IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 10, 2018, accepted February 8, 2018, date of publication February 27, 2018, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2805818

Energy-Efficient Secure Transmission Design for the Internet of Things With an Untrusted Relay

DECHUAN CHEN[1,2], WEIWEI YANG[1], (Member, IEEE), JIANWEI HU[1], (Student Member, IEEE), YUEMING CAI[1], (Senior Member, IEEE), AND XUANXUAN TANG[1]

[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Wuhan Zhongyuan Electronics Group Company, Ltd., Wuhan 430205, China

Corresponding author: Weiwei Yang (wwyang1981@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61771487, Grant 61471393, and Grant 61371122.

ABSTRACT In this paper, we investigate secure uplink transmission in a typical Internet of Things (IoT) deployment, where multiple sensors communicate with a controller via the assistance of an untrusted relay. By taking both the relay and direct links into account, three different scheduling schemes, e.g., optimal scheduling (OS) scheme, threshold-based scheduling (TS) scheme, and random scheduling (RS) scheme, are proposed to cope with the implementation complexity of user scheduling in IoT communications. For each scheduling scheme, we first derive the closed-form expressions for the secrecy outage probability and the secrecy throughput, as well as characterizing the secure energy efficiency to help facilitate an energy-efficient secure transmission design. Finally, numerical simulations demonstrate that increasing the number of sensors is an efficient method to boost the security and energy efficiency under the OS scheme. Moreover, the TS scheme provides a good tradeoff between implementation complexity and secrecy performance.

INDEX TERMS IoT, physical layer security, untrusted relay, secrecy outage probability, secure energy efficiency.

I. INTRODUCTION

Internet of Things (IoT), which is excepted to connect with a variety of devices (e.g., mobile phones, robots, and sensors) from any place at any time, is regarded as a crucial architecture in the forthcoming fifth generation (5G) system to enhance our life quality [1]–[5]. Meanwhile, wireless communication technologies, such as LTE-A, IEEE 802.15.4, and Bluetooth, will be key enablers for actualizing the current landscape of IoT. Furthermore, due to the limited resources of IoT devices, relay transmission is particularly necessary for IoT to save the transmit power and increase the reliability of communication networks [4], [5].

On the other hand, the inherent openness of wireless communication channel poses a practical challenge that must be solved, namely, eavesdropping attacks from unauthorized nodes [6]. Fortunately, physical layer security is emerging as a promising solution to safeguard information theoretic security without increasing neither the complexity of the system nor the needed hardware, and it has gained increasing research attention [2]–[7]. Based on this nature, recent efforts about secure transmission in IoT communications have focused on employing the physical layer security approach. The secrecy outage probability was derived in [4] to understand the secrecy performance of a two-hop IoT network under eavesdropper collusion. In [5], maximizing the secrecy rate under the secrecy outage probability constraint was formulated for relay communication in IoT networks.

However, in practice, the relay node used to achieve cooperative communications may be honest-and-curious. That is, it is willing to comply with the communication protocols forwarding the source's information and at the same time, wants to intercept the confidential information [8]–[12]. Without doubt, these objects connected by the IoT, such as smart sensors, vehicles, and phones, do not always have the authority in accessing the data, even through it may be a cooperating node. Thus, the scenario, where the relay and source-destination pair belong to different heterogenous networks, is very worthy of our attention in IoT communications.

A main scenario behind IoT is a localized group of nodes that perform monitoring or operating tasks. To date, the secure transmission scheme of multiuser networks with untrusted relay node was proposed in [9] and [10]. In [9], a joint opportunistic scheduling and cooperative jamming scheme was designed to enhance the secrecy performance of multiuser untrusted relay networks without the direct link. Furthermore, the ergodic secrecy rate was examined in [10] by proposing a suboptimal user selection scheme based only on the direct link or the relay link.

Apart from security considerations, energy efficiency issue is another obviously essential design concern for the IoT, since the users of IoT are confined by limited power in many situations. The importance of energy efficiency in secure communications has gained further attention with the dramatic growth in the number of devices and massive demands for data traffic in the IoT [13]–[15]. Thus, it is an urgent need to understand the fundamental throughput and energy efficiency limits in order to develop low power green communication. The concept of secure energy efficiency goes back to [16], which addressed cost-efficient wide band secrecy communication in degraded and general wiretap channels. Subsequently, this work was extended to multiple-input and multiple-output (MIMO) relay networks [17], collaborative relay networks [18], and cognitive relay networks [19], [20]. All relays in these works are assumed trusted, and eavesdroppers are external nodes. For two-way untrusted relay networks, [21] maximized secure energy efficiency with the constraints of power and secrecy rate by jointly optimizing power allocation for all nodes. However, energy efficiency of physical layer security has not been considered in multiuser untrusted relay networks. Moreover, scheduling schemes coped with the implementation complexity in untrusted-relay-aided IoT networks remain unexplored.

