Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5012096, 8 pages
https://doi.org/10.1155/2018/5012096

Research Article

Energy-Efficient Transmission Based on Direct Links: Toward Secure Cooperative Internet of Things

Xiaohui Shang, Aijun Liu, Yida Wang, Qing Xie, and Yong Wang

Department of Satellite Communications, Army Engineering University of PLA, Nanjing 210014, China

Correspondence should be addressed to Xiaohui Shang; shangxiaohui1214@126.com

Received 17 September 2018; Accepted 4 December 2018; Published 17 December 2018

Guest Editor: Dajiang Chen

In this paper, the secure uplink transmission scenario in Internet of Things (IoT) applications is investigated, where one of multiple sensors communicates with the controller aided by the cooperative relay. Firstly, by considering the direct link, an energy-efficient transmission scheme (EET) is proposed, which can be suitable for the resource-constrained devices and applications in IoT communication. Moreover, the secrecy outage probability (SOP) and secure energy efficiency (SEE) of different transmission strategies are derived, which contributes to the design of energy-efficient secure transmission. Finally, simulation results demonstrate that EET outperforms other transmission protocols in terms of SEE in most situations. To improve the secrecy performance and energy efficiency of the IoT deployment, EET can be adopted as an effective additional strategy in practical applications.

1. Introduction

The Internet of Things (IoT), serving as an important architecture in the fifth-generation (5G) mobile communication systems, has drawn dramatic interest all over the world [1–3]. However, most of IoT terminal devices are resource-constrained commonly, which causes low computing power and energy storage capacity. Generally, it is necessary for IoT applications to operate at low power. Meanwhile, since most devices are battery-powered sensor nodes that cannot be replaced for some reasons, such as being embedded in a human body, these sensors are required to work for a long time without human intervention [4]. Consequently, energy efficiency is worthy of concern in the IoT system especially.

Cooperative transmission in wireless communications has been considered as a promising solution in order to economize the power of transmitter, improve throughput, and enhance the reliability of communications [5]. Because of limited resources of IoT devices, the employment of relay transmission is of utmost importance for IoT to cope with the issue of energy efficiency. Traditional cooperative protocols have been studied deeply by many researchers [6, 7], such as amplify-and-forward (AF) and decode-and-forward (DF), in which DF can be further subdivided into fixed DF and selective DF [8], as well as cooperative jamming (CJ) [9, 10]. In particular, for the CJ scheme, the relay does not forward confidential information but emits interference signals (also known as artificial noise) to interfere with the eavesdropper. It is worth noting that a common problem in [6–10] is that the direct link between the source and the target has been unexploited.

On the other hand, it is also necessary to consider the security and privacy issues for IoT. Obviously, not all devices connected via the IoT are able to access the network data. Moreover, the wireless communication channel is open, which may also lead to the eavesdropping risk caused by unauthorized users. In general, security has always been regarded as a problem that needs to be solved by high-layer computing methods. However, physical layer security (PLS), which is an emerging method to ensure the security of wireless communication, has become an effective supplement to existing solutions. In terms of wireless PLS, the basic idea is to make use of the characteristics of wireless channels to transmit information reliably from the source to the intended receiver as well as to ensure the confidentiality of the information, that is, not to be intercepted or eavesdropped [11]. In recent years, PLS techniques have been widely explored to ensure security of future wireless communications, as it could

provide the security of new network architectures such as the IoT. Unfortunately, energy efficiency of PLS has not aroused sufficient attention in the cooperative relay networks and IoT scenario.

The measurements of PLS are generally related to the availability of channel state information (CSI) for source. When the source well knows global CSI, the confidential information will not leak to the eavesdropper via the adaption of secure coding rate; thus the so-called perfect secrecy can be realized [12]. In this case, the measurement of security is secrecy capacity [13–15]. However, the hypothesis of knowing global CSI is too strong to be realized easily, since it may require the intended destination to report its information of the position; in addition, eavesdroppers collaboration to give feedback on CSI to the source is also required. Obviously, above requirement may be not suitable for the IoT devices because it will lead to higher cost and power consumption as well as more serious latency, which are unacceptable to the effective deployment of massive IoT. Therefore, a more realistic way of applying the probabilistic view is proposed, in which it was assumed that only part of the CSI of the legitimate channel is known and communication operates at a fixed secure transmission rate. At this point, security is denoted by the secrecy outage probability (SOP) [16].

Inspired by previous work, this paper focuses on secure uplink transmission scenario in IoT applications, in which one of multiple sensors in the localized group transmits collected data to a controller aided by the cooperative relay when considering the presence of a passive eavesdropper. A more practical scenario worthy of concern is that there exists a direct link between controller and sensor. With the optimal performance and controllable cost, MRC technique is usually utilized by controller to process the received signal [17]. The main contributions of this work are listed below.

(1) By making use of the advantages of both direct and relay links, we propose a novel energy-efficient secure transmission strategy based on the CSI of the legitimate link, that is, energy-efficient transmission (EET), by which the best path is selected (direct or cooperative transmission), to cope with implementation limits of the IoT devices. Since the source has known about CSI of main links, then the direct or cooperative transmission could be performed based on the above information, which contributes to decreasing energy consumption and improving secure energy efficiency (SEE).

