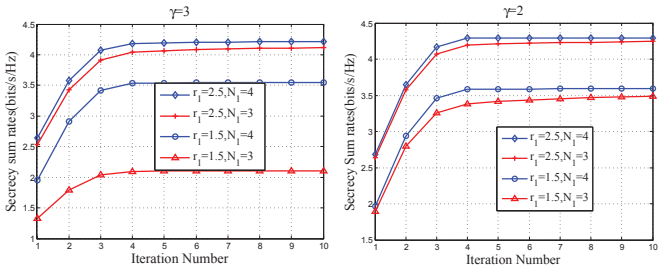

Fig. 2. SSR versus the number of iteration for different N_1s and r_1s.

A. Performance Evaluation of Proposed AN-aided Scheme Without Eves' CSI

Fig. 2 presents the SSR versus the number of iterations for different N_1 and r_1, where the SINR threshold $\gamma = 2, 3$ in Fig. 2(a) and Fig. 2(b), respectively. We set the number of eavesdroppers, $N_e = 3$, the transmit power constraint at S,$P_s = 30$ dBm. These performance evaluation results clearly show that the proposed ASBD scheme converges to a stationary point in few iterations. Furthermore, the SSR performance improves as γ (i.e., the QoS requirement of D_2) decreases. This happens because the harvested power at D_1 is larger if γ become smaller, and then more power can be used to transmit AN.

Fig. 3 presents the SSR performance of the ASBD scheme versus the transmit power at S for different values of N_1 by fixing $N_s = N_2 = 4$, $N_e = 3$ and $\gamma = 3$. For comparison purposes, the performance of the secure beamforming design scheme without AN-aided (denoted as "Without AN") has been also obtained. These results clearly show that the SSR obtained by ASBD scheme is larger compared with the benchmarks. Furthermore, it is observed that, with the increase of N_1, the SSR achieved by different schemes is improved significantly.

Fig. 4 shows the SSR versus the predefined threshold of achievable ergodic rate of D_1 for different values of N_s, where $P_s = 30$ dBm, $N_1 = N_2 = 4$, $\gamma = 3$. It can be seen that the SSR performance is enhanced as r_1 increases, which is consistent with previous findings presented in [7]. The reason is that the transmitter S allocates more power to the strong user D_1 to satisfy the predefined threshold of achievable ergodic rate of D_1, which leads to the increasing of SSR. Meanwhile, compared with the OMA-based secure beamforming design with AN-aided (denoted as "OMA w/ AN"), the proposed design exhibits better SSR performance when N_s increases.

B. SSR Comparison With Eves' CSI

In Fig. 5, the convergence property of the proposed OSBD algorithm and the algorithm given in [2] for the active Eves

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.2019.2908821, IEEE Internet of Things Journal

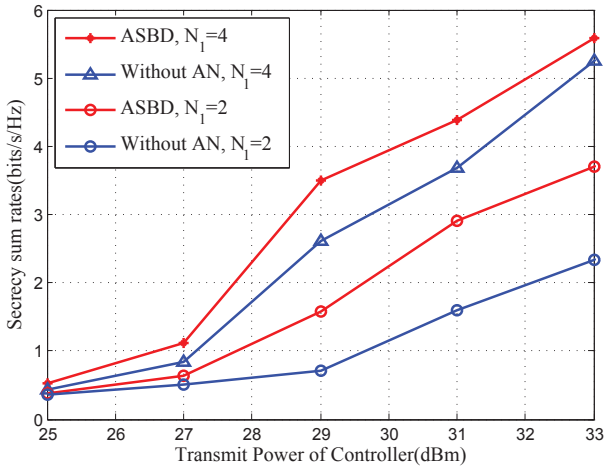

Fig. 3. SSR versus P_s, comparisons of the proposed ASBD scheme and the scheme without AN-aided, for different N_1s.

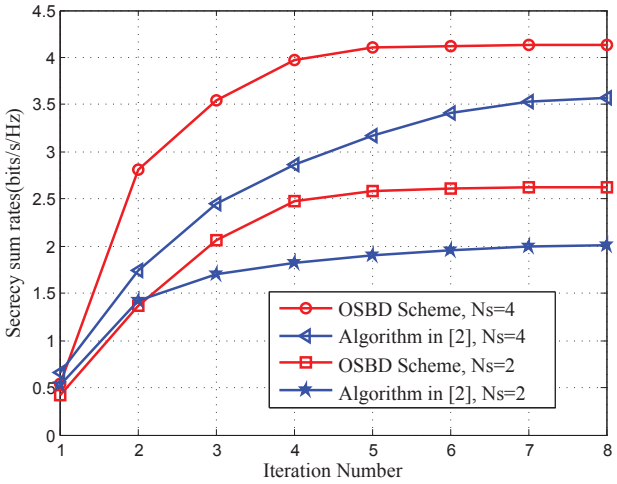

Fig. 5. The SSR performance versus the number of iteration for different N_ss.