Enlightened by aforementioned works, we concentrate on secure uplink communications in an IoT scenario, where multiple sensors transmit collected data to a controller in the presence of an untrusted relay. We consider the realistic scenario where the direct links between sensors and controller are available. The maximal ratio combining (MRC) technique is employed at the controller due to its optimality and manageable cost [22]. In particular, the main contributions of the paper are summarized as follows:

- Taking both the relay and direct links into account, we propose three different scheduling schemes, e.g., optimal scheduling (OS) scheme, threshold-based scheduling (TS) scheme, and random scheduling (RS) scheme, to cope with the implementation complexity of user scheduling in IoT communications.
- We derive the closed-form expressions of secrecy outage probability (SOP), secrecy throughput (ST) as well as secure energy efficiency (SEE) to help facilitate an energy-efficient secure transmission design. In order to gain deeper understanding on the practical application of three proposed schemes, we further conduct an asymptotic analysis of the SOPs.
- Our results demonstrate that increasing the number of sensors is an efficient method to boost the SOP and SEE of IoT system under the OS scheme. Moreover, a good tradeoff between implementation complexity and secrecy performance is introduced by the TS scheme for the IoT communications.

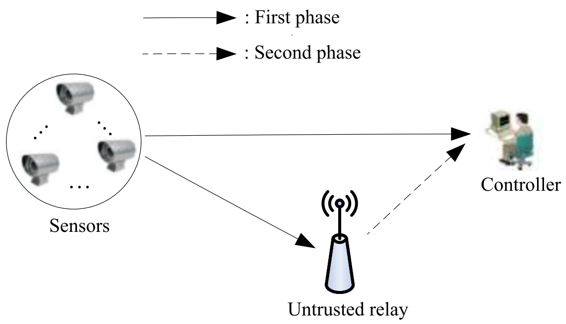

FIGURE 1. System Model.

The remainder of the paper is organized as follows. The system model and user scheduling schemes are presented in the next section. Section III derives the exact SOP, ST and SEE of all the proposed schemes. In section IV, performance of the three scheduling schemes is validated by simulation results. Finally, conclusions are stated in section V.

II. SYSTEM MODEL AND SCHEDULING SCHEME

A. SYSTEM MODEL

Fig. 1 shows a lightweight single-antenna IoT deployment with heterogeneous wireless communication links, where a set of sources $S_n, n = \{1, 2, \cdots N\}$ (e.g., sensors) transmit the detected data to a destination D (e.g., controller) with the help of an untrusted relay R. The untrusted relay has different levels of security clearance as the source and destination nodes in heterogeneous networks, although it is utilized to supplement the direct links to enhance the reliability [23], [24]. Throughout the paper, the main assumptions are listed as follows: 1) We assume the N sources are gathered together to form a cluster, and thereby undergo the same large-scale fading [9]–[11]. 2) A Rayleigh quasi-static fading environment is assumed, i.e., the channel coefficients remain static over one block time and vary independently in different block time. 3) The channel state information (CSI) can be perfectly estimated by the receiver [3]–[5], [9]–[11], [25]–[27]. Therefore, the destination is able to know the global CSI and implement user scheduling. This is reasonable because the channel parameters of the communication links can be obtained at R and D with the help of channel training and estimation, such that D gathers the accurate CSI through relay's cooperation [25]–[27].

The half-duplex relay performs one completed transmission in two phases. In the first phase, the selected source S_n broadcasts a normalized signal x_s at a power of P. Thus, we can express the corresponding received signals at R and D as, respectively,

$$y_R = \sqrt{P} h_{S_nR} x_s + n_R, \tag{1}$$

$$y_{D_1} = \sqrt{P} h_{S_nD} x_s + n_{D_1}, \tag{2}$$

where h_{S_nR} and h_{S_nD} respectively represent the channel coefficients of the $S_n - R$ and $S_n - D$ links with parameters $\bar{\gamma}_{SR}$ and $\bar{\gamma}_{SD}$, n_R and n_{D_1} denote the zero mean additive white Gaussian noise (AWGN) at R and D with variance N_0.

In the second phase, R amplifies and forwards the received signal to D at a power of P with a variable gain $G = 1\Big/\sqrt{P\left|h_{S_nR}\right|^2 + N_0}$. Therefore, the received signal at D during this phase can be written as

$$y_{D_2} = \sqrt{P} G h_{RD} y_R + n_{D_2}, \tag{3}$$

where h_{RD} is the channel coefficient of the $R-D$ link with parameters $\bar{\gamma}_{RD}$, and n_{D_2} is the zero mean AWGN at D with a variance of N_0 in the second phase.

From (1), the achievable instantaneous rate between S_n and R is given by

$$C_{R_n} = \frac{1}{2}\log_2\left(1 + \lambda\left|h_{S_nR}\right|^2\right), \tag{4}$$

where $\lambda = P/N_0$ denotes the transmit signal-to-noise ratio (SNR), and the factor $\frac{1}{2}$ results from the half-duplex constraint. Similarly, the achievable instantaneous rate between S_n and D is given by

$$C_{D_n} = \frac{1}{2}\log_2\left(1 + \lambda\left|h_{S_nD}\right|^2 + \frac{\lambda\left|h_{S_nR}\right|^2 \cdot \lambda\left|h_{RD}\right|^2}{\lambda\left|h_{S_nR}\right|^2 + \lambda\left|h_{RD}\right|^2 + 1}\right). \tag{5}$$

According to [28], the achievable secrecy rate of $S_n - D$ is given by

$$C_{S_n} = \left[C_{D_n} - C_{R_n}\right]^+ = \left[\frac{1}{2}\log_2\left(\gamma_n\right)\right]^+ \tag{6}$$

where $\gamma_n = \frac{1+\lambda\left|h_{S_nD}\right|^2 + \frac{\lambda\left|h_{S_nR}\right|^2 \cdot \lambda\left|h_{RD}\right|^2}{\lambda\left|h_{S_nR}\right|^2 + \lambda\left|h_{RD}\right|^2 + 1}}{1+\lambda\left|h_{S_nR}\right|^2}$, and $[x]^+ \triangleq \max\{0, x\}$.

B. SCHEDULING SCHEME

1) OPTIMAL SCHEDULING

For the optimal scheduling (OS) scheme, the selection criterion is to select a source user that maximizes the secrecy rate, and it is equivalent to maximization of γ_n according to (6), which can be described by

$$n^* = \arg \max_{1\le n\le N} \gamma_n. \tag{7}$$

Different from [9] and [10], this scheduling scheme can provide a much better performance by taking into account all links of the system.

2) THRESHOLD-BASED SCHEDULING

For the threshold-based scheduling (TS) scheme, a predefined threshold γ_T is introduced to select an acceptable user for data transmission. The basic principle of TS scheme can be characterized as:

- The first user is selected for data transmission and no further processing is needed once γ_1 exceeds the threshold, i.e., $\gamma_1 > \gamma_T$.
- The nth user is adopted for data transmission when γ_{n-1} is low than the threshold, whilst γ_n is above than the threshold, i.e., $\max(\gamma_1, \cdots, \gamma_{n-1}) < \gamma_T$ and $\gamma_T < \gamma_n$.
- The best user is employed for data transmission if each γ_n is below the threshold, i.e., $\max(\gamma_1, \cdots, \gamma_N) < \gamma_T$.

3) RANDOM SCHEDULING

For the random scheduling (RS) scheme, it not only circumvents the need for channel estimation, but also obviates the need for feedback overhead. In each transmission, a source user is randomly scheduled for data transmission. This simple scheduling scheme also can be regarded as a benchmark for the OS and TS schemes.

III. PERFORMANCE ANALYSIS

In this section, the SOP, asymptotic SOP, ST, and SEE are characterized to comprehensively evaluate the secrecy performance and energy efficiency for the OS, TS and RS schemes.

A. SECRECY OUTAGE PROBABILITY

1) OPTIMAL SCHEDULING

In this paper, SOP is defined as the probability of instantaneous secrecy capacity being lower than a target secrecy rate R_s, which can be mathematically formulated as

$$P_{out}^{OS} = \Pr\left(C_{S_{n^*}} < R_s\right) = \Pr\left(\max_{1\le n\le N} \gamma_n < \gamma_{th}\right), \tag{8}$$

where $\gamma_{th} = 2^{2R_s}$.

From (8), the key challenge in the analysis lies in the fact that the received SNRs of γ_n with N sources are statistically dependent, because of the common random variable (RV) $|h_{RD}|^2$. In the following, the condition-and-average approach is adopted to tackle this troublesome. Specifically, we define $Z_n = \gamma_n$ and $v = |h_{RD}|^2$, and derive the cumulative distribution function (CDF) Z_n conditioned on v in the following lemma.

Lemma 1:

$$F_{Z_n}(z|v) = \begin{cases} \frac{z\bar{\gamma}_{SR}}{\bar{\gamma}_{SD} + z\bar{\gamma}_{SR}} e^{-\frac{1-z}{z\lambda\bar{\gamma}_{SR}} - \frac{v}{z\bar{\gamma}_{SR}}}, & 0 < z < 1 \\ 1 - \frac{\bar{\gamma}_{SD} e^{-\frac{z-1}{\lambda\bar{\gamma}_{SD}}}}{\bar{\gamma}_{SD} + (z-1)\bar{\gamma}_{SR}} + \left(\frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD} + (z-1)\bar{\gamma}_{SR}} - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD} + z\bar{\gamma}_{SR}}\right) e^{-\frac{z-1}{\lambda\bar{\gamma}_{SD}} - \left(\frac{1}{\bar{\gamma}_{SR}} + \frac{z-1}{\bar{\gamma}_{SD}}\right)v}, & z \ge 1 \end{cases} \tag{9}$$

Proof: See Appendix A.

Based on Lemma 1, the SOP in (8) can be characterized by

$$\begin{aligned} P_{out}^{OS} &= \int_0^\infty F_{Z_n}^N(\gamma_{th}|v) f_v(v)\, dv \\ &= \frac{1}{\bar{\gamma}_{RD}} \int_0^\infty \left(a_1 + a_2 e^{-a_3 v}\right)^N e^{-\frac{v}{\bar{\gamma}_{RD}}} dv \\ &= \sum_{r=0}^N \binom{N}{r} \frac{a_1^{N-r} a_2^r}{1 + a_3 r \bar{\gamma}_{RD}}, \end{aligned} \tag{10}$$

where $a_1 = 1 - \frac{\bar{\gamma}_{SD} e^{-\frac{\gamma_{th}-1}{\lambda \bar{\gamma}_{SD}}}}{\bar{\gamma}_{SD}+(\gamma_{th}-1)\bar{\gamma}_{SR}}$, $a_3 = \frac{1}{\bar{\gamma}_{SR}} + \frac{\gamma_{th}-1}{\bar{\gamma}_{SD}}$, and $a_2 = \left(\frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_{th}-1)\bar{\gamma}_{SR}} - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+\gamma_{th}\bar{\gamma}_{SR}}\right) e^{-\frac{\gamma_{th}-1}{\lambda \bar{\gamma}_{SD}}}$.

2) THRESHOLD-BASED SCHEDULING

According to the basic principle of the TS scheme, the SOP can be formulated as

$$P_{out}^{TS} = \begin{cases} \Pr[\gamma_T < \gamma_1 < \gamma_{th}] \\ + \sum_{k=2}^{N} \Pr[\max(\gamma_1, \cdots, \gamma_{k-1}) < \gamma_T \& \gamma_T < \gamma_k < \gamma_{th}] \\ + \Pr[\max(\gamma_1, \cdots, \gamma_N) < \gamma_T], & \gamma_{th} > \gamma_T \\ \Pr[\max(\gamma_1, \cdots, \gamma_N) < \gamma_{th}], & \gamma_{th} \le \gamma_T. \end{cases} \tag{11}$$

Then, we can derive a close-form expression for (11) in the following theorem.

Theorem 1:

$$P_{out}^{TS} = \begin{cases} P_{out}^{OS}, & \gamma_T \ge \gamma_{th} \\ I_1 + I_2, & 1 \le \gamma_T < \gamma_{th} \\ I_3 + I_4, & 0 < \gamma_T < 1 \end{cases} \tag{12}$$

where I_1, I_2, I_3 and I_4 are respectively expressed as

$$I_1 = a_1 - a_6 + \frac{a_2}{1 + a_3 \bar{\gamma}_{RD}} - \frac{a_7}{1 + a_8 \bar{\gamma}_{RD}} + \sum_{r=0}^{N} \binom{N}{r} \frac{a_6^{N-r} a_7^r}{1 + a_8 r \bar{\gamma}_{RD}}, \tag{13}$$

$$I_2 = \sum_{k=2}^{N} \sum_{r=0}^{k-1} \binom{k-1}{r} a_6^{k-1-r} a_7^r \cdot \left(\frac{a_1 - a_6}{1 + r a_8} + \frac{a_2}{1 + a_3 \bar{\gamma}_{RD} + a_8 r \bar{\gamma}_{RD}} - \frac{a_7}{1 + a_8 \bar{\gamma}_{RD} + a_8 r \bar{\gamma}_{RD}} \right), \tag{14}$$

$$I_3 = a_1 + \frac{a_2}{1 + a_3 \bar{\gamma}_{RD}} - \frac{a_9 \gamma_T \bar{\gamma}_{SR}}{\gamma_T \bar{\gamma}_{SR} + \bar{\gamma}_{RD}} + \frac{a_9^N \gamma_T \bar{\gamma}_{SR}}{\gamma_T \bar{\gamma}_{SR} + N \bar{\gamma}_{RD}}, \tag{15}$$

$$I_4 = \sum_{k=2}^{N} a_9^{k-1} \left(\frac{a_2 \gamma_T \bar{\gamma}_{SR}}{\gamma_T \bar{\gamma}_{SR} + a_3 \gamma_T \bar{\gamma}_{SR} \bar{\gamma}_{RD} + (k-1) \bar{\gamma}_{RD}} + \frac{a_1 \gamma_T \bar{\gamma}_{SR}}{\gamma_T \bar{\gamma}_{SR} + (k-1) \bar{\gamma}_{RD}} - \frac{a_9 \gamma_T \bar{\gamma}_{SR}}{\gamma_T \bar{\gamma}_{SR} + \bar{\gamma}_{RD} + (k-1) \bar{\gamma}_{RD}} \right), \tag{16}$$

with $a_6 = 1 - \frac{\bar{\gamma}_{SD} e^{-\frac{\gamma_T-1}{\lambda \bar{\gamma}_{SD}}}}{\bar{\gamma}_{SD}+(\gamma_T-1)\bar{\gamma}_{SR}}$, $a_8 = \frac{1}{\bar{\gamma}_{SR}} + \frac{\gamma_T-1}{\bar{\gamma}_{SD}}$, $a_7 = \left(\frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_T-1)\bar{\gamma}_{SR}} - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+\gamma_T\bar{\gamma}_{SR}}\right) e^{-\frac{\gamma_T-1}{\lambda \bar{\gamma}_{SD}}}$, and $a_9 = \frac{\gamma_T \bar{\gamma}_{SR} e^{-\frac{1-\gamma_T}{\lambda \gamma_T \bar{\gamma}_{SR}}}}{\gamma_T \bar{\gamma}_{SR} + \bar{\gamma}_{SD}}$.

Proof: See Appendix B.

3) RANDOM SCHEDULING

By using the similar procedures, the exact expression of SOP for the RS scheme is given by

$$P_{out}^{RS} = 1 - \frac{\bar{\gamma}_{SD} e^{-\frac{\gamma_{th}-1}{\lambda \bar{\gamma}_{SD}}}}{\bar{\gamma}_{SD} + (\gamma_{th} - 1) \bar{\gamma}_{SR}} + \frac{a_2}{1 + a_3 \bar{\gamma}_{RD}}. \tag{17}$$

Remark 1: According to (10), we state that for the OS scheme, increasing the number of sources can effectively enhance the secrecy performance of IoT communications. Moreover, the secrecy performance of the TS scheme switches between the RS scheme and the OS scheme with the increase of the predefined threshold. Thus, a good trade-off between implementation complexity and secrecy performance is introduced by the TS scheme. In addition, the RS scheme is an alternate way with a reduced implementation complexity, when the CSI of the considered system is unavailable.

B. ASYMPTOTIC BEHAVIOUR

In order to gain deeper understanding on the practical application of three proposed schemes, we now turn our attention to investigating the asymptotic behaviour of the secrecy outage probability in high SNR region, e.g., $\lambda \to \infty$.

1) OPTIMAL SCHEDULING

From (10), we have

$$\lim_{\lambda \to \infty} P_{out}^{OS} = \sum_{r=0}^{N} \binom{N}{r} \frac{a_4^{N-r} a_5^r}{1 + a_3 r \bar{\gamma}_{RD}}, \tag{18}$$

where $a_4 = 1 - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_{th}-1)\bar{\gamma}_{SR}}$, and $a_5 = \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_{th}-1)\bar{\gamma}_{SR}} - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+\gamma_{th}\bar{\gamma}_{SR}}$.

2) THRESHOLD-BASED SCHEDULING

For the TS scheme, according to (12), the SOP will converge to

$$\lim_{\lambda \to \infty} P_{out}^{TS} = \begin{cases} \sum_{r=0}^{N} \binom{N}{r} \frac{a_4^{N-r} a_5^r}{1 + a_3 r \bar{\gamma}_{RD}}, & \gamma_T \ge \gamma_{th} \\ I_5 + I_6, & 1 \le \gamma_T < \gamma_{th} \\ I_7 + I_8, & 0 < \gamma_T < 1 \end{cases} \tag{19}$$

where I_5, I_6, I_7 and I_8 are respectively expressed as

$$I_5 = a_4 - a_{10} + \frac{a_5}{1 + a_3 \bar{\gamma}_{RD}} - \frac{a_{11}}{1 + a_8 \bar{\gamma}_{RD}} + \sum_{r=0}^{N} \binom{N}{r} \frac{a_{10}^{N-r} a_{11}^r}{1 + a_8 r \bar{\gamma}_{RD}}, \tag{20}$$

$$I_6 = \sum_{k=2}^{N} \sum_{r=0}^{k-1} \binom{k-1}{r} a_{10}^{k-1-r} a_{11}^r \left(\frac{a_1 - a_{10}}{1 + r a_8} + \frac{a_5}{1 + a_3 \bar{\gamma}_{RD} + a_8 r \bar{\gamma}_{RD}} - \frac{a_{11}}{1 + a_8 \bar{\gamma}_{RD} + a_8 r \bar{\gamma}_{RD}} \right), \tag{21}$$

$$I_7 = a_4 + \frac{a_5}{1+a_3\bar{\gamma}_{RD}} - \frac{a_{12}\gamma_T\bar{\gamma}_{SR}}{\gamma_T\bar{\gamma}_{SR}+\bar{\gamma}_{RD}} + \frac{a_{12}^N\gamma_T\bar{\gamma}_{SR}}{\gamma_T\bar{\gamma}_{SR}+N\bar{\gamma}_{RD}}, \tag{22}$$

$$I_8 = \sum_{k=2}^{N} a_{12}^{k-1}\left(\frac{a_5\gamma_T\bar{\gamma}_{SR}}{\gamma_T\bar{\gamma}_{SR}+a_3\gamma_T\bar{\gamma}_{SR}\bar{\gamma}_{RD}+(k-1)\bar{\gamma}_{RD}} + \frac{a_4\gamma_T\bar{\gamma}_{SR}}{\gamma_T\bar{\gamma}_{SR}+(k-1)\bar{\gamma}_{RD}} - \frac{a_{12}\gamma_T\bar{\gamma}_{SR}}{\gamma_T\bar{\gamma}_{SR}+\bar{\gamma}_{RD}+(k-1)\bar{\gamma}_{RD}}\right), \tag{23}$$

with $a_{10} = 1 - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_T-1)\bar{\gamma}_{SR}}$, $a_{12} = \frac{\gamma_T\bar{\gamma}_{SR}}{\gamma_T\bar{\gamma}_{SR}+\bar{\gamma}_{SD}}$, and $a_{11} = \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_T-1)\bar{\gamma}_{SR}} - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+\gamma_T\bar{\gamma}_{SR}}$.

3) RANDOM SCHEDULING

It is also straightforward to verify from (17) that, for the RS scheme,

$$\lim_{\lambda\to\infty} P_{out}^{RS} = 1 - \frac{\bar{\gamma}_{SD}}{\bar{\gamma}_{SD}+(\gamma_{th}-1)\bar{\gamma}_{SR}} + \frac{a_5}{1+a_3\bar{\gamma}_{RD}}. \tag{24}$$

Remark 2: It is observed that the asymptotic SOP of the three schemes are nonzero constants independent of λ, which indicates that the SOP will not approach zero even increasing transmit power unboundedly. Therefore, too large transmit power is not helpful, