IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTERNET OF THINGS (IoT) IN 5G WIRELESS COMMUNICATIONS

Received April 29, 2016, accepted May 18, 2016, date of publication June 7, 2016, date of current version June 24, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2575863

Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations

QIAN XU[1,2], PINYI REN[1,2], HOUBING SONG[3], AND QINGHE DU[1,2]

[1]School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[2]Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an Jiaotong University, Xi'an 710049, China
[3]Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136, USA

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

This work was supported in part by the National Natural Science Foundation of China under Grant 61431011, in part by the Research Fund for the Doctoral Program of Higher Education of China under Grant 20120201110066, and in part by the Fundamental Research Funds for the Central Universities.

ABSTRACT The Internet of Things (IoT) depicts a bright future, where any devices having sensorial and computing capabilities can interact with each other. Among all existing technologies, the techniques for the fifth generation (5G) systems are the main driving force for the actualization of IoT concept. However, due to the heterogeneous environment in 5G networks and the broadcast nature of radio propagation, the security assurance against eavesdropping is a vital yet challenging task. In this paper, we focus on the transmission design for secure relay communications in IoT networks, where the communication is exposed to eavesdroppers with unknown number and locations. The randomize-and-forward relay strategy specially designed for secure multi-hop communications is employed in our transmission protocol. First, we consider a single-antenna scenario, where all the devices in the network are equipped with the single antenna. We derive the expression for the secrecy outage probability of the two-hop transmission. Following this, a secrecy-rate-maximization problem subject to a secrecy-outage-probability constraint is formulated. The optimal power allocation and codeword rate design are obtained. Furthermore, we generalize the above analyses to a more generic scenario, where the relay and eavesdroppers are equipped with multiple antennas. Numerical results show that the proper use of relay transmission can enhance the secrecy throughput and extend the secure coverage range.

INDEX TERMS Internet of Things (IoT), physical layer security, relay transmission, resource allocation, stochastic geometry.

I. INTRODUCTION

A. BACKGROUND

The Internet of Things (IoT), which has aroused great interest in the research community, is expected to provide ubiquitous connectivity and information exchange among a variety of physical objects (e.g., sensors, vehicles, mobile phones) in any place and at any time [1], [2]. It enables objects possessing sensorial and computing capabilities to work together efficiently. Meanwhile, it also facilitates the delivering of mobile content based on the concept of social networks [3], [4]. Those physical objects in IoT are more intelligent than before as they can see, hear, think and cooperate with one another [5]. With such smart objects deployed in home, hospital, factory, and farmland, the quality of people's daily lives and the world's economy are both promised to get a big boost. Although the idea of IoT can date back to the last century [6], the corresponding technologies and protocols are still open research issues. Among all existing technologies, the techniques for the forthcoming fifth generation (5G) system will be important enablers for actualizing the IoT concept. The 5G system, which is expected to achieve 1000 times the system capacity and 10 times the data rate and spectral efficiency of the present 4G system, will not be available until after 2020. It is assumed that 5G networks should meet the following six requirements: larger system capacity, higher data rate, lower end-to-end latency, ubiquitous connectivity, reduced energy consumption, and consistent quality of experience [7]. All these characteristics show

the capabilities of 5G technologies to construct a seamless connection of massive things. Hence, with the development of 5G technologies, the IoT will become a significant part of the next-generation wireless communication system in the near future.

Besides the reliability and efficiency of communications, information security is obviously another essential requirement for the IoT, since the application field of the IoT encompasses industry, healthcare, market, and transportation. Any disclosure of these sensitive messages (e.g., patients' data, financial files, chat records) is unacceptable. However, the heterogeneous environment in 5G systems (e.g., device-to-device communication [8] and cognitive ad hoc networks [9]) and the broadcast nature of radio propagation makes the transmission vulnerable to eavesdropping attack. Traditional cryptographic encryption is a widely used approach [10], [11] protecting the message from being recovered by eavesdroppers. The basic idea is to use a secret key to encrypt the secret message so that even if the ciphertext is intercepted, the original message is still secure. Nevertheless, the management and distribution of the secret keys often require complex protocols and architectures, which makes the cryptographic method difficult to be implemented in the IoT [12]–[14] with plenty of resource-constrained devices as well as heterogeneous radio access technologies (RATs) including WiFi, Bluetooth, IEEE 802.15.4, and LTE-Advanced. In addition, the risk of information leakage faced by the encryption method is increasing due to the enhancement of eavesdroppers' computing capabilities. Thus, some highly efficient and easily operational protocols are needed to guarantee the secrecy of the communications in the IoT.

Fortunately, in recent years the concept of physical layer security (PLS) [15], which is agnostic to the system infrastructures and RATs, has shown great potential in providing information-theoretically unbreakable secrecy. In other words, the security is still guaranteed even if the eavesdroppers (e.g., smart devices in 5G systems) have unbounded computational power. The core idea of PLS is utilizing the inherent randomness and difference of wireless channels to keep the confidential message secure from eavesdroppers, regardless of their computing capabilities. Based on the celebrated theoretical analyses of PLS [16], [17], a serial of transmission strategies have been proposed, such as cooperative relay transmission [18], artificial noise [19], secure beamforming [20], and noise aggregation [21]. Among all these strategies, relay transmission is of great significance to the IoT for the following reasons. The transmit power of many IoT objects (e.g., sensors and mobile phones) is low, which limits the coverage range for the reliable communication. Furthermore, the multi-path fading, coupled with undesirable propagation environment resulting from machinery obstacles, engine vibrations, and equipment noise in some industrial environment [22], makes the cooperative relaying much more necessary.

Up to now, a great number of secure relay transmission strategies based on the concept of PLS have been proposed [23]–[27]. The authors in [23] studied the relay and jammer selection problem to minimize the secrecy outage probability and the authors in [24] proposed a joint relay and jammer selection strategy in two-way relay networks to maximize the secrecy throughput. In [25] and [26], the authors improved the performance of secure transmission by employing multiple cooperative relays to form a virtual antenna array. The authors in [27] optimized the power allocation and transmission region for the decode-and-forward (DF) relay network under the secrecy outage constraint. It is worth noting that all these research works assume that the system designer knows the instantaneous channel state information (CSI) or at least the channel distribution information (CDI) of eavesdroppers. This is an impractical assumption since most eavesdroppers are passive attackers, that is, they only listen without transmitting any signals. Moreover, the potential eavesdroppers in IoT may be some curious legitimate devices belonging to different subsystems. Hence, even the exact number and locations of these eavesdroppers are difficult to obtain.

To study the secure transmission problem without eavesdroppers' channel states, stochastic geometry has been introduced as a powerful tool in many works [28]–[31]. These works usually model the distribution of eavesdroppers as homogenous Poisson point process (PPP) and study the secrecy performance for such networks. In [28], the authors investigated the secrecy outage probability for multi-input single-output (MISO) channels in the Nakagami-m fading environment. The authors in [29] studied the secrecy performance of multi-input multi-output (MIMO) channels with and without artificial noise. The authors in [30] derived the secure connection probability for relay transmission while the authors in [31] obtained the secrecy outage probability for multi-hop transmission. Although the above works have studied both the single- and multi-hop transmission with a single antenna or multiple antennas, the system parameters are all preset as constants and not able to be adapted according to some available channel states. To the best of our knowledge, there has been no work considering the power allocation and codeword rate design for a relay network against eavesdroppers with uncertain number and locations.

B. APPROACH AND CONTRIBUTIONS

In this paper, we investigate the secure transmission from a source (e.g., surveillance camera) to a destination (e.g., controller) in the IoT with non-colluding unknown eavesdroppers. We assume that the locations of eavesdroppers are randomly distributed according to homogenous PPP. Besides the source and the destination, a relay (e.g., sensor node) is employed to retransmit the secret message. To avoid the using of maximum ratio combining (MRC) at any eavesdropper, the widely-used randomize-and-forward (RF) strategy [32], [33] is exploited. For the RF protocol, the source and the relay use different codebooks to transmit the same secret message. By optimizing the power allocation between the source and the relay as well as the codeword rate for each

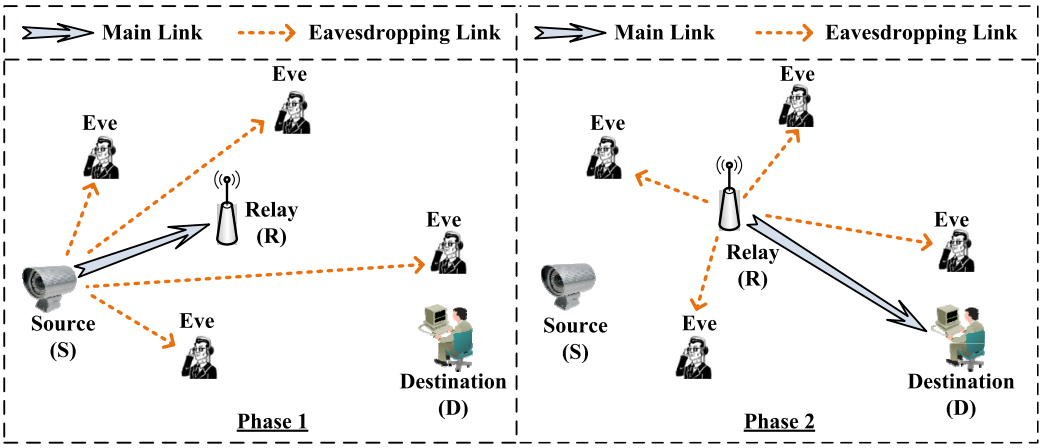

FIGURE 1. System model: the source node *S* is transmitting confidential message to the destination node *D* with the help of a selected relay *R*. Randomly distributed eavesdroppers are trying to intercept the message.

hop of the relay transmission, we maximize the secrecy rate under a secrecy-outage-probability constraint.

First, we concentrate on the single antenna system where all the devices including eavesdroppers are equipped with the single antenna. With the assumption that the locations of eavesdroppers change independently from hop to hop, we derive an expression for the secrecy outage probability of the two-hop transmission, which is shown to be the upper bound of the outage probability when the locations of eavesdroppers remain unchanged. Following this expression, we formulate a secrecy rate maximization problem with the secrecy-outage-probability constraint. The optimal rate design for codebooks and power allocation between the source and relay are derived. By studying the performance of the optimal scheme in some special cases, we obtain several insights concerning the setting of system parameters.

To further study the secrecy performance of relay transmission, we then generalize the above results to a more generic system where the relay and eavesdroppers are equipped with multiple antennas. This model describes one kind of relay transmission in heterogeneous sensor networks [34], [35] composed of two kinds of nodes: Low-end sensor and High-end sensor. The source and the destination are Low-end sensors with single antenna while a High-end sensor with multiple antennas serves as a relay. In practice, artificial noise is not suitable for IoT applications since it requires high consumption of energy as well as causes interference to adjacent nodes [13]. Thus, in this work we only adopt beamforming as our transmit strategy without employing artificial noise. An accurate expression for the secrecy outage probability is derived, based on which a similar secrecy rate maximization problem is formulated. Through the same optimizing method, we obtain the optimal solution which is a generalization of the solution derived for the single-antenna system.

The rest of this paper is organized as follows. Section II presents the system model and derives the formulation for the optimization problem. Section III and Section IV studies the optimization problem in the single- and multi-antenna systems, respectively. Section V presents numerical examples to evaluate the secrecy performance of the relay transmission. Finally, the paper concludes with Section VI.

II. SYSTEM MODEL

A. SYSTEM DESCRIPTION

The system model is illustrated in Fig. 1 for the application of the intelligent security monitoring. The source node S (e.g., surveillance camera) needs to transmit the collected data to the destination node D (e.g., controller) for the safety management. A relay node R is employed to help forward the message. Thus, the whole transmission is composed of two phases (hops), as shown in Fig. 1. It is supposed that the relay has already been selected before communications, and the discussion on relay selection is beyond the scope of this paper. In the network, there also exist non-colluding passive eavesdroppers $\{\mathrm{E}_j, j = 1, 2, \ldots\}$ who work independently to intercept the confidential message without information sharing among them. As illustrated in Fig. 1, the main link is defined as the link between the legitimate devices while the eavesdropping link is defined as the link between the legitimate transmitter and the eavesdropper. In general, the locations and channel states of these eavesdroppers are unknown since passive eavesdroppers only listen without transmitting any signal. For analytical tractability, we assume that the spatial distributions of eavesdroppers change independently from one transmit phase to another and the location set of eavesdroppers in phase i ($i = 1, 2$) is modeled as homogeneous PPP, denoted as $\Phi_{\mathrm{E},i}$, with the same density λ_{E}. It is worth noting that the secrecy outage probability under this assumption is an upper bound of the outage probability when eavesdroppers' locations remain unchanged during the two phases [30]. Although the authors in [30] only presented the proofs for single-antenna system, it is not difficult to see that the conclusion also holds for the multi-antenna system described in Section IV and we omit the proof here.

The above conclusion implies that the scenario considered in this paper is a worse case.

Although the introduction of relay can improve communication reliability, it may bring a higher risk of information leakage since the message is transmitted for two times over the two-phase transmission. For traditional relay strategies such as DF or amplify-and-forward (AF), eavesdropper can enhance the decoding capability by combining the two observations together. However, by using the RF strategy, the combination of the two observations will not help recovering the confidential message if the message in each phase is irrecoverable [32]. In other words, securing each phase of the transmission is sufficient to ensure the security of the whole transmission. Thus, the secure transmission probability for the relay network can be written as

$$P_{\text{sec}} = P_{\text{sec},1} P_{\text{sec},2}, \tag{1}$$

where $P_{\text{sec},i}$ $(i = 1, 2)$ denotes the secure transmission probability for the ith phase.

According to [32], RF strategy means that the source and the relay use different codebooks with independent randomness, and for each transmission phase the source (relay) adopts the well-known Wyner's wiretap code [16]. The encoder needs to choose two rates to construct a wiretap code: the rate of transmitted codewords and the rate of confidential message. For the codebook of phase i $(i = 1, 2)$, denote the rates of transmitted codewords and the confidential message as $R_{t,i}$ and $R_{s,i}$, respectively. Note that in the relay network, although the codeword rates for different phases can be different, the rate of the confidential message should be the same [27], i.e., $R_{s,1} = R_{s,2} = R_s$. The rate difference $R_{e,i} \triangleq R_{t,i} - R_s$, namely, the rate redundancy, reflects the cost of securing the message against eavesdropping. We use $C_{\text{M},i}$ and $C_{\text{E},i}$ to denote the channel capacities of the main link and the best eavesdropping link in phase i, respectively. The expressions for $C_{\text{M},i}$ and $C_{\text{E},i}$ will be detailed later in Section III and Section IV. For any transmitted confidential message, the legitimate node can decode correctly if $C_{\text{M},i} \geq R_{t,i}$. Moreover, only when $C_{\text{E},i} < R_{e,i}$ can perfect secrecy be guaranteed [36]. Otherwise, the perfect secrecy fails and a secrecy outage occurs. Thus, the secure transmission probability for phase i can be written as

$$P_{\text{sec},i} = \Pr\left\{C_{\text{E},i} < R_{t,i} - R_s\right\}. \tag{2}$$

Plugging (2) into (1), we obtain the secrecy outage probability for the whole two-hop transmission as below

$$\begin{aligned} P_{\text{out}} &= 1 - P_{\text{sec}} \\ &= 1 - \Pr\left\{C_{\text{E},1} < R_{t,1} - R_s\right\} \Pr\left\{C_{\text{E},2} < R_{t,2} - R_s\right\}. \end{aligned} \tag{3}$$

B. PROBLEM FORMULATION

We consider a secrecy rate maximization problem under the constraint on the secrecy outage probability. We assume that the instantaneous CSI of the main links (S − R link and R − D link) is available while the CSI of eavesdroppers is unknown. In the following, we define the transmit signal-to-noise ratio (SNR) ρ as the ratio of the transmit power P to the noise power σ^2, i.e., $\rho \triangleq P/\sigma^2$, with the assumption that the noise power at all the receivers is the same. Denote the transmit SNRs at the source and the relay as ρ_1 and ρ_2, respectively. An aggregate transmit power (transmit SNR) constraint ρ_0 is assumed, i.e., $\rho_1 + \rho_2 \leq \rho_0$. According to the aforementioned RF strategy, the source and the relay use different codebooks to transmit the same confidential message. Therefore, we aim to maximize the instantaneous secrecy rate with the given CSI of main links by optimizing the rates of the two codebooks and the power allocation between the source and relay. Based on the above discussions, the optimization problem can be formulated as the problem **P**1:

$$\max_{R_{t,1}, R_{t,2}, R_s, \rho_1, \rho_2} \quad T_s \tag{4a}$$

$$\text{s.t. } P_{\text{out}} \leq \varepsilon, \tag{4b}$$

$$0 \leq R_{t,1} \leq C_{\text{M},1}, \quad 0 \leq R_{t,2} \leq C_{\text{M},2}, \tag{4c}$$

$$0 \leq R_s \leq \min\{R_{t,1}, R_{t,2}\}, \tag{4d}$$

$$\rho_1 + \rho_2 \leq \rho_0, \quad \rho_1 \geq 0, \ \rho_2 \geq 0, \tag{4e}$$

where $T_s = \frac{1}{2} R_s$ is the secrecy rate which is half of the rate of the confidential message due to the two-hop transmission. The constraint in (4b) limits the secrecy outage probability, the constraint in (4c) guarantees the decodability at the legitimate receiver, the constraint in (4d) implies that the rate of the confidential message should be less than the rate of the codeword, and the constraint in (4e) gives the feasible range of the allocated power.

III. SINGLE-ANTENNA SYSTEMS

In this section, we study the optimization problem **P1** in a single-antenna system. We consider a scenario where all the devices in the network including eavesdroppers are equipped with single antenna. The channel model in this paper includes both large- and small-scale fading. For the large-scale fading, we adopt the traditional path-loss fading model $d_{m,n}^{-\alpha/2}$, where $d_{m,n}$ denotes the distance between node m and node n, α is the path-loss exponent. The small-scale fading, denoted as $h_{m,n}$, is assumed to follow the circularly symmetric complex Gaussian distribution with zero mean and unit variance, i.e., $h_{m,n} \sim \mathcal{CN}(0, 1)$. We assume that a dedicated frequency band is allocated to this IoT network and all transmissions happen on orthogonal channels in frequency or in time by using some collision-free multiple access techniques. In this case, the channel capacity is only determined by the transmit SNR and the fading coefficient of the channel. Thus, for the ith $(i = 1, 2)$ phase, the channel capacity of the main link is given by

$$C_{\text{M},1} = \log_2\left(1 + \rho_1 |h_{\text{SR}}|^2 d_{\text{SR}}^{-\alpha}\right) \tag{5}$$

and

$$C_{\text{M},2} = \log_2\left(1 + \rho_2 |h_{\text{RD}}|^2 d_{\text{RD}}^{-\alpha}\right), \tag{6}$$

respectively.

Similarly, due to the assumption of the non-colluding eavesdropping scenario, we only need to calculate the channel capacity of the best eavesdropping link for each phase, respectively given as

$$C_{\mathrm{E},1} = \log_2\left(1 + \max_{\mathrm{E}_j \in \Phi_{\mathrm{E},1}} \rho_1 \left|h_{\mathrm{SE}_j}\right|^2 d_{\mathrm{SE}_j}^{-\alpha}\right) \tag{7}$$

and

$$C_{\mathrm{E},2} = \log_2\left(1 + \max_{\mathrm{E}_j \in \Phi_{\mathrm{E},2}} \rho_2 \left|h_{\mathrm{RE}_j}\right|^2 d_{\mathrm{RE}_j}^{-\alpha}\right). \tag{8}$$

According to the constraints in (4c) and (4d), to maximize the secrecy rate T_s, the transmitted codeword rates $R_{t,1}$ and $R_{t,2}$ should be maximized first. Hence, we set $R_{t,1} = C_{\mathrm{M},1}$ and $R_{t,2} = C_{\mathrm{M},2}$. Based on the expression in (2), the secure transmission probability for the first phase can now be derived as

$$\begin{aligned}
&P_{\mathrm{sec},1} \\
&= \Pr\left\{C_{\mathrm{E},1} < C_{\mathrm{M},1} - R_s\right\} \\
&= \mathbb{E}_{\Phi_{\mathrm{E},1}}\left\{\Pr\left(\max_{\mathrm{E}_j \in \Phi_{\mathrm{E},1}} \left\{\left|h_{\mathrm{SE}_j}\right|^2 d_{\mathrm{SE}_j}^{-\alpha}\right\}\right.\right. \\
&\qquad \left.\left. < \frac{1 + \rho_1 \left|h_{\mathrm{SR}}\right|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}{\rho_1 2^{R_s}} \,\middle|\, \Phi_{\mathrm{E},1}\right)\right\} \\
&= \mathbb{E}_{\Phi_{\mathrm{E},1}}\left\{\prod_{\mathrm{E}_j \in \Phi_{\mathrm{E},1}} \Pr\left(\left|h_{\mathrm{SE}_j}\right|^2\right.\right. \\
&\qquad \left.\left. < \frac{1 + \rho_1 \left|h_{\mathrm{SR}}\right|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}{\rho_1 2^{R_s} d_{\mathrm{SE}_j}^{-\alpha}} \,\middle|\, \Phi_{\mathrm{E},1}\right)\right\} \\
&= \mathbb{E}_{\Phi_{\mathrm{E},1}}\left\{\prod_{\mathrm{E}_j \in \Phi_{\mathrm{E},1}} \left[1 - \exp\left(-\frac{1 + \rho_1 \left|h_{\mathrm{SR}}\right|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}{\rho_1 2^{R_s} d_{\mathrm{SE}_j}^{-\alpha}}\right)\right]\right\} \\
&\overset{(a)}{=} \exp\left[-\lambda_{\mathrm{E}} \int_0^{2\pi} \int_0^{\infty} r \exp\left(-\frac{1 + \rho_1 \left|h_{\mathrm{SR}}\right|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}{\rho_1 2^{R_s} r^{-\alpha}}\right) dr d\theta\right] \\
&\overset{(b)}{=} \exp\left[-\theta\left(\frac{\rho_1 2^{R_s}}{1 + \rho_1 \left|h_{\mathrm{SR}}\right|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}\right)^{\beta}\right],
\end{aligned} \tag{9}$$

where $\theta = 2\pi\lambda_{\mathrm{E}}\Gamma\left(2/\alpha\right)/\alpha$ and $\beta = 2/\alpha$. (a) is calculated in a polar coordinate based on the probability generating functional lemma over PPP [37]. In this coordinate, the source is located at the origin and the location of E_j is denoted as $\left(r_j, \theta_j\right) \in \mathbb{R}^2$. (b) is obtained by using the formula [38, eq. (3.326.2)].

Similarly, the secure transmission probability for the second phase is given by

$$P_{\mathrm{sec},2} = \exp\left[-\theta\left(\frac{\rho_2 2^{R_s}}{1 + \rho_2 \left|h_{\mathrm{RD}}\right|^2 d_{\mathrm{RD}}^{-\alpha} - 2^{R_s}}\right)^{\beta}\right]. \tag{10}$$

By plugging (9) and (10) into (3), we obtain the secrecy outage probability for the whole transmission as

$$\begin{aligned}
P_{\mathrm{out}} = 1 - \exp\Bigg[-\theta\Bigg(&\left(\frac{\rho_1 2^{R_s}}{1 + \rho_1 \left|h_{\mathrm{SR}}\right|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}\right)^{\beta} \\
&+ \left(\frac{\rho_2 2^{R_s}}{1 + \rho_2 \left|h_{\mathrm{RD}}\right|^2 d_{\mathrm{RD}}^{-\alpha} - 2^{R_s}}\right)^{\beta}\Bigg)\Bigg].
\end{aligned} \tag{11}$$

To derive the optimal solution, the inequality constraint on the transmit SNR in (4e) can be first transformed into an equality constraint based on the following lemma.

Lemma 1: For the maximization of the secrecy rate, all the available transmit power should be utilized, i.e., $\rho_1 + \rho_2 = \rho_0$.

Proof: From (11), we can see that the transmission is allowed only when the following two conditions $\rho_1 > \left(2^{R_s} - 1\right) d_{\mathrm{SR}}^{\alpha} / \left|h_{\mathrm{SR}}\right|^2$ and $\rho_2 > \left(2^{R_s} - 1\right) d_{\mathrm{RD}}^{\alpha} / \left|h_{\mathrm{RD}}\right|^2$ hold. When the transmission is carried out, one can validate that $\partial P_{\mathrm{out}}/\partial\rho_1 < 0$ and $\partial P_{\mathrm{out}}/\partial\rho_2 < 0$, which shows that the increase of transmit SNR will lower the secrecy outage probability. This result seems not so intuitive since the received SNR at eavesdropper rises with the increase of transmit power, which will result in higher secrecy outage probability. However, the capacity of the main link is also enhanced, which enables higher codeword rate as well as higher redundancy rate. Note that higher redundancy rate can decrease the secrecy outage probability, as discussed in Section II-A. After taking all these into consideration and averaging the outage probability over eavesdroppers' locations and channel states, we find that it is still beneficial to improve the transmit power.

In addition, since $\partial P_{\mathrm{out}}/\partial R_s > 0$, the maximum R_s that satisfies the outage probability constraint is reached when $P_{\mathrm{out}} = \varepsilon$. Then, according to the derivative rule for implicit functions, we have

$$\frac{dR_s}{d\rho_i} = -\frac{\partial P_{\mathrm{out}}}{\partial \rho_i} \Big/ \frac{\partial P_{\mathrm{out}}}{\partial R_s} > 0, \quad i = 1, 2. \tag{12}$$

This shows that improving the transmit power will enhance the maximum rate of the confidential message, which completes our proof. ■

Thus, we can use a power allocation parameter η to describe the power allocation scheme where $\eta\rho_0$ denotes the transmit SNR of the source and $(1-\eta)\rho_0$ denotes the transmit SNR of the relay. The secrecy rate maximization problem **P1** can now be transformed into the following power allocation problem **P2** :

$$\max_{\eta, R_s} \; T_s \tag{13a}$$

$$\text{s.t.}\; \tilde{P}_{\mathrm{out}} \le \varepsilon, \tag{13b}$$

$$0 \le \eta \le 1, \tag{13c}$$

where the expression for $\tilde{P}_{\mathrm{out}}$ is obtained by replacing ρ_1 and ρ_2 in (11) with $\eta\rho_0$ and $(1-\eta)\rho_0$, respectively,

shown as

$$\tilde{P}_{\text{out}} = 1 - \exp\left[-\theta\left(\left(\frac{\eta\rho_0 2^{R_s}}{1+\eta\rho_0\left|h_{\text{SR}}\right|^2 d_{\text{SR}}^{-\alpha} - 2^{R_s}}\right)^{\beta} + \left(\frac{(1-\eta)\rho_0 2^{R_s}}{1+(1-\eta)\rho_0\left|h_{\text{RD}}\right|^2 d_{\text{RD}}^{-\alpha} - 2^{R_s}}\right)^{\beta}\right)\right]. \tag{14}$$

The constraint in (4c) is omitted since we set the rate of the transmitted codeword as the channel capacity. The constraint in (4d) has been considered in the derivation process of $\tilde{P}_{\text{out}}$ so it is also omitted in the problem **P2**. We now give the optimal solution to problem **P2**, as shown in the following proposition.

Proposition 1: For the given channel gains of the main links $\mathbf{h} = \left(|h_{\text{SR}}|^2, |h_{\text{RD}}|^2\right)$, only when $\mathbf{h} \in \mathcal{H}$ can transmission be carried out. Denote the optimal power allocation parameter as $\eta^*(\mathbf{h})$. The optimal rate settings are

$$\begin{cases} \mathcal{R}_{t,1}^*(\mathbf{h}) = \log_2\left(1+\eta^*(\mathbf{h})\rho_0\left|h_{\text{SR}}\right|^2 d_{\text{SR}}^{-\alpha}\right), \\ \mathcal{R}_{t,2}^*(\mathbf{h}) = \log_2\left(1+(1-\eta^*(\mathbf{h}))\,\rho_0\left|h_{\text{RD}}\right|^2 d_{\text{RD}}^{-\alpha}\right), \\ \mathcal{R}_s^*(\mathbf{h}) = \tilde{R}_s\left(\eta,\mathbf{h}\right)|_{\eta=\eta^*(\mathbf{h})}, \end{cases} \tag{15}$$

where $\tilde{R}_s\left(\eta,\mathbf{h}\right)$ is the unique root of $\tilde{P}_{\text{out}} = \varepsilon$ for any given η. The value of $\eta^*(\mathbf{h})$ is the unique root of the following equation

$$\left(\frac{1+(1-\eta)\rho_0\left|h_{\text{RD}}\right|^2 d_{\text{RD}}^{-\alpha} - 2^{R_s}}{1+\eta\rho_0\left|h_{\text{SR}}\right|^2 d_{\text{SR}}^{-\alpha} - 2^{R_s}}\right)^{1+\beta}\left(\frac{1-\eta}{\eta}\right)^{1-\beta} = 1. \tag{16}$$

Denote the maximum achievable secrecy rate for any given η by $\tilde{T}_s\left(\eta,\mathbf{h}\right) = \frac{1}{2}\tilde{R}_s\left(\eta,\mathbf{h}\right)$. Thus, the maximum secrecy rate for given main channel states is

$$\mathcal{T}_s^*(\mathbf{h}) = \tilde{T}_s\left(\eta,\mathbf{h}\right)|_{\eta=\eta^*(\mathbf{h})} = \begin{cases} \frac{1}{2}\mathcal{R}_s^*(\mathbf{h}), & \mathbf{h}\in\mathcal{H}, \\ 0, & \mathbf{h}\notin\mathcal{H}, \end{cases} \tag{17}$$

where the transmission set is

$$\mathcal{H} = \left\{\mathbf{h}\left|1-\exp\left[-\theta\left(\left(d_{\text{SR}}^{\alpha}/\left|h_{\text{SR}}\right|^2\right)^{\beta} + \left(d_{\text{RD}}^{\alpha}/\left|h_{\text{RD}}\right|^2\right)^{\beta}\right)\right] < \varepsilon\right.\right\}. \tag{18}$$

Proof: Note that the above optimal settings are related to $\mathbf{h}$ since we adjust transmission strategy based on main channels' instantaneous CSI. As mentioned in previous paragraphs, to maximize R_s, the transmitted codeword rate $R_{t,1}$ and $R_{t,2}$ should be set as the maximum value. Hence, we have $R_{t,1} = C_{\text{M},1} = \log_2\left(1+\eta\rho_0\left|h_{\text{SR}}\right|^2 d_{\text{SR}}^{-\alpha}\right)$ and $R_{t,2} = C_{\text{M},2} = \log_2\left(1+(1-\eta)\rho_0\left|h_{\text{RD}}\right|^2 d_{\text{RD}}^{-\alpha}\right)$. The derivation of $\eta^*(\mathbf{h})$ is given as follows.

For any fixed η, since $\partial\tilde{P}_{\text{out}}/\partial R_s > 0$, the maximum achievable rate of confidential message, denoted as $\tilde{R}_s(\eta,\mathbf{h})$, is achieved when $\tilde{P}_{\text{out}} = \varepsilon$. Thus, according to the derivative rule for implicit functions, we have

$$\frac{d\tilde{R}_s(\eta,\mathbf{h})}{d\eta} = -\frac{\partial\tilde{P}_{\text{out}}}{\partial\eta}\Big/\frac{\partial\tilde{P}_{\text{out}}}{\partial\tilde{R}_s(\eta,\mathbf{h})}, \tag{19}$$

where $\partial\tilde{P}_{\text{out}}/\partial\tilde{R}_s(\eta,\mathbf{h}) > 0$ always holds.

To simplify the discussion of $\partial\tilde{P}_{\text{out}}/\partial\eta$, we define a function $\tilde{g}_{\text{out}}$ shown as

$$\tilde{g}_{\text{out}} = \left(\frac{\eta\rho_0 2^{R_s}}{1+\eta\rho_0\left|h_{\text{SR}}\right|^2 d_{\text{SR}}^{-\alpha} - 2^{R_s}}\right)^{\beta} + \left(\frac{(1-\eta)\rho_0 2^{R_s}}{1+(1-\eta)\rho_0\left|h_{\text{RD}}\right|^2 d_{\text{RD}}^{-\alpha} - 2^{R_s}}\right)^{\beta}. \tag{20}$$

By studying the derivative, we find that $\tilde{P}_{\text{out}}$ and $\tilde{g}_{\text{out}}$ have the same monotonicity w.r.t η. Therefore, we will investigate the property of $\tilde{g}_{\text{out}}$ instead. The expression of $\partial\tilde{g}_{\text{out}}/\partial\eta$ is given by

$$\frac{\partial\tilde{g}_{\text{out}}}{\partial\eta} = \beta\left(2^{R_s}-1\right)\left[\frac{\left((1-\eta)\rho_0 2^{R_s}\right)^{\beta}}{(1-\eta)I_2^{\beta+1}} - \frac{\left(\eta\rho_0 2^{R_s}\right)^{\beta}}{\eta I_1^{\beta+1}}\right], \tag{21}$$

where $I_1 = 1+\eta\rho_0\left|h_{\text{SR}}\right|^2 d_{\text{SR}}^{-\alpha} - 2^{R_s}$ and $I_2 = 1+(1-\eta)\rho_0\left|h_{\text{RD}}\right|^2 d_{\text{RD}}^{-\alpha} - 2^{R_s}$. Note that $2^{R_s}-1 \geq 0$ always holds since $R_s \geq 0$. Hence, when $\partial\tilde{g}_{\text{out}}/\partial\eta \geq 0$, the following inequality should hold, given as

$$\underbrace{\left(\frac{I_2}{I_1}\right)^{1+\beta}\left(\frac{1-\eta}{\eta}\right)^{1-\beta}}_{L(\eta)} \leq 1. \tag{22}$$

It is not difficult to validate that $dL(\eta)/d\eta < 0$. Moreover, since $L(\eta)|_{\eta=0} = \infty$ and $L(\eta)|_{\eta=1} = 0$, with the increase of η, $L(\eta)$ is first larger than 1 and then smaller than 1. Recalling the requirement in (22), we find that $\partial\tilde{g}_{\text{out}}/\partial\eta$ is first negative and then positive, which means that $d\tilde{R}_s(\eta,\mathbf{h})/d\eta$ is first positive and then negative according to (19). Therefore, the optimal $\eta^*(\mathbf{h})$ that maximizes R_s is the root of the equation $L(\eta) = 1$ which is the same as (16).

Finally, we derive the transmission set $\mathcal{H}$. Since $\tilde{P}_{\text{out}}$ is a monotonically increasing function of R_s, $\tilde{P}_{\text{out}}$ achieves its minimum value when $R_s = 0$. Therefore, to realize a positive secrecy rate with the secrecy-outage-probability constraint, we should have $\tilde{P}_{\text{out}}|_{R_s=0} < \varepsilon$. Thus, the transmission set can be derived as

$$\mathcal{H} = \left\{\mathbf{h}\left|\tilde{P}_{\text{out}}|_{R_s=0} < \varepsilon\right.\right\} \tag{23}$$

with

$$\tilde{P}_{\text{out}}|_{R_s=0} = 1-\exp\left[-\theta\left(\left(d_{\text{SR}}^{\alpha}/\left|h_{\text{SR}}\right|^2\right)^{\beta} + \left(d_{\text{RD}}^{\alpha}/\left|h_{\text{RD}}\right|^2\right)^{\beta}\right)\right].$$

■

According to Proposition 1, the optimal $\left(\eta^*(\mathbf{h}), \mathcal{R}_s^*(\mathbf{h})\right)$ is the unique root of the nonlinear equations constituted by $\tilde{P}_{\text{out}} = \varepsilon$ and the equation in (16), which can be easily solved by the Newton-Raphson method. Moreover, for the special case $\alpha = 2$, a closed-form $\eta^*(\mathbf{h})$ is derived below from which we can gain some insights into the optimal power allocation.

Corollary 1: For the special case where $\alpha = 2$, we can obtain a closed-form expression for $\eta^*(\mathbf{h})$, shown as

$$\eta^*(\mathbf{h}) = \frac{|h_{\mathrm{RD}}|^2 d_{\mathrm{RD}}^{-2}}{|h_{\mathrm{SR}}|^2 d_{\mathrm{SR}}^{-2} + |h_{\mathrm{RD}}|^2 d_{\mathrm{RD}}^{-2}} \tag{24}$$

with which the capacities of main links in the two phases are the same.

Proof: Substituting $\alpha = 2$ and $\beta = 1$ into (16), we get

$$\frac{1 + (1-\eta)\rho_0 |h_{\mathrm{RD}}|^2 d_{\mathrm{RD}}^{-2} - 2^{R_s}}{1 + \eta\rho_0 |h_{\mathrm{SR}}|^2 d_{\mathrm{SR}}^{-2} - 2^{R_s}} = 1. \tag{25}$$

Solving the above equation we can obtain the optimal power allocation parameter in (24). With this parameter, the main channel's capacities in the two phases are the same, i.e., $C_{\mathrm{M},1} = C_{\mathrm{M},2} = \log_2(1 + \rho_0 K_1 K_2/(K_1 + K_2))$ where $K_1 = |h_{\mathrm{SR}}|^2 d_{\mathrm{SR}}^{-2}$ and$K_2 = |h_{\mathrm{RD}}|^2 d_{\mathrm{RD}}^{-2}$. ■

For the DF relay network without secrecy requirement, the system throughput depends on the minimum of two phases' capacities. Thus, the optimal power allocation should balance the capacities of two phases. It is interesting that when $\alpha = 2$, the optimal power allocation in (24) is the same as the capacity balancing scheme. However, when $\alpha \neq 2$, the power allocation result is much more complex and cannot be expressed in a simple formula. Recalling the equation in (16), we find that the main difference between the optimal power allocation for systems with and without secrecy requirement is the term $((1-\eta)/\eta)^{1-\beta}$. For the case $\alpha = 2$, this term is exactly equal to 1 and leads to the same result as the capacity balancing scheme. For other cases, this term works and leads to a different result, which considers both the capacity of the main link as well as the intercepted signal strength at eavesdroppers. Although the optimal scheme $\eta^*(\mathbf{h})$ and the capacity balancing scheme are different, they can achieve similar performances, which will be shown by numerical examples in Section V.

Similar to the proof in (12), it is not difficult to prove that $\mathcal{R}_s^*(\mathbf{h})$ is a monotonically increasing function of the total transmit SNR ρ_0. However, when $\rho_0 \to \infty$, $\mathcal{R}_s^*(\mathbf{h})$ tends to a finite constant $\mathcal{R}_{s,max}^*(\mathbf{h})$, which shows that at high SNR, increasing the transmit power cannot further enhance the secrecy rate. The value of $\mathcal{R}_{s,max}^*(\mathbf{h})$ is analyzed in the following corollary.

Corollary 2: As $\rho_0 \to \infty$, $\mathcal{R}_s^*(\mathbf{h})$ tends to a finite constant $\mathcal{R}_{s,max}^*(\mathbf{h})$, given as

$$\mathcal{R}_{s,max}^*(\mathbf{h}) = \frac{1}{\beta}\left[\log_2\left(-\frac{1}{\theta}\ln(1-\varepsilon)\right) - \log_2\left(\frac{d_{\mathrm{SR}}^2}{|h_{\mathrm{SR}}|^{2\beta}} + \frac{d_{\mathrm{RD}}^2}{|h_{\mathrm{RD}}|^{2\beta}}\right)\right], \tag{26}$$

which does not depend on the total transmit SNR ρ_0 or power allocation parameter η.

Proof: When $\rho_0 \to \infty$, the secrecy outage probability in (14) can be simplified as

$$\tilde{P}_{\mathrm{out}}|_{\rho_0=\infty} = 1 - \exp\left[-\theta\left(\left(\frac{2^{R_s}}{|h_{\mathrm{SR}}|^2 d_{\mathrm{SR}}^{-\alpha}}\right)^{\beta} + \left(\frac{2^{R_s}}{|h_{\mathrm{RD}}|^2 d_{\mathrm{RD}}^{-\alpha}}\right)^{\beta}\right)\right]. \tag{27}$$

By solving the equation $\tilde{P}_{\mathrm{out}}|_{\rho_0=\infty} = \varepsilon$ we can obtain the finite constant $\mathcal{R}_{s,max}^*(\mathbf{h})$. ■

For the communication system without secrecy requirement, improving transmit power can always enhance the message rate. In other words, the message rate will be infinite if the transmit power goes to infinity. However, this is not true for system with secrecy requirement. Although improving transmit power can enhance $\mathcal{R}_s^*(\mathbf{h})$ at first, when the SNR is high enough, $\mathcal{R}_s^*(\mathbf{h})$ tends to a constant value determined by the channel states. The essential reason is that the improvement of transmit power benefits both the main and eavesdropping links.

IV. MULTI-ANTENNA SYSTEMS

In Section III, we investigate the secure transmission in the single-antenna system where all devices including eavesdroppers are equipped with single antenna. In the IoT network, different kinds of devices are connected together, whose number of antennas may be different. To further improve security, the source can choose a multi-antenna relay to help forward the confidential message. For example, in the heterogeneous sensor networks [34], [35], there are two physically different types of nodes: High-end sensors (H-sensors) and Low-end sensors (L-sensors). It is usually assumed that H-sensors are more capable than L-sensors in terms of energy supply or signal processing capabilities. When two L-sensors want to exchange information, they can either choose an L-sensor or an H-sensor to help relay the message. In Section III we have studied the case where all legitimate devices are L-sensors with the single antenna. In this section we will concentrate on the scenario where the source and the destination are still L-sensors while the relay is an H-sensor equipped with multiple antennas. Due to the improvement of legitimate devices' capabilities, in the following analyses we assume that the randomly distributed eavesdroppers are also equipped with multiple antennas.

Assume that the relay is equipped with N_{R} antennas and each eavesdropper is equipped with N_{E} antennas. The large-scale channel model is the same as the one defined in Section III. For the legitimate nodes, denote the small-scale fading coefficient from the source to the relay, the relay to the destination as $\mathbf{h}_{\mathrm{SR}} \in \mathbb{C}^{N_{\mathrm{R}}\times 1}$ and $\mathbf{h}_{\mathrm{RD}}^H \in \mathbb{C}^{1\times N_{\mathrm{R}}}$, respectively, where $(\cdot)^H$ represents the Hermitian transpose. For eavesdroppers, denote the small-scale fading coefficients from the source and the relay to eavesdropper E_j as $\mathbf{h}_{\mathrm{SE}_j} \in \mathbb{C}^{N_{\mathrm{E}}\times 1}$ and $\mathbf{H}_{RE_j} \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{R}}}$, respectively. The entries of all the above

coefficients follow the identical and independent $\mathcal{CN}(0,1)$ distributions.

During the first transmission phase, the relay performs MRC on the received signal to enhance decoding capability. Similarly, eavesdroppers also utilize MRC to maximize their received SNRs. Thus, for the first transmission phase the channel capacities of the main and the eavesdropping link are respectively given by

$$C_{\mathrm{M},1} = \log_2\left(1+\rho_1 \left\|\mathbf{h}_{\mathrm{SR}}\right\|^2 d_{\mathrm{SR}}^{-\alpha}\right) \tag{28}$$

and

$$C_{\mathrm{E},1} = \log_2\left(1+\max_{\mathrm{E}_j\in\Phi_{\mathrm{E},1}} \rho_1 \left\|\mathbf{h}_{\mathrm{SE}_j}\right\|^2 d_{\mathrm{SE}_j}^{-\alpha}\right), \tag{29}$$

where ρ_i $(i=1,2)$ is the transmit SNR defined in the last section.

During the second transmission phase, the relay employs the maximum ratio transmission (MRT) beamforming with the normalized beamforming vector $\mathbf{t} = \mathbf{h}_{\mathrm{RD}}/\left\|\mathbf{h}_{\mathrm{RD}}\right\|$. We consider a worst case where eavesdroppers E_j knows the beamforming vector $\mathbf{t}$ and the eavesdropping link $\mathbf{H}_{RE_j}$, and exploits MRC to maximize the received SNR. Thus, for the second phase the channel capacities of the main and the eavesdropping link are respectively given by

$$C_{\mathrm{M},2} = \log_2\left(1+\rho_2 \left\|\mathbf{h}_{\mathrm{RD}}\right\|^2 d_{\mathrm{RD}}^{-\alpha}\right) \tag{30}$$

and

$$C_{\mathrm{E},2} = \log_2\left(1+\max_{\mathrm{E}_j\in\Phi_{\mathrm{E},2}} \rho_2 \left\|\mathbf{H}_{\mathrm{RE}_j}\mathbf{t}\right\|^2 d_{\mathrm{RE}_j}^{-\alpha}\right). \tag{31}$$

As discussed in the last section, to maximize R_s we should set $R_{t,1} = C_{\mathrm{M},1}$ and $R_{t,2} = C_{\mathrm{M},2}$. Before deriving the secure transmission probability for the first phase, we establish a polar coordinate where the source is located at the origin. We use x_{E_j} to denote the location of eavesdropper E_j, the detailed polar coordinate of which is $(r_j,\theta_j)\in\mathbb{R}^2$. Moreover, since the entries of $\mathbf{h}_{\mathrm{SE}_j}$ follow independent $\mathcal{CN}(0,1)$, the square of each entry's modulus follows exponential distribution with mean 1. Therefore, we have $\left\|\mathbf{h}_{\mathrm{SE}_j}\right\|^2 \sim \Gamma(N_{\mathrm{E}},1)$. Then, according to the expression in (2), the secure transmission probability for the first phase is given by

$$\begin{aligned}
&P_{\mathrm{sec},1}\\
&= \Pr\left\{C_{\mathrm{E},1} < C_{\mathrm{M},1} - R_s\right\}\\
&= \mathbb{E}_{\Phi_{\mathrm{E},1}}\left\{\prod_{\mathrm{E}_j\in\Phi_{\mathrm{E},1}} \Pr\left(\left\|\mathbf{h}_{\mathrm{SE}_j}\right\|^2 < \underbrace{\frac{1+\rho_1\left\|\mathbf{h}_{\mathrm{SR}}\right\|^2 d_{\mathrm{SR}}^{-\alpha} - 2^{R_s}}{\rho_1 2^{R_s} d_{\mathrm{SE}_j}^{-\alpha}}}_{c_j}\middle|\Phi_{\mathrm{E},1}\right)\right\}\\
&\overset{(a)}{=} \mathbb{E}_{\Phi_{\mathrm{E},1}}\left\{\prod_{\mathrm{E}_j\in\Phi_{\mathrm{E},1}} \frac{1}{\Gamma(N_{\mathrm{E}})}\gamma\left(N_{\mathrm{E}},c_j\right)\right\}\\
&= \exp\left[-\lambda_{\mathrm{E}}\int_{\mathbb{R}^2}\left(1-\frac{1}{\Gamma(N_{\mathrm{E}})}\gamma\left(N_{\mathrm{E}},c_j\right)\right)dx_{\mathrm{E}_j}\right]\\
&\overset{(b)}{=} \exp\left[-\lambda_{\mathrm{E}}\int_{\mathbb{R}^2} e^{-c_j}\sum_{m=0}^{N_{\mathrm{E}}-1}\frac{c_j^m}{m!}\,dx_{\mathrm{E}_j}\right]\\
&= \exp\left[-\lambda_{\mathrm{E}}\int_0^{2\pi}\int_0^{\infty} r\exp\left(-\frac{1+\rho_1\left\|\mathbf{h}_{\mathrm{SR}}\right\|^2 d_{\mathrm{SR}}^{-\alpha}-2^{R_s}}{\rho_1 2^{R_s} r^{-\alpha}}\right)\right.\\
&\qquad\left.\times\sum_{m=0}^{N_{\mathrm{E}}-1}\frac{1}{m!}\left(\frac{1+\rho_1\left\|\mathbf{h}_{\mathrm{SR}}\right\|^2 d_{\mathrm{SR}}^{-\alpha}-2^{R_s}}{\rho_1 2^{R_s} r^{-\alpha}}\right)^m dr d\theta\right]\\
&\overset{(c)}{=} \exp\left[-\frac{2\pi\lambda_{\mathrm{E}}}{\alpha}\sum_{m=0}^{N_{\mathrm{E}}-1}\frac{\Gamma(m+\beta)}{m!}\right.\\
&\qquad\left.\times\left(\frac{\rho_1 2^{R_s}}{1+\rho_1\left\|\mathbf{h}_{\mathrm{SR}}\right\|^2 d_{\mathrm{SR}}^{-\alpha}-2^{R_s}}\right)^{\beta}\right],
\end{aligned} \tag{32}$$

where (a) is obtained by using the formula [38, eq. (8.350.1)] and $\gamma(a,x)$ is the incomplete gamma function $\gamma(a,x) = \int_0^x e^{-t}t^{a-1}dt$. (b) follows from the expression for $\gamma(a,x)$ in [38, eq. (8.352.6)] when a is a positive integer. (c) is calculated by the formula in [38, eq. (3.326.2)] with the variable transformation $\beta = 2/\alpha$.

As for the second transmission phase, since the beamforming vector $\mathbf{t}$ has been normalized, we have $\left\|\mathbf{H}_{\mathrm{RE}_j}\mathbf{t}\right\|^2 \sim \Gamma(N_{\mathrm{E}},1)$, which has the same distribution as $\left\|\mathbf{h}_{\mathrm{SE}_j}\right\|^2$. Similarly, by moving the origin of the polar coordinate to the relay, which has no influence on the PPP distribution [37], we obtain the secure transmission probability for the second phase, shown as

$$\begin{aligned}
P_{\mathrm{sec},2} = \exp\left[-\frac{2\pi\lambda_{\mathrm{E}}}{\alpha}\sum_{m=0}^{N_{\mathrm{E}}-1}\frac{\Gamma(m+\beta)}{m!}\right.\\
\left.\times\left(\frac{\rho_2 2^{R_s}}{1+\rho_2\left\|\mathbf{h}_{\mathrm{RD}}\right\|^2 d_{\mathrm{RD}}^{-\alpha}-2^{R_s}}\right)^{\beta}\right].
\end{aligned} \tag{33}$$

According to the expression in (3), the secrecy outage probability for the whole transmission can be derived as

$$\begin{aligned}
P_{\mathrm{out}} = 1-\exp\left[-\phi\left(\left(\frac{\rho_1 2^{R_s}}{1+\rho_1\left\|\mathbf{h}_{\mathrm{SR}}\right\|^2 d_{\mathrm{SR}}^{-\alpha}-2^{R_s}}\right)^{\beta}\right.\right.\\
\left.\left.+\left(\frac{\rho_2 2^{R_s}}{1+\rho_2\left\|\mathbf{h}_{\mathrm{RD}}\right\|^2 d_{\mathrm{RD}}^{-\alpha}-2^{R_s}}\right)^{\beta}\right)\right],
\end{aligned} \tag{34}$$

where $\phi = \frac{2\pi\lambda_{\mathrm{E}}}{\alpha}\sum_{m=0}^{N_{\mathrm{E}}-1}\frac{\Gamma(m+\beta)}{m!}$. Comparing (34) with (11), we find that the secrecy outage probabilities for the two systems have the similar expressions. Actually, (11) can be directly

obtained from (34) by setting $N_{\mathrm{E}} = 1$, after which we have $\phi|_{N_{\mathrm{E}}=1} = \theta$. This is because the source and the destination in both systems are equipped with single antenna, in which case we can only transmit one data stream in the network. Moreover, we only employ MRT beamforming at the multi-antenna relay without broadcasting artificial noise. Thus, the single-antenna system is a special case of the multi-antenna system with $N_{\mathrm{R}} = 1$ and $N_{\mathrm{E}} = 1$.

Since the expression in (34) is similar to the expression in (11), we can directly use the results given in Section III to derive the optimal solution to problem **P1** for the multi-antenna system. Likewise, according to Lemma 1, we change the inequality constraint in (4e) to an equality constraint with power allocation parameter η. Thus, the optimization problem **P1** can now be transformed into the following power allocation problem **P3**:

$$\max_{\eta, R_s} \; T_s \tag{35a}$$

$$\text{s.t. } \tilde{P}_{\text{out}} \leq \varepsilon, \tag{35b}$$

$$0 \leq \eta \leq 1, \tag{35c}$$

where $\tilde{P}_{\text{out}}$ is given as

$$\tilde{P}_{\text{out}} = 1 - \exp\left[-\phi\left(\left(\frac{\eta\rho_0 2^{R_s}}{1+\eta\rho_0\left\|\mathbf{h}_{\text{SR}}\right\|^2 d_{\text{SR}}^{-\alpha} - 2^{R_s}}\right)^{\beta} + \left(\frac{(1-\eta)\rho_0 2^{R_s}}{1+(1-\eta)\rho_0\left\|\mathbf{h}_{\text{RD}}\right\|^2 d_{\text{RD}}^{-\alpha} - 2^{R_s}}\right)^{\beta}\right)\right]. \tag{36}$$

The optimal solution to problem **P3** can be directly obtained based on the Proposition 1. We omit the derivations here and present the optimal solutions in the following proposition.

Proposition 2: For the given channel gains of the main links $\mathbf{h} = \left(\left\|\mathbf{h}_{\text{SR}}\right\|^2, \left\|\mathbf{h}_{\text{RD}}\right\|^2\right)$, only when $\mathbf{h} \in \mathcal{H}$ can transmission be carried out. Denote the optimal power allocation parameter as $\eta^*(\mathbf{h})$. The optimal rate settings are

$$\begin{cases} \mathcal{R}_{t,1}^*(\mathbf{h}) = \log_2\left(1+\eta^*(\mathbf{h})\rho_0\left\|\mathbf{h}_{\text{SR}}\right\|^2 d_{\text{SR}}^{-\alpha}\right), \\ \mathcal{R}_{t,2}^*(\mathbf{h}) = \log_2\left(1+(1-\eta^*(\mathbf{h}))\,\rho_0\left\|\mathbf{h}_{\text{RD}}\right\|^2 d_{\text{RD}}^{-\alpha}\right), \\ \mathcal{R}_s^*(\mathbf{h}) = \tilde{R}_s\left(\eta, \mathbf{h}\right)|_{\eta=\eta^*(\mathbf{h})}, \end{cases} \tag{37}$$

where $\tilde{R}_s\left(\eta, \mathbf{h}\right)$ is the unique root of $\tilde{P}_{\text{out}} = \varepsilon$ for any given η. The value of $\eta^*(\mathbf{h})$ is the unique root of the following equation

$$\left(\frac{1+(1-\eta)\rho_0\left\|\mathbf{h}_{\text{RD}}\right\|^2 d_{\text{RD}}^{-\alpha} - 2^{R_s}}{1+\eta\rho_0\left\|\mathbf{h}_{\text{SR}}\right\|^2 d_{\text{SR}}^{-\alpha} - 2^{R_s}}\right)^{1+\beta}\left(\frac{1-\eta}{\eta}\right)^{1-\beta} = 1. \tag{38}$$

Denote the maximum achievable secrecy rate for any given η by $\tilde{T}_s\left(\eta, \mathbf{h}\right) = \frac{1}{2}\tilde{R}_s\left(\eta, \mathbf{h}\right)$. Thus, the maximum secrecy rate for given main channel states is

$$\mathcal{T}_s^*(\mathbf{h}) = \tilde{T}_s\left(\eta, \mathbf{h}\right)|_{\eta=\eta^*(\mathbf{h})} = \begin{cases} \frac{1}{2}\mathcal{R}_s^*(\mathbf{h}), & \mathbf{h} \in \mathcal{H}, \\ 0, & \mathbf{h} \notin \mathcal{H}, \end{cases} \tag{39}$$

where the transmission set is

$$\mathcal{H} = \left\{\mathbf{h}\left|1-\exp\left[-\phi\left(\left(d_{\text{SR}}^{\alpha}/\left\|\mathbf{h}_{\text{SR}}\right\|^2\right)^{\beta} + \left(d_{\text{RD}}^{\alpha}/\left\|\mathbf{h}_{\text{RD}}\right\|^2\right)^{\beta}\right)\right] < \varepsilon\right\}. \tag{40}$$

Remark 1: The above proposition presents the optimal solution to problem **P1** in a more generalized scenario where both eavesdroppers and the relay are equipped with multiple antennas. Therefore, in the following simulations we use the results in Proposition 2 to validate the optimization of our proposed scheme and evaluate the secrecy performance of the relay system. Note that the two corollaries given in Section III can also be generalized by replacing $|h_{\text{SR}}|^2$ and $|h_{\text{RD}}|^2$ with $\|\mathbf{h}_{\text{SR}}\|^2$ and $\|\mathbf{h}_{\text{RD}}\|^2$, respectively.

V. NUMERICAL RESULTS

In this section, we present numerical results to evaluate the secrecy performance of the relay transmission. As aforementioned, when the rate of transmitted codeword for each phase is maximized, i.e., $R_{t,i} = C_{\text{M},i}$ $(i = 1, 2)$, the optimization problem **P1** is equivalent to the power allocation problem **P3**. In this case, the transmission strategy is only determined by η and the optimal transmission scheme is simplified into the optimal power allocation scheme. In the following simulations, unless otherwise noted, the distances between legitimate nodes is fixed as $d_{\text{SR}} = 6$ m and $d_{\text{RD}} = 8$ m, and the secrecy-outage-probability constraint is set as $\varepsilon = 0.2$.

First of all, we run Monte Carlo simulations to validate the theoretical result given in (36). We consider a two dimensional circular area with radius 2000 m. The source is located at the origin (the center of the circle) of the polar coordinate and the relay is located at $(d_{\text{SR}}, 0)$. Eavesdroppers are distributed according to the PPP with $\lambda_{\text{E}} = 10^{-3}$ units/m^2. The total transmit SNR is $\rho_0 = 30$ dB and the power allocation parameter is preset as $\eta = 0.5$. Other simulation settings are $\|\mathbf{h}_{\text{SR}}\|^2 = \|\mathbf{h}_{\text{RD}}\|^2 = 2$ and $\alpha = 3$. Fig. 2 plots the

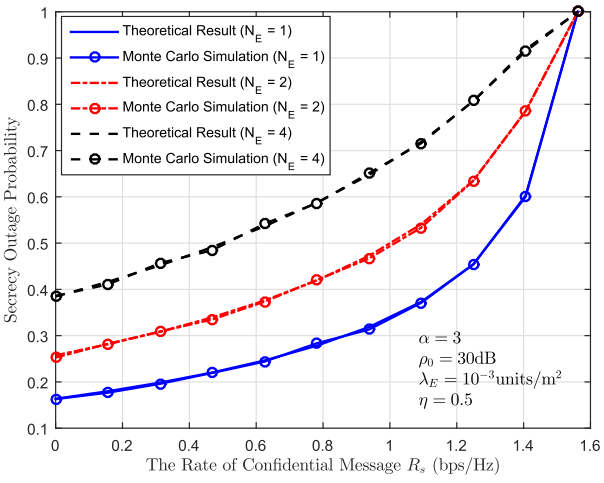

FIGURE 2. Monte Carlo simulation results and the theoretical results for secrecy outage probability.

secrecy outage probability versus the rate of the confidential message. One can see that the theoretical results agree with the simulation results well, which validates our mathematical analysis. Hence, we only use the theoretical expression (36) in the following simulations without showing the Monte Carlo results. Note that when $R_s = 0$, the outage probability is not equal to zero since the scenario where $C_{\mathrm{M}} - C_{\mathrm{E}} < 0$ is also considered, which represents the probability of losing secrecy connectivity.

The optimality of $\eta^*(\mathbf{h})$ is validated in the following numerical results shown in Fig. 3, where the main channel gains are given as $\|\mathbf{h}_{\mathrm{SR}}\|^2 = \|\mathbf{h}_{\mathrm{RD}}\|^2 = 2$ and each eavesdropper is equipped with single antenna. Under this scenario, the R − D link suffers from severer propagation loss compared with the S − R link, due to the longer transmission distance. Fig. 3(a) plots the maximum achievable secrecy rate versus the power allocation parameter for different path-loss exponent. The lines are calculated by solving the equation $\tilde{P}_{\mathrm{out}} = \varepsilon$ with given η and the star markers represent the optimal solutions $\big(\eta^*(\mathbf{h}), \mathcal{T}_s^*(\mathbf{h})\big)$ according to Proposition 2. One can see that each star marker reaches the highest point of its corresponding line, which validates the optimality of the proposed scheme. Moreover, we find that larger path-loss exponent leads to lower achievable secrecy rate. This result shows that although the signals received at legitimate devices and eavesdroppers both suffer severer path loss, the capacity loss of the main link still plays a leading role in the secure transmission. It can also be observed that with the increase of path-loss exponent, more power is allocated to the weaker link (R − D link). This implicitly shows that the secrecy rate in the RF relay network is also bottlenecked by the weaker link's capacity.

Fig. 3(b) depicts the maximum achievable secrecy rate versus the power allocation parameter for different densities of eavesdropper. As illustrated in Fig. 3(b), with the rise of η, $\tilde{T}_s(\eta, \mathbf{h})$ first increases and then decreases, reaching the highest point at the star marker. For any fixed η, $\tilde{T}_s(\eta, \mathbf{h})$ decreases with the increase of λ_{E}, due to the higher probability for the existence of a near eavesdropper. It is also observed that with the rise of λ_{E}, the effect of power allocation is less obvious. This is because the achievable secrecy rate is low with dense eavesdroppers and only simple power allocation cannot further improve the secrecy rate.

Fig. 3(c) shows the maximum achievable secrecy rate versus the power allocation parameter for different total transmit SNRs. Similarly, one can easily validate the optimality of our proposed scheme from this figure. Moreover, with the rise of ρ_0, the maximum secrecy rate, i.e., $\mathcal{T}_s^*(\mathbf{h})$, keeps increasing and finally converges to a constant, shown as the horizontal dark line calculated by (26). In addition, when $\rho_0 \to \infty$, the curve tends to a straight line, which validates our analysis in Corollary 2 that $\mathcal{T}_s^*(\mathbf{h})$ does not depend on power allocation parameter when the transmit SNR is high enough.

Note that the aforementioned maximum achievable secrecy rate $\tilde{T}_s(\eta, \mathbf{h})$ is the instantaneous rate for given channel gains $\mathbf{h}$. To obtain an ergodic performance, we introduce the concept of average achievable secrecy throughput $T_s^{ave}(\eta)$, given as

$$T_s^{ave}(\eta) = \mathcal{P}_t \int_{\mathbf{h}\in\mathcal{H}} \tilde{T}_s(\eta, \mathbf{h})\, d\mathbf{h}, \tag{41}$$

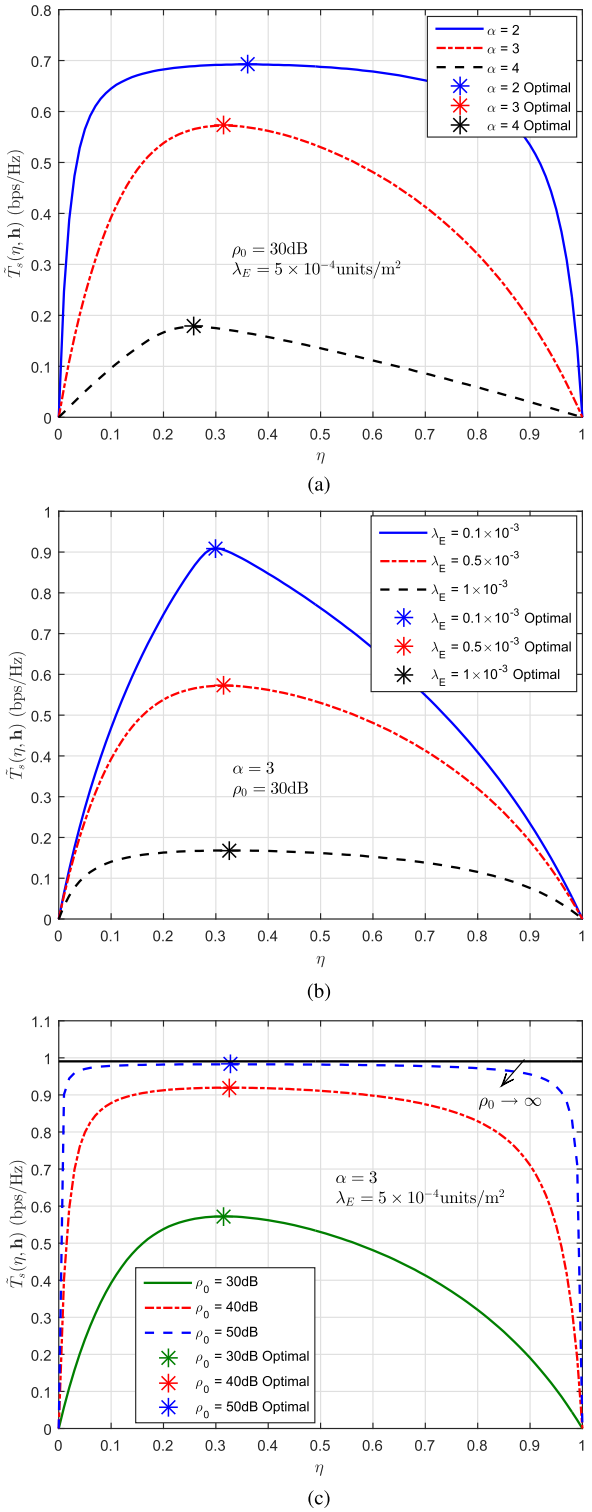

FIGURE 3. Maximum achievable secrecy rate as a function of power allocation parameter with different simulation settings. (a) Different path-loss exponents. (b) Different densities of eavesdropper. (c) Different total transmit SNRs.

where $\mathcal{P}_t$ is the transmission probability. Note that the transmission set given by (40) is not a function of η. Thus, we have $\mathcal{P}_t = \Pr\{\mathbf{h} \in \mathcal{H}\}$ for all power allocation schemes. Moreover, it is easy to show that the distributions of main channel gains are $\|\mathbf{h}_{\mathrm{SR}}\|^2 \sim \Gamma(N_{\mathrm{R}}, 1)$ and $\|\mathbf{h}_{\mathrm{RD}}\|^2 \sim \Gamma(N_{\mathrm{R}}, 1)$. However, it is difficult to derive the closed-form expression for $T_s^{ave}(\eta)$ since the expressions for $\mathcal{P}_t$ and $\tilde{T}_s(\eta, \mathbf{h})$ are complicated. Thus, we only provide numerical results of $T_s^{ave}(\eta)$ in the text below.

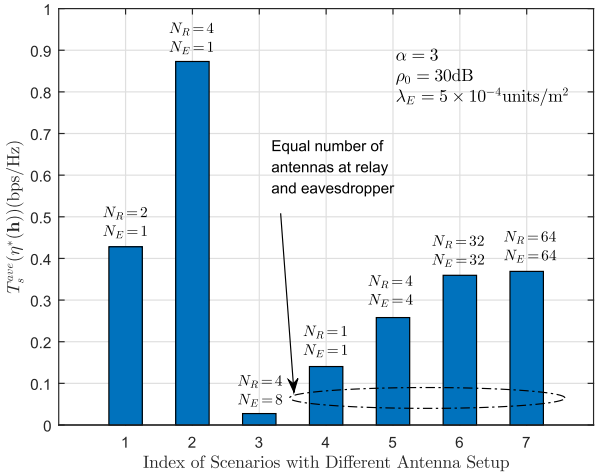

FIGURE 4. Average achievable secrecy throughput with optimal power allocation for different antenna setups, where $\alpha = 3$, $\rho_0 = 30$ dB and $\lambda_E = 5 \times 10^{-4}$ units/m^2.

Fig. 4 shows the average achievable secrecy throughput with optimal power allocation $\eta^*(\mathbf{h})$ under different antenna setups. It is observed that when $N_{\mathrm{R}} > N_{\mathrm{E}}$ the secrecy throughput can be enhanced a lot while when $N_{\mathrm{R}} < N_{\mathrm{E}}$ the secrecy requirement is hard to guarantee. This is expected since more antennas can bring higher received SNR. Thus, the secrecy level of the network is determined by the relative amount of antennas at legitimate devices and eavesdroppers. A more meaningful scenario where the relay and the eavesdropper have the same number of antennas is also illustrated in Fig. 4. We can see that with the increasing number of antennas, although the received SNRs at both the legitimate devices and eavesdroppers get improved, the average secrecy throughput can still rise and eventually flatten out. Therefore, equipping the relay with multiple antennas is always beneficial even if the eavesdropper has the same number of antennas.

Fig. 5 plots the average achievable secrecy throughput versus the total transmit SNR with different power allocation schemes. Besides the optimal power allocation $\eta^{\mathrm{opt}} = \eta^*(\mathbf{h})$, we introduce two other allocation schemes as baseline algorithms. One is the equal power allocation scheme with $\eta^{\mathrm{eql}} = 0.5$. The other is the capacity balancing allocation scheme with $\eta^{\mathrm{bal}} = \|\mathbf{h}_{\mathrm{RD}}\|^2 d_{\mathrm{RD}}^{-\alpha} / \left(\|\mathbf{h}_{\mathrm{SR}}\|^2 d_{\mathrm{SR}}^{-\alpha} + \|\mathbf{h}_{\mathrm{RD}}\|^2 d_{\mathrm{RD}}^{-\alpha}\right)$, which makes the capacities of S$-$R link and R$-$D link equal. As illustrated in Fig. 5, the optimal scheme outperforms the two baseline schemes, especially the equal power allocation scheme. Moreover, the performance difference between the

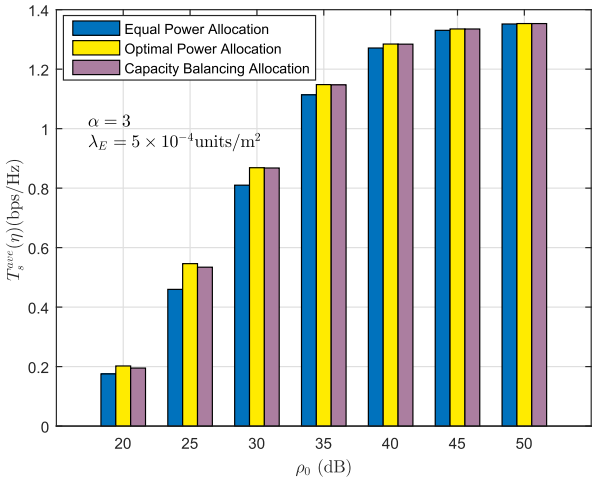

FIGURE 5. Average achievable secrecy throughput as a function of total transmit SNR for different power allocation schemes, where $N_{\mathrm{R}} = 4$ and $N_{\mathrm{E}} = 1$.

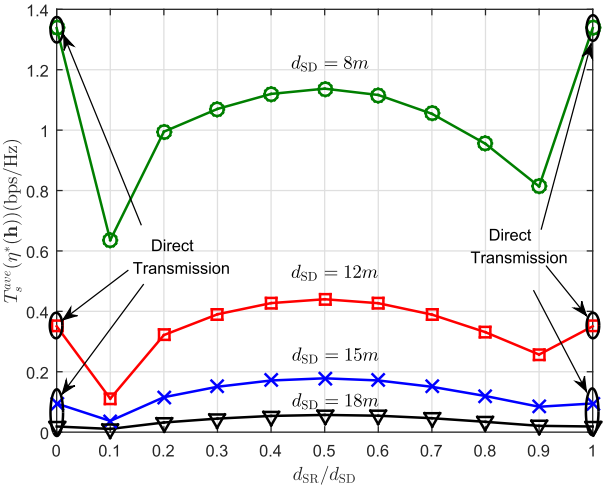

FIGURE 6. Average achievable secrecy throughput as a function of the location of relay, where the source, relay, and the destination lie on a straight line. Other simulation settings are $\alpha = 3$, $\varepsilon = 0.2$, $\rho_0 = 40$ dB, and $\lambda_E = 5 \times 10^{-4}$ units/m^2.

optimal scheme and the capacity balancing scheme is small, which indicates that the optimal scheme also tends to equalize the capacities of two main links, as discussed in Corollary 1 for the special case $\alpha = 2$. Thus, we can simply use the suboptimal solution η^{bal} instead of η^{opt} without obvious performance loss. In addition, with the rise of ρ_0, the performance differences among the three schemes are negligible, which validates the analysis in Corollary 2.

Finally, we compare the secrecy performance of relay transmission with direct transmission, where the optimal power allocation $\eta^*(\mathbf{h})$ is adopted for relay transmission. In order to make a fair comparison which is independent of the number of antennas, we assume a single-antenna relay and single-antenna eavesdroppers in the following simulations. For direct transmission, similar to Lemma 1, it can also be proved that all the transmit power should be utilized.

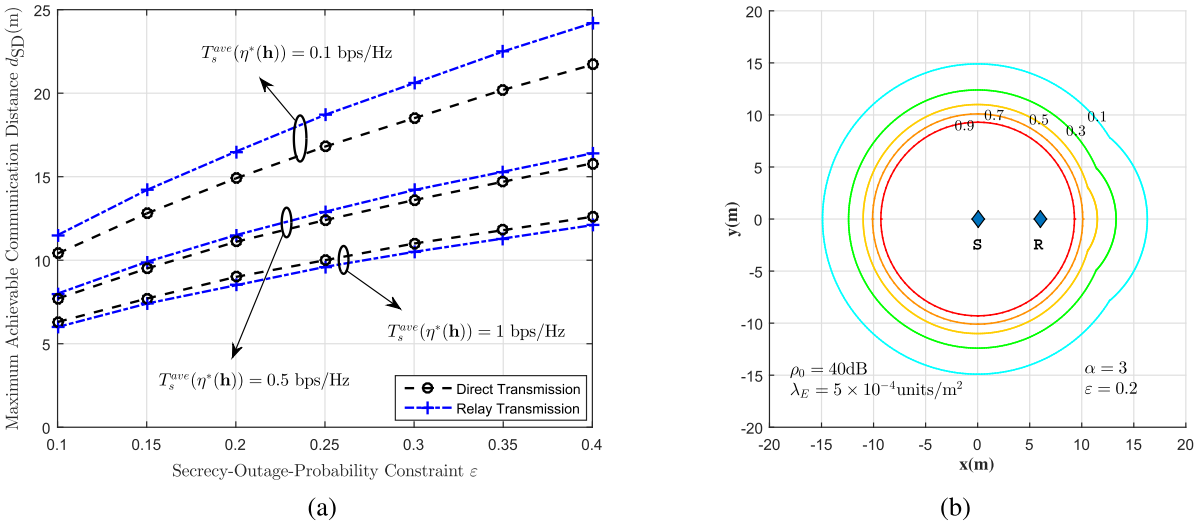

FIGURE 7. Maximum achievable communication distance d_{SD} for given required throughput $T_s^{ave}(\eta^*(\mathbf{h}))$. (a) Comparisons between relay transmission and direct transmission, where $\alpha = 3$, $\varepsilon = 0.2$, $\rho_0 = 40$ dB, and $\lambda_E = 5 \times 10^{-4}$ units/m^2. The relay is located at the midpoint between the source and the destination. (b) Secure coverage range within two-hop transmission where the locations of the source and relay are fixed. All points on the same contour line achieve the same secrecy throughput $T_s^{ave}(\eta^*(\mathbf{h}))$.

Thus, the secrecy outage probability can be derived as

$$P_{\text{out}}^{\text{direct}} = 1 - \exp\left[-\phi\left(\frac{\rho_0 2^{R_s}}{1 + \rho_0 |h_{\text{SD}}|^2 d_{\text{SD}}^{-\alpha} - 2^{R_s}}\right)^{\beta}\right], \tag{42}$$

where ϕ and β are given in (34). Accordingly, for given main channel gain $\mathbf{h} = |h_{\text{SD}}|^2$, the maximum achievable rate of confidential message, denoted as $\mathcal{R}_s^*(\mathbf{h})$, is the root of $P_{\text{out}}^{\text{direct}} = \varepsilon$. Note that for direct transmission, the maximum secrecy rate $\mathcal{T}_s^*(\mathbf{h})$ is the same as $\mathcal{R}_s^*(\mathbf{h})$ since there is only one transmission phase. With some abuse of notation, we still use $T_s^{ave}(\eta)$ to denote the average achievable secrecy throughput for direct transmission although it is actually independent of η. The expression of $T_s^{ave}(\eta)$ for direct transmission is given by

$$T_s^{ave}(\eta) = \mathcal{P}_t \int_{\mathbf{h}\in\mathcal{H}} \mathcal{T}_s^*(\mathbf{h})\, d\mathbf{h}, \tag{43}$$

where $\mathcal{P}_t = \Pr\{\mathbf{h} \in \mathcal{H}\}$ and the transmission set is now given by

$$\mathcal{H} = \left\{\mathbf{h} \,\middle|\, 1 - \exp\left[-\phi\left(d_{\text{SD}}^{\alpha}/\,|h_{\text{SD}}|^2\right)^{\beta}\right] < \varepsilon\right\}.$$

Fig. 6 depicts the average achievable secrecy throughput as a function of relay's location, where the source, relay, and the destination lie on a straight line. It is observed that the optimal location for relay is the midpoint between the source and the destination. The points with $d_{\text{SR}}/d_{\text{SD}} = 0$ or $d_{\text{SR}}/d_{\text{SD}} = 1$ actually describe the performance of direct transmission. As illustrated in Fig. 6, when the communication distance d_{SD} is short (e.g., $d_{\text{SD}} = 8$ m), it is not wise to adopt relay transmission. When the communication distance is long, relay transmission can significantly increase the secrecy throughput. This is because the retransmission of relay provides eavesdroppers additional chance to intercept the confidential message. Thus, only when the propagation loss of direct link (S − D link) is large can relay transmission improve the secrecy throughput.

Fig. 7(a) makes a comparison of maximum achievable communication distance between relay transmission and direct transmission. Inspired by the results in Fig. 6, the relay is always placed at the midpoint between the source and the destination, namely, $d_{\text{SR}} = d_{\text{RD}} = \frac{1}{2}d_{\text{SD}}$. It is observed that in some cases relay transmission can enhance the communication distance but in some cases it cannot. This is because the high secrecy throughput limits the achievable communication distance. With such short distance it is unnecessary to employ a relay for message retransmission, which gives eavesdroppers additional opportunity to intercept the confidential message. Hence, relay transmission is more suitable for long-distance communication.

Fig. 7(b) plots the secure coverage area in a two-dimensional plane where the locations of the source and the relay are fixed. The value on a particular contour line represents the average achievable secrecy throughput that can be achieved by all the points on this line. Note that the final coverage area is formed by merging the coverage of direct transmission and relay transmission. Similar to the observations in Fig. 7(a), when the required secrecy throughput is high (e.g., $T_s^{ave}(\eta^*(\mathbf{h})) = 0.9$ or 0.7 bps/Hz), relay transmission cannot enlarge the secure coverage. However, when the required throughput is low, it can provide a larger coverage area. As discussed in [30], if we consider the secrecy connectivity problem that only requires $T_s^{ave}(\eta^*(\mathbf{h})) > 0$, relay transmission has the capability to extend the coverage

area within which the secrecy connectivity is guaranteed. Hence, relay transmission is helpful if we want to make the insecure communication secure.

VI. CONCLUSIONS

With the development of the upcoming 5G communication system, the concept of IoT is attracting more and more attention. 5G technologies hold the potential to enable a seamless connection among different kinds of things. However, the heterogeneous environment in 5G systems make the IoT communications vulnerable to eavesdropping attack. In this paper, we studied the secure relay communications in IoT networks against randomly distributed eavesdroppers. We first considered a simple scenario where all the devices including eavesdroppers are equipped with the single antenna. The secrecy outage probability under this scenario was derived, based on which we formulated a secrecy-rate-maximization problem. The optimal power allocation and codeword rates were derived. We then studied this optimization problem in a more generic scenario where the relay and eavesdroppers are equipped with multiple antennas. We obtained the expression for the secrecy outage probability which is similar to the expression derived for the single antenna system. Due to the similarity, we directly utilized the previous results to obtain a generalized optimal scheme. By using numerical simulations, we validated the optimality of the proposed scheme and found that the optimal scheme can be replaced by a simple suboptimal one with only a little performance loss. Moreover, it was shown by numerical results that equipping the relay with multiple antennas is always beneficial even if the eavesdropper has the same number of antennas. Finally, by comparing the performance of relay transmission with direct transmission, we found that the appropriate introduction of relay transmission can enhance the secrecy throughput and extend the secure coverage area.

REFERENCES

[1] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. T. Mouftah, "The Internet of Things," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 30–31, Nov. 2011.
[2] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. FIT*, Islamabad, Pakistan, Dec. 2012, pp. 257–260.
[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. 2015.
[4] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: A QoE-oriented framework," *IEEE Netw.*, vol. 30, no. 1, pp. 52–57, Jan./Feb. 2016.
[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[6] M. Weiser, "The computer for the 21st century," *Sci. Amer.*, vol. 265, no. 3, pp. 94–104, 1991.
[7] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.
[8] Q. Du, H. Song, Q. Xu, P. Ren, and L. Sun, "Interference-controlled D2D routing aided by knowledge extraction at cellular infrastructure towards ubiquitous CPS," *Pers. Ubiquitous Comput.*, vol. 19, no. 7, pp. 1033–1043, Oct. 2015.
[9] P. Ren, Y. Wang, and Q. Du, "CAD-MAC: A channel-aggregation diversity based MAC protocol for spectrum and energy efficient cognitive ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 2, pp. 237–250, Feb. 2014.
[10] S. LoongKeoh, 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.
[11] J. Granjal, E. Monteiro, and J. Sá 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.
[12] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[13] 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.
[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. PP, no. 99, pp. 1–13, Dec. 2015.
[15] 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, Aug. 2014.
[16] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[17] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[18] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[20] 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.
[21] 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, May 2016.
[22] 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.
[23] 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.
[24] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.
[25] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[26] 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.
[27] T. X. Zheng, H. M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.
[28] S. Vuppala, W. Liu, G. Abreu, and T. Ratnarajah, "Secrecy outage of Nakagami-m MISO channels with randomly located receivers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 6295–6299.
[29] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.
[30] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014.
[31] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.
[32] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[33] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.
[34] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "Two tier secure routing protocol for heterogeneous sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3395–3401, Sep. 2007.
[35] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.
[36] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[37] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.
[38] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

QIAN XU received the B.S. degree from Xi'an Jiaotong University, China, in 2014, where she is currently pursuing the Ph.D. degree with the Department of Information and Communications Engineering. Her 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, 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 in 2012. Since 2012, he has been an Assistant Professor with the Department of Electrical and Computer Engineering, West Virginia University Institute of Technology. His research interests are focused on 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, China, and the Ph.D. degree from Texas A&M University, TX, USA. He is currently an Assistant Professor with the Information and Communications Engineering Department, Xi'an Jiaotong University. His research interests include mobile wireless communications and networking with emphasis on mobile multicast, statistical QoS provisioning, and cognitive radio networks.