(2) We obtain the closed-form expressions of SOP and SEE, which will be helpful to secure the applications of cooperative IoT. In order to show the effectiveness of our new strategy, we further compare the secrecy performance of different transmission schemes such as EET, DF, AF, and CJ as well as direct transmission (DT).

(3) Our results demonstrate that the proposed EET is superior to other transmission protocols in many cases when considering SEE. To improve the secrecy performance and energy efficiency of the IoT deployment with the help of cooperative relay, EET can be regarded as an effective additional strategy in practical applications.

This paper is organized as follows. In Section 2, we present the system model and our EET design. The exact SOP and SEE of proposed strategy and DT as well as other conventional cooperative protocols are derived in Section 3. Then the secrecy performance of above transmission strategies is shown by simulation results in Section 4. Finally, conclusions of this paper are drawn in Section 5.

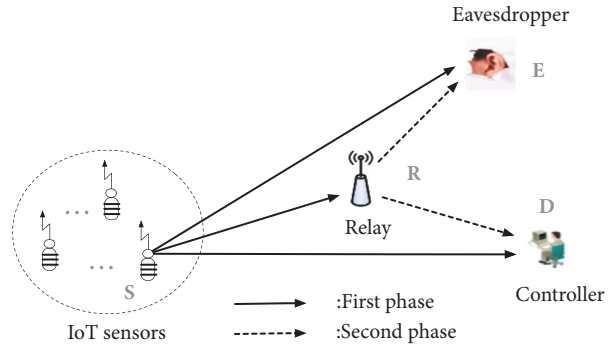


Figure 1: System model.

2. System Model and EET Design

2.1. System Model and Notation. Figure 1 shows the communication model of a single-antenna IoT device in the presence of wireless cooperative links, where one of multiple IoT sensors (S) transmits the detected data to a desired controller (D) aided by a relay (R) when considering the presence of a passive eavesdropper (E). This model can use the direct link to improve the reliability of the system [18]. The helper node, which is adopted as a relay or as a jammer, is equipped with a single antenna used for data transmission and reception in a half-duplex manner. The signal received by any node $j \in (\mathrm{R}, \mathrm{D}, \mathrm{E})$ from the transmitting terminal of $i \in (\mathrm{S}, \mathrm{R})$, $i \neq j$, is expressed as

$$y_{ij} = \sqrt{k_{ij} P_i} h_{ij} x_i + n_{ij} \tag{1}$$

where we denote k_{ij} as the path-loss between nodes i and j, P_i as the transmit power of i, x_i as the useful data signal, and n_{ij} as the zero-mean and variance $N_0/2$ additive white Gaussian noise (AWGN). Furthermore, we denote h_{ij} as the channel coefficient between nodes i and j, which exhibits Rayleigh flat-fading that remains constant for the duration of one transmission block time and varies in different block independently. Assuming that all wireless channels are independent and distributed as exponential random variables, the receiver can fully obtain the CSI of legitimate link [19]. Consequently, the intended end can obtain CSI of the main links. It is reasonable due to the fact that R and D can get available channel parameters of the main link with the assistance of channel estimation; then D is able to attain accurate CSI through cooperative relays [20]. The path-loss is $k_{ij} = G\lambda^2 / 4\pi^2 d_{ij}^{v} M_l N_f$, where G is the total antenna gain, λ denotes the wavelength, d_{ij} represents the distance between nodes i and j, v is the path-loss exponent, M_l denotes the link margin, and N_f is the noise at the intended receiver. Next, the instantaneous signal-to-noise ratio (SNR) at any $i-j$ channel can be expressed as $\gamma_{ij} = |h_{ij}|^2 \overline{\gamma}_{ij}$, where $\overline{\gamma}_{ij} = k_{ij} P_i / N$

represents the average SNR, $N = N_0B$ is defined as the noise power and B denotes the channel bandwidth, and any γ_{ij} is exponentially distributed according to the probability density function (PDF) $f_{\gamma_{ij}} = (1/\gamma_{ij})e^{-\gamma_{ij}/\overline{\gamma}_{ij}}$ for $\gamma_{ij} > 0$.

In line with [13], the achievable secrecy rate of source-destination (C_S) is given by

$$C_S = [C_L - C_E]^+ \tag{2}$$

$$C_L = \frac{1}{2}\log(1+\gamma_L) \tag{3}$$

$$C_E = \frac{1}{2}\log(1+\gamma_E) \tag{4}$$

where C_L denotes the capacity of the legitimate link and C_E represents the capacity of the eavesdropper link, γ_L and γ_E are the end-to-end instantaneous SNR of the legitimate and eavesdropper links, respectively, and $[x]^+ \triangleq \max\{0, x\}$.

2.2. EET Design. For the EET strategy, the selection criterion is that the sensor determines the most secure method (the direct or cooperative transmission) to be transmited to D with the aid of the available CSI. Different from the conventional cooperative protocols, since we consider both the direct and relay links simultaneously, the proposed EET can achieve better security performance. Then, in ETT, the capacity of the legitimate channel can be described by

$$C_L^{ETT} = \frac{1}{2}\max\left\{\overbrace{\log_2(1+2\gamma_{SD})}^{C_{L_{dir}}}, \underbrace{\min\{\log_2(1+\gamma_{SR}), \log_2(1+\gamma_{SD}+\gamma_{RD})\}}_{C_{L_{coop}}}\right\} \tag{5}$$

It is worth noting that the term 1/2 in (5) denotes the half duplexing cost. Then, the corresponding secrecy capacity of EET is expressed as $C_S^{EET} = [C_L^{EET} - C_E^{EET}]^+$, where C_E^{EET} is obtained from (5) by replacing D by E.

3. Secrecy Performance Analysis

We resort to the SOP and SEE to analyze the secure performance for EET as well as DT, DF, AF, and CJ protocols in this section.

3.1. Secrecy Outage Probability. In the following, the SOP can be formulated as

$$P_{out}^{sch} = \Pr\left\{C_S^{sch} < R_S\right\} = \Pr\left\{C_L^{sch} - C_E^{sch} < R_S\right\} \tag{6}$$

where $sch \in$ EET, DT, DF, AF, and CJ.

3.1.1. Derivation for EET. In general, the relay R is located in the middle position of the source S and the controller D, and we make the following considerations to (5): S (or the relay R) transmits data when $\gamma_{SD} \geq \gamma_{SR}$ (or when $\gamma_{SR} > \gamma_{SD}$). Based on the fundamental principle of EET, SOP can be expressed by

$$P_{out}^{EET} = \overbrace{\Pr\left\{C_{L_{dir}}^{EET} - C_{E_{dir}}^{EET} < 2R_S \cap \gamma_{SD} \geq \gamma_{SR}\right\}}^{p_{dir}} + \underbrace{\Pr\left\{C_{L_{coop}}^{EET} - C_{E_{coop}}^{EET} < 2R_S \cap \gamma_{SR} > \gamma_{SD}\right\}}_{P_{coop}} \tag{7}$$

where p_{dir} is obtained as

$$\begin{aligned} p_{dir} &= \Pr\left\{\left(\frac{1+2\gamma_{SD}}{1+2\gamma_{SE}}\right) < 2^{2R_S} \cap \gamma_{SD} \geq \gamma_{SR}\right\} \\ &= \Pr\left\{\gamma_{SE} > \Delta \cap \gamma_{SD} \geq \gamma_{SR}\right\} \end{aligned} \tag{8}$$

where $\Delta \triangleq (2^{-2R_S}(1+2\gamma_{SD})-1)/2$. For the Rayleigh fading, γ_{SD} and γ_{SR} are random variables that follow the exponential distribution, and their PDFs have been given above; thus,

$$\begin{aligned} p_{dir} &= \int_0^{\infty}\int_0^{\gamma_{SD}}\int_{\Delta} f_{\gamma_{SD}} f_{\gamma_{SR}} f_{\gamma_{SE}} d\gamma_{SE} d\gamma_{SR} d\gamma_{SD} \\ &= \frac{2^{4R_S}\overline{\gamma_{SD}}\,\overline{\gamma_{SE}}\exp\left(\left(1-2^{-2R_S}\right)/2\overline{\gamma_{SE}}\right)}{\left(\overline{\gamma_{SD}}+2^{R_S}\overline{\gamma_{SE}}\right)\left[\overline{\gamma_{SD}}\,\overline{\gamma_{SR}}+2^{2R_S}\overline{\gamma_{SE}}\left(\overline{\gamma_{SD}}+\overline{\gamma_{SR}}\right)\right]} \end{aligned} \tag{9}$$

When the sensor decides to utilize the relay, we consider that $\gamma_D = \gamma_{SD} + \gamma_{RD}$ and $\gamma_E = \gamma_{SE} + \gamma_{RE}$ are the SNRs at D and E, respectively, and their PDFs are expressed by $g_{\gamma_i} = g_{\gamma_{Si}+\gamma_{Ri}} = (1/(\overline{\gamma_{Ri}} - \overline{\gamma_{Si}}))(e^{-\gamma_i/\overline{\gamma_{Ri}}} - e^{-\gamma_i/\overline{\gamma_{Si}}}), i \in \{D, E\}$. Then, the SOP yields in the following cases

$$\begin{aligned} p_{coop} &= \overbrace{\Pr\left\{\frac{1+\gamma_{SR}}{1+\gamma_E} < 2^{2R_S} \cap \gamma_{SR} < \gamma_D \cap \gamma_{SR} > \gamma_{SD}\right\}}^{p_1} \\ &\quad + \underbrace{\Pr\left\{\frac{1+\gamma_{SR}}{1+\gamma_E} < 2^{2R_S} \cap \gamma_{SR} \geq \gamma_D \cap \gamma_{SR} > \gamma_{SD}\right\}}_{p_2} \end{aligned} \tag{10}$$

To obtain p_1, we isolate γ_E and use the integral that $\int_{\gamma_{SD}}^{\gamma_D} f_{\gamma_{SR}} d\gamma_{SR} = \int_0^{\gamma_D} f_{\gamma_{SR}} d\gamma_{SR} - \int_0^{\gamma_{SD}} f_{\gamma_{SR}} d\gamma_{SR}$. Thus

$$\begin{aligned} p_1 &= \int_0^{\infty}\int_0^{\gamma_D}\int_{2^{-2R_S}(1+\gamma_{SR})-1}^{\infty} g_{\gamma_D} f_{\gamma_{SR}} g_{\gamma_E} d\gamma_E d\gamma_{SR} d\gamma_D \\ &\quad - \int_0^{\infty}\int_0^{\gamma_{SD}}\int_{2^{-2R_S}(1+\gamma_{SR})-1}^{\infty} g_{\gamma_{SD}} f_{\gamma_{SR}} g_{\gamma_E} d\gamma_E d\gamma_{SR} d\gamma_{SD} \end{aligned} \tag{11}$$

Similarly, p_2 is derevid as shown in (12). It is worth noting that both intersections, $\gamma_{SR} > \gamma_{SD}$ and $\gamma_{SR} \geq \gamma_D$, are not to be considered, for the sake of the fact that last intersection contains the first area.

$$p_2 = \int_0^{\infty}\int_{\gamma_D}^{\infty}\int_{2^{-2R_S}(1+\gamma_D)-1}^{\infty} g_{\gamma_D} f_{\gamma_{SR}} g_{\gamma_E} d\gamma_E d\gamma_{SR} d\gamma_D \tag{12}$$

From what has been discussed above, by combining the results of (11) and (12) and substituting back into (10), the SOP of the cooperative phase is obtained as

$$p_{coop} = \frac{2^{4R_S}\overline{\gamma_{SR}}\left(\overline{\gamma_{RD}} + \overline{\gamma_{SR}}\right)}{\overline{\gamma_{RE}} - \overline{\gamma_{SE}}}\left[A\left(\overline{\gamma_{RE}}\right) - A\left(\overline{\gamma_{SE}}\right)\right] \tag{13}$$

where $A(x) = e^{(1-2^{-2R_S})/x}x^3[\overline{\gamma_{SR}}\,\overline{\gamma_{RD}} + 2^{2R_S}x(\overline{\gamma_{SR}} + \overline{\gamma_{RD}})]^{-1}/(\overline{\gamma_{SR}}\,\overline{\gamma_{SD}} + 2^{2R_S}x(\overline{\gamma_{SR}} + \overline{\gamma_{SD}}))$.

Finally, the overall SOP of EET is derived after plugging (9) and (13) in (7).

3.1.2. Derivation for DT. In the direct transmission scheme, the sensor S always sends collected data to intended controller D according to a transmit rate R_S in the two phases, while the relay remains silent. Then we can obtain an exact expression for the SOP of DT in the following theorem.

Theorem 1.

$$P_{out}^{DT} = 1 - \frac{\overline{\gamma_{SD}}}{\overline{\gamma_{SD}} + 2^{2R_S}\overline{\gamma_{SE}}}\exp\left(\frac{1-2^{2R_S}}{2\overline{\gamma_{SD}}}\right) \tag{14}$$

Proof. See the appendix. □

3.1.3. Derivation for DF. Notably, different from EET, the relay R is always active in DF. The capacity of the main channel $C_L^{DF} = (1/2)\min[\log_2(1+\gamma_{SR}), \log_2(1+\gamma_{SD}+\gamma_{RD})]$, which obviously indicates a performance deficiency, as the transmission rate must meet the requirements of the S-R link. The SOP of DF can be formulated as [21]

$$\begin{aligned} P_{out}^{DF} &= \Pr\left\{\frac{1+\min\left(\gamma_{SR},\gamma_D\right)}{1+\gamma_E} < 2^{2R_S}\right\} \\ &= \frac{B\left(\overline{\gamma_{SR}},\overline{\gamma_{RE}}\right) - B\left(\overline{\gamma_{SR}},\overline{\gamma_{SE}}\right)}{\overline{\gamma_{RE}} - \overline{\gamma_{SE}}} \\ &\quad + \frac{\overline{\gamma_{SR}}B\left(\overline{\gamma_{SR}},\overline{\gamma_{SE}}\right)\left[D\left(\overline{\gamma_{SE}},\overline{\gamma_{SD}}\right) - D\left(\overline{\gamma_{SE}},\overline{\gamma_{RD}}\right)\right]}{2^{2R_S}\left(\overline{\gamma_{RE}} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_{RD}} - \overline{\gamma_{SD}}\right)} \\ &\quad - \frac{\overline{\gamma_{SR}}B\left(\overline{\gamma_{SR}},\overline{\gamma_{RE}}\right)\left[D\left(\overline{\gamma_{RE}},\overline{\gamma_{SD}}\right) - D\left(\overline{\gamma_{RE}},\overline{\gamma_{RD}}\right)\right]}{2^{2R_S}\left(\overline{\gamma_{RE}} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_{RD}} - \overline{\gamma_{SD}}\right)} \end{aligned} \tag{15}$$

where $B(x,y) \triangleq (y^2/(x2^{-2R_S}+y))\exp((1-2^{-2R_S})/y)$ and $D(x,y) \triangleq y\overline{\gamma_{SR}}/(x(y+\overline{\gamma_{SR}}) + y\overline{\gamma_{SR}}2^{-2R_S})$.

3.1.4. Derivation for AF. For AF scheme, similar to DF, the relay completes a total transmission in two stages; that is, the source broadcasts the signal, which is then amplified and transmitted to D by the relay R with a variable gain. The SOP of the AF scheme as found in [22] is reproduced as

$$\begin{aligned} P_{out}^{AF} &= \Pr\left\{\log_2\left(\frac{1+\gamma_{SD}+\gamma_{SR}\gamma_{RD}/\left(1+\gamma_{SR}+\gamma_{RD}\right)}{1+\gamma_{SE}+\gamma_{SR}\gamma_{RE}/\left(1+\gamma_{SR}+\gamma_{RE}\right)}\right)\right. \\ &\quad \left. < 2R_S\right\} \approx \frac{\overline{\gamma_D}\left[B\left(\overline{\gamma_D},\overline{\gamma_E}\right) - B\left(\overline{\gamma_D},\overline{\gamma_{SE}}\right)\right]}{\left(\overline{\gamma_E} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_D} - \overline{\gamma_{SD}}\right)} \\ &\quad - \frac{\overline{\gamma_{SD}}\left[B\left(\overline{\gamma_{SD}},\overline{\gamma_E}\right) - B\left(\overline{\gamma_{SD}},\overline{\gamma_{SE}}\right)\right]}{\left(\overline{\gamma_E} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_D} - \overline{\gamma_{SD}}\right)} \end{aligned} \tag{16}$$

3.1.5. Derivation for CJ. CJ can be adopted to interfere E by resorting to the relay to transmit interference signal, in which jamming is utilized in a cooperative manner to provide a secure communication link between the sensor and the desired controller to improve the secrecy performance of IoT uplink transmission. Thus, the SOP of CJ can be derived as [21]

$$\begin{aligned} P_{out}^{CJ} &= \Pr\left\{\log_2\left(\frac{1+\gamma_{SD}/\left(1+\gamma_{RD}\right)}{1+\gamma_{SE}/\left(1+\gamma_{RE}\right)}\right) < R_S\right\} \\ &= 1 + \frac{\exp\left(-c\right)}{\overline{\gamma_{RE}}\,\overline{\gamma_{RD}}l}\left(\frac{1}{g} - \frac{1}{h\lg^2}\right)F\left(g+gh\right) \\ &\quad + \frac{\exp\left(-c\right)}{\overline{\gamma_{RE}}\,\overline{\gamma_{RD}}l}\left[\left(\frac{1}{h\lg^2} + \frac{1}{hg}\right)F\left(\frac{1+h}{h\overline{\gamma_{RE}}}\right) - \frac{\overline{\gamma_{RE}}}{g}\right] \end{aligned} \tag{17}$$

where $c \triangleq (2^{R_S}-1)/\overline{\gamma_{SD}}$, $g \triangleq (1+\overline{\gamma_{RD}}c)/\overline{\gamma_{RD}}$, $h \triangleq \overline{\gamma_{SD}}/\overline{\gamma_{SE}}(1+\overline{\gamma_{SD}}c)$, $l \triangleq 1 - 1/\overline{\gamma_{RE}}gh$, $F(x) \triangleq \exp(x)E(x)$, and $E(x) \triangleq \int_x^\infty(\exp(-t)/t)dt$.

3.2. Secure Energy Efficiency. Actually, improvements of security often come at the cost of higher power. In consideration of sustainability, excessive pursuit of security performance is detrimental to IoT devices. In terms of IoT applications, secrecy communications should be conducted in an energy-efficient manner. Consequently, the SEE is used here as the best metric to measure physical layer security and energy efficiency at the same time. Mathematically, the SEE is expressed as

$$\eta_S = \frac{R_S\left(1 - P_{out}^{sch}\right)}{P_{total}^{sch}} \tag{18}$$

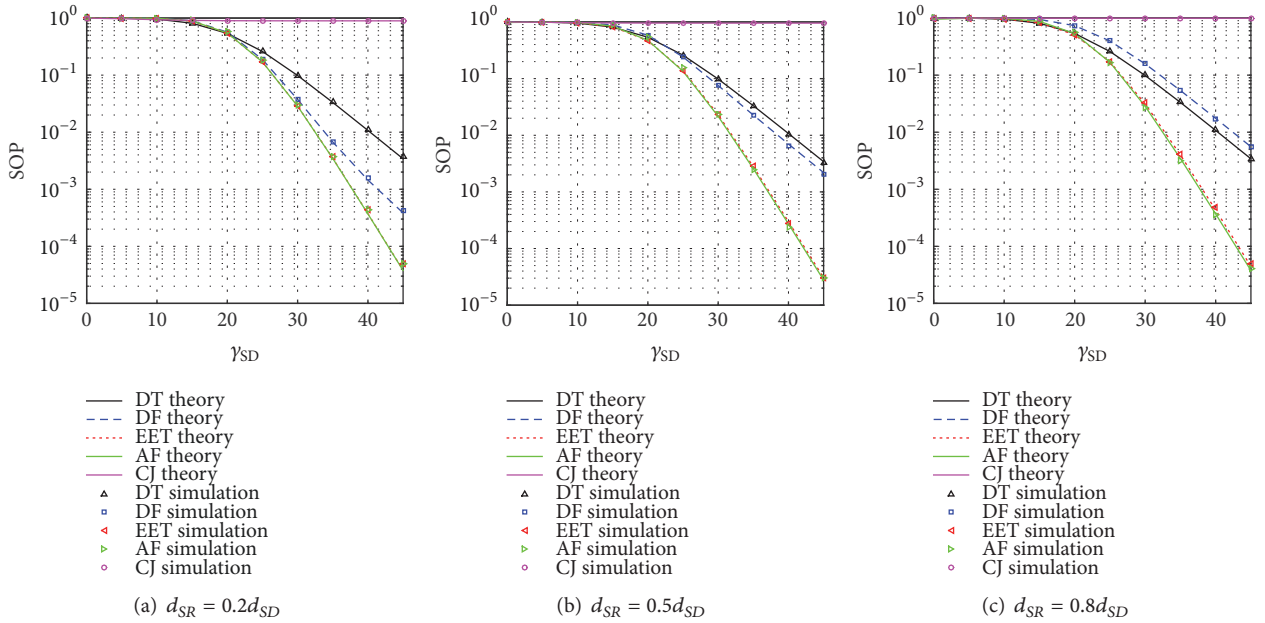
where P_{total}^{sch} denotes the total power consumption of each transmission strategy; that is, $sch \in$ EET, DT, DF, AF, and CJ, which are derived as

$$\begin{aligned} P_{total}^{EET} &= \left(2P_S + 2P_{TX} + 2P_{RX}\right)\Pr\left\{\gamma_{SD} \geq \gamma_{SR}\right\} \\ &\quad + \left(P_S + P_R + 2P_{TX} + 3P_{RX}\right)\Pr\left\{\gamma_{SD} < \gamma_{SR}\right\} \end{aligned} \tag{19}$$

$$P_{total}^{DT} = 2P_S + 2P_{TX} + 2P_{RX} \tag{20}$$

$$P_{total}^{DF} = P_{total}^{AF} = P_S + P_R + 2P_{TX} + 3P_{RX} \tag{21}$$

$$P_{total}^{CJ} = P_S + P_R + 2P_{TX} + P_{RX} \tag{22}$$



(a) $d_{SR} = 0.2d_{SD}$ (b) $d_{SR} = 0.5d_{SD}$ (c) $d_{SR} = 0.8d_{SD}$

FIGURE 2: Secrecy outage probability versus γ_{SD} for different positions of the relay.

where P_{TX} and P_{RX} denote the power costed by the transmit and receive circuitry, respectively. P_S and P_R represent the power spent by the sensor source and by the relay. For simplicity, we assume that $P_S = P_R = P$ in this paper. Furthermore, it is worth noting that the power consumption at E is neglected. Obviously, the denominator of SEE is an increasing function for sending power. Thus, increasement of the power will cause SEE to drop. Note that SEE works as a convex function of the targeted rate. Therefore, we illustrate the optimization problem as

$$\max_{R_S,P} \eta_S \tag{23}$$

It is obviously seen that the exact optimal expressions of R_S and P are very difficult to derive. However, we can use simulation and numerical evaluation to obtain the desired R_S and P via searching algorithm. It should be emphasized that the above expression in (23) has more pragmatic significance for IoT.

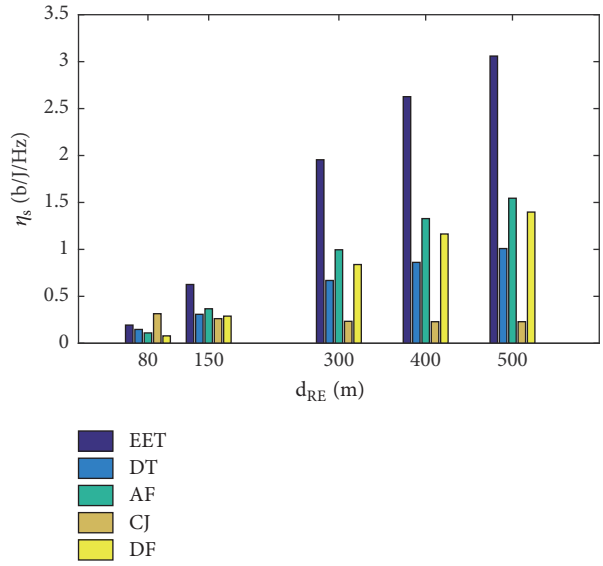


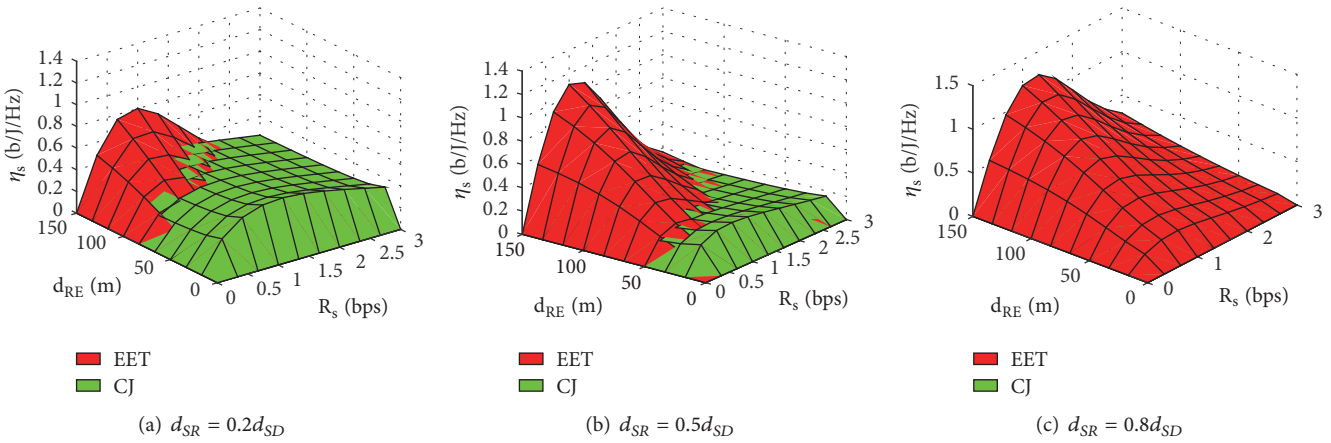
FIGURE 3: Secure energy efficiency versus d_{RE}.

4. Numerical Results

This section provides some numerical simulations to prove the previous theoretical analysis. The parameter configurations in the simulation are set as follows: R_S = 2bps/Hz, d_{SD} = 100m, υ = 2, P_{TX} = 112.2mW, P_{RX} = 97.9mW, B = 10kHz, N_0 = -174dBm/Hz, a link margin of M_l = 10dB, antenna gain G = 5dBi, noise N_f = 10dB, and f = 2.5GHz.

Figures 2(a), 2(b), and 2(c) show the impact of γ_{SD} on the SOP of EET, DT, DF, AF, and CJ transmission strategies for different positions of the relay, respectively, where we observe that, except CJ, the SOP of different transmission strategies was improved by increasing γ_{SD}. This is because increasing the transmitting power benefits both the legitimate destination and cooperative relay. Additionally, it is clearly seen that the simulation results and the theoretical curve match exactly in the whole region, which verifies the accuracy of our conclusions. On the other hand, although the location of the relay changes constantly, the proposed EET and AF can always achieve almost the same optimal secrecy performance. In fact, AF outperforms conventional cooperative schemes (i.e., DF and CJ) in terms of SOP; only if E is closer to relay, CJ has better performance than AF [21]; then we can conclude that the designed EET is a secure cooperative transmission strategy.

When the distance between relay R and E changes, Figure 3 compares the maximum SEE of EET, DT, DF, AF,



(a) $d_{SR} = 0.2d_{SD}$ (b) $d_{SR} = 0.5d_{SD}$ (c) $d_{SR} = 0.8d_{SD}$

FIGURE 4: Secure energy efficiency of EET and CJ versus R_S and d_{RE} for different positions of the relay.

and CJ with the assist of searching methods, which can be used to find the optimal R_S and transmit power. We observe that when E is closer to the legal node, CJ can obtain the best efficiency. On the other hand, when E is far from the legal node, EET performs better in energy efficiency, which confirms that the designed EET is a more energy-efficient secure transmission strategy. Therefore, EET is a low-power green transmission protocol to improve unit energy efficiency for the IoT communication.

In Figure 4, we compare the performance at different transmission rates and at different distances between E and the relay R. For ease of analysis, we just provide the performance comparison between EET and CJ. As the figures show, it is obvious that the performance of the strategies relies on both d_{RE} and R_S. Meanwhile, it is clearly seen that the transmission rate produces a greater impact on EET, and its performance is better when the rate is appropriately low. Thereby, when the EET strategy is adopted in the IoT uplink transmission, for the sake of improving the secrecy performance and energy efficiency of communication systems, a much lower R_S is more suitable. In addition, the location of the relay also has some effects on the EET scheme. Figure 4(a) describes that if the sensor S is closer to the relay R and E stays away from R, EET performs better in contrast to the scenario where E is closer to R. However, if the relay R is closer to the controller D, as shown in Figure 4(c), the jamming signal sent by the relay R will cause serious impact on D, which makes SEE of proposed EET better than CJ. Therefore, we conclude that a more effective energy-efficient secure transmission is introduced by the EET scheme.

5. Conclusion

Secure energy efficiency and physical layer security were investigated in the secure uplink transmission scenario for IoT applications in this paper. Utilizing the advantages of direct and relay links, we proposed a novel energy-efficient secure transmission strategy based on the CSI of the legitimate link (EET), by which the best path is decided between direct and cooperative transmissions, to deal with implementation limits of the IoT devices. The closed-form expressions of SOP and SEE of EET were also derived. In order to show the effectiveness of our new strategy, we further compared the secrecy performance of different transmission schemes such as DF, AF, and CJ as well as DT. The simulation results demonstrated that the proposed EET outperforms other protocols in terms of SEE in most situations. To further enhance the secrecy performance of the IoT networks, EET can be adopted as an effective additional strategy in practical applications. For future work, one interesting aspect is to design the energy-efficient transmission scheme toward secure cooperative IoT in the presence of the multiple eavesdroppers. Other extensions can address another practical issue such as studying the untrusted relays case.

Appendix

By using the formula of full probability, the SOP of DT (14) can be formulated as

$$\begin{aligned} P_{out}^{DT} &= \Pr\left\{C_L^{DT} - C_E^{DT} < R_S\right\} = \Pr\left\{\gamma_{SD} < \nabla\right\} \\ &= \overbrace{\Pr\left\{\gamma_{SD} < \nabla \mid \gamma_{SD} > \gamma_{SE}\right\}}^{\phi_1} \overbrace{\Pr\left\{\gamma_{SD} > \gamma_{SE}\right\}}^{\phi_2} \\ &\quad + \underbrace{\Pr\left\{\gamma_{SD} < \nabla \mid \gamma_{SD} < \gamma_{SE}\right\}}_{\phi_3} \underbrace{\Pr\left\{\gamma_{SD} < \gamma_{SE}\right\}}_{\phi_4} \end{aligned} \tag{A.1}$$

where $\nabla = 2^{2R_S - 1}(1 + 2\gamma_{SE}) - 1/2$. Thus ϕ_2 can be solved as follows:

$$\begin{aligned} \phi_2 &= \Pr\left\{\gamma_{SD} > \gamma_{SE}\right\} = \int_0^{\infty} f_{\gamma_{SD}} d\gamma_{SD} \int_0^{\gamma_{SD}} f_{\gamma_{SE}} d_{\gamma_{SE}} \\ &= \frac{\overline{\gamma_{SD}}}{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}} \end{aligned} \tag{A.2}$$

Similarly, ϕ_4 can be expressed as

$$\phi_4 = \Pr\left\{\gamma_{SD} < \gamma_{SE}\right\} = 1 - \phi_2 = \frac{\overline{\gamma_{SE}}}{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}} \tag{A.3}$$

and ϕ_1 can be obtained as

$$\begin{aligned}\phi_1 &= \Pr\{\gamma_{SD} < \nabla \mid \gamma_{SD} > \gamma_{SE}\} \\ &= \frac{1}{\Pr\{\gamma_{SD} > \gamma_{SE}\}} \int_0^{\infty} f_{\gamma_{SE}} d\gamma_{SE} \overbrace{\int_{\gamma_{SE}}^{\nabla} f_{\gamma_{SD}} d\gamma_{SD}}^{\phi_5}\end{aligned} \tag{A.4}$$

After some simple mathematical manipulations, ϕ_5 in (A.4) can be directly derived as

$$\begin{aligned}\phi_5 = &\exp\left(-\frac{1}{\overline{\gamma_{SD}}}\gamma_{SE}\right) \\ &- \exp\left(\frac{1-2^{2R_S}}{\overline{2\gamma_{SD}}}\right)\exp\left(-\frac{2^{2R_S}}{\overline{\gamma_{SD}}}\gamma_{SE}\right)\end{aligned} \tag{A.5}$$

Therefore, ϕ_1 given by (A.4) can be rewritten as

$$\begin{aligned}\phi_1 &= \frac{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}}{\overline{\gamma_{SD}}} \frac{1}{\overline{\gamma_{SE}}} \int_0^{\infty} \exp\left(-\frac{\gamma_{SE}}{\overline{\gamma_{SE}}}\right) \phi_5 d\gamma_{SE} \\ &= 1 - \frac{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}}{\overline{\gamma_{SD}} + 2^{2R_S}\overline{\gamma_{SE}}} \exp\left(\frac{1-2^{2R_S}}{2\overline{\gamma_{SD}}}\right)\end{aligned} \tag{A.6}$$

Note that when $\gamma_{SD} < \gamma_{SE}$, $C_S = 0 < R_S$; then ϕ_3 can be solved as

$$\phi_3 = \Pr\{\gamma_{SD} < \nabla \mid \gamma_{SD} < \gamma_{SE}\} = 1 \tag{A.7}$$

Finally, the desired expression in (14) can be achieved by summarizing results of (A.2), (A.3), (A.6), and (A.7).

Data Availability

The data in this paper is generated from the simulation in Matlab, and the detail simulation settings can refer to Section 5. Therefore, the data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61501508 and Grant 61671476.

References

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017.

[2] V. N. Vo, T. G. Nguyen, C. So-In, and D. Ha, "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer," *IEEE Access*, vol. 5, pp. 25196–25206, 2017.

[3] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[4] S. Cho, B. F. Spencer, H. Jo et al., "Bridge monitoring using wireless smart sensors," *SPIE Newsroom*, pp. 1–3, 2011.

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

[6] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[7] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[8] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[9] P. Mu, X. Hu, B. Wang, and Z. Li, "Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2174–2177, 2015.

[10] 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 *Proceedings of the ICC 2016 - 2016 IEEE International Conference on Communications*, pp. 1–5, Kuala Lumpur, Malaysia, May 2016.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, UK, 2011.

[12] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

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

[15] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 359–368, 2012.

[16] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage Constrained Secrecy Throughput Maximization for DF Relay Networks," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1741–1755, 2015.

[17] J. Farhat, G. Brante, and R. D. Souza, "On the Secure Energy Efficiency of TAS/MRC with Relaying and Jamming Strategies," *IEEE Signal Processing Letters*, vol. 24, no. 8, pp. 1228–1232, 2017.

[18] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 4874–4883, 2013.

[19] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2703–2709, 2015.

[20] J.-B. Kim, J. Lim, and J. M. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3866–3876, 2015.

[21] F. Gabry, R. Thobaben, and M. Skoglund, "Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel," in *Proceedings of the 2011 IEEE Wireless Communications and Networking Conference, WCNC 2011*, pp. 1328–1333, Mexico, March 2011.

[22] F. Gabry, S. Salimi, R. Thobaben, and M. Skoglund, "High SNR performance of amplify-and-forward relaying in Rayleigh fading wiretap channels," in *Proceedings of the 2013 Iran Workshop on Communication and Information Theory, IWCIT 2013*, pp. 1–5, Iran, May 2013.