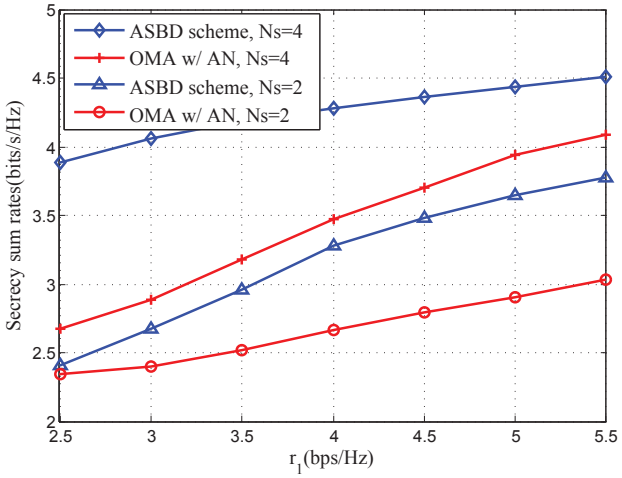

Fig. 4. SSR versus r_1, for different N_s.

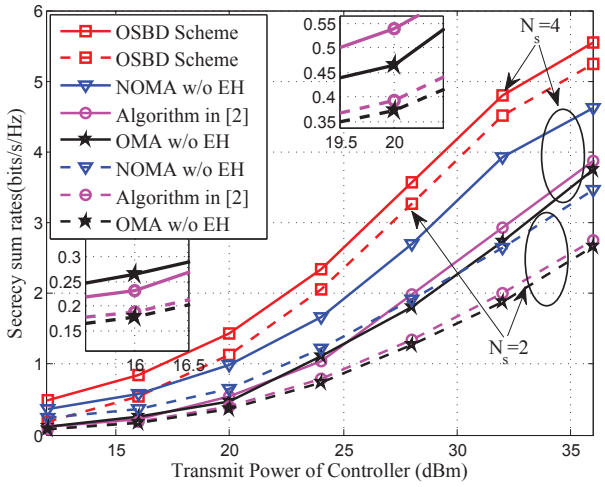

Fig. 6. The SSR performance of different schemes versus P_s.

case is presented, with $P_s = 30$ dBm, $\gamma = 3$, $N_e = 3, N_i = 4, N_s = \{2, 4\}$. It is noted that, although the algorithm of [2] also employs a NOMA transmission protocol and optimizes the SSR of downlink systems, it only considers the direct transmission link and does not use any physical layer security technology. From Fig. 5, consensus has been reached that the proposed algorithm converges to a stationary point in a fewer steps than that in [2], especially for higher values of N_s. To demonstrate the computational efficiency of the proposed approach, we give the time needed for the two algorithms to converge. Our proposed algorithm takes about 4.75 s for each independent channel realizations, while the time required for the algorithm given in [2] is about 7.11 s.

Fig. 6 illustrates the SSR performance of the proposed OSBD scheme for the active Eves case. Set $N_e = 3, N_i = 4, N_s = \{2, 4\}, \gamma = 3$. We also consider the secure transmission design given in [2], the NOMA secure transmission protocol without relay-aided (denoted as "NOMA w/o EH") as well as the conventional OMA-based secure beamforming design without relay-aided (denoted as "OMA w/o EH") as baseline algorithms. As expected, the proposed OSBD scheme based on the cooperative secure transmission protocol can obtain higher secrecy rate than that in [2]. In addition, numerical results also indicate that the proposed scheme can achieve much better SSR performance than the other two benchmark schemes (i.e., NOMA w/o EH scheme and OMA w/o EH scheme). With the fixed P_s, we can observe that, as N_s grows, the SSR performance becomes better in different schemes, since more array gains are provided.

Fig. 7 illustrates the SSR performance under different transmit powers of controller for the single-antenna configuration. Similar to Fig. 6, the three benchmarks are employed as baseline algorithms, where $N_1 = N_2 = N_s = 1, N_e = 3, \gamma_1 = 2, \gamma_2 = 3$. Obviously, the SSR performance of the proposed power control scheme outperforms that of the other three benchmarks, especially in large transmit power region. The reason is that the received signal at D_2 is consisted of two parts from the relay-assisted system so that the SSR of the IoT is further enhanced.

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.2019.2908821, IEEE Internet of Things Journal

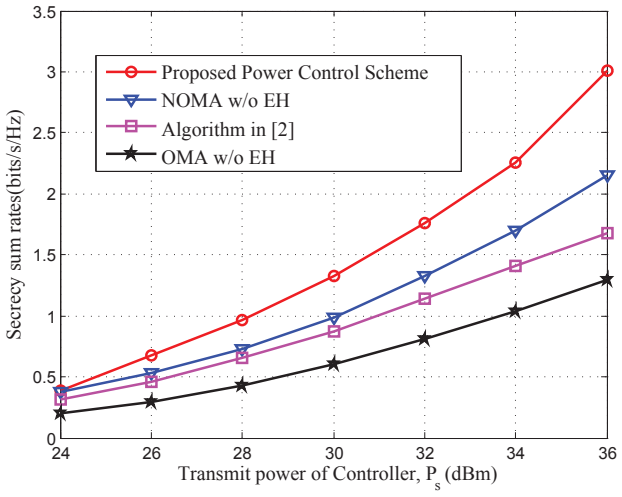

Fig. 7. The SSR performance of different schemes versus P_s with single-antenna configurations.

VI. Conclusions

In this paper, we investigated the secure transmit beamforming design in the downlink IoT system. Taking diversified QoS requirements of IoT users into account, a novel relay-aided cooperative secure transmission strategy was proposed to further improve the SSR of the IoT system. Two Eves cases have been considered based on the availability of the CSIs of Eves. For the passive Eves case, ASBD scheme was proposed to jointly optimize the secure beamforming vectors, AN covariance matrix as well as PS ratio. For the active multi-antennas Eves case, OSBD scheme was proposed to maximize the SSR of the considered IoT system. When the transmitters (i.e., S and D_1) are single-antenna configurations, the orthogonal-projection-based optimization problem is degraded into a power allocation problem and the optimal solution can be found by fully exploiting the specific property of the optimization problem. Various performance evaluation results have demonstrated the superiority of the proposed schemes compared to the existing benchmarks.

The proposed cooperative SWIPT secure transmission protocol can be applied to massively connected IoT systems in the future, such as Healthcare IoT, in which a large quantity of smart devices are involved in sensing health parameters and these devices are confined by the limited power. For Healthcare IoT applications, it is noted that security is a vital yet challenging requirement during data collection from patients to a centralized data collection center. Thus, as the proposed secure transmission scheme is capable of ensuring the security of Healthcare IoT, it could be very well used for such kind of applications.

References

[1] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[2] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, "Secrecy sum rate optimization for downlink MIMO nonorthogonal multiple access systems," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1113–1117, Aug. 2017.

[3] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," *IEEE Trans. Signal Process.*, vol. 64, no. 1, pp. 76–88, Jan. 2016.

[4] Q. Sun, S. Han, C. L. I, and Z. Pan, "On the ergodic capacity of MIMO NOMA systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 405–408, Aug. 2015.

[5] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C. L. I, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[6] Y. Xu, C. Shen, Z. Ding, X. Sun, S. Yan, G. Zhu, and Z. Zhong, "Joint beamforming and power-splitting control in downlink cooperative SWIPT NOMA systems," *IEEE Trans. Signal Process.*, vol. 65, no. 18, pp. 4874–4886, Sept. 2017.

[7] M. Zeng, A. Yadav, O. A. Dobre, G. I. Tsiropoulos, and H. V. Poor, "Capacity comparison between MIMO-NOMA and MIMO-OMA with multiple users in a cluster," *IEEE J. Sel. Areas in Commun.*, vol. 35, no. 10, pp. 2413–2424, Oct. 2017.

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

[9] 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.

[10] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept. 2013.

[11] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 524–527, Mar. 2017.

[12] A. Behnad, M. B. Shahbaz, T. J. Willink, and X. Wang, "Statistical analysis and minimization of security vulnerability region in amplify-and-forward cooperative systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2534–2547, Apr. 2017.

[13] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans Veh. Technol.*, vol. 66, no. 5, pp. 4457–4462, May 2017.

[14] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281–1293, July 2016.

[15] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[16] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 2809–2812.

[17] Q. Li and W. K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-Eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[18] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun 2013.

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

[20] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[21] Y. Hao, T. Lv, and H. Gao, "AN-aided robust secure beamforming design in MIMO two-way relay systems with PNC," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, Spain, Apr. 2018, pp. 1–6.

[22] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[23] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9006–9019, Nov. 2016.

[24] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[25] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. L. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative

jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[26] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proc. IEEE Int. Conf. Commun.*, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.

[27] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9006–9019, Nov. 2016.

[28] Z. Ding, P. Fan, and H. V. Poor, "User pairing in non-orthogonal multiple access downlink transmissions," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–5.

[29] T. Lv, Y. Ma, J. Zeng, and P. T. Mathiopoulos, "Millimeter-wave NOMA transmission in cellular M2M communications for internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1989–2000, June 2018.

[30] Q. Shi, C. Peng, W. Xu, M. Hong, and Y. Cai, "Energy efficiency optimization for MISO SWIPT systems with zero-forcing beamforming," *IEEE Trans. Signal Process.*, vol. 64, no. 4, pp. 842–854, Feb. 2016.

[31] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[32] H. M. Wang, Q. Yin, and X. G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[33] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[34] W. C. Li, T. H. Chang, C. Lin, and C. Y. Chi, "Coordinated beamforming for multiuser miso interference channel under rate outage constraints," *IEEE Trans. Signal Process.*, vol. 61, no. 5, pp. 1087–1103, Mar. 2013.

[35] S. Boyd and L. Vandenberghe, "Convex optimization," *Cambridge, U.K.: Cambridge Univ. Press*, 2009.

[36] J. Lofberg, "Yalmip: a toolbox for modeling and optimization in MATLAB," in *Proc. IEEE International Conference on Robotics and Automation (IEEE Cat. No.04CH37508)*, Taipei, 2004, pp. 284–289.

[37] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, Feb. 2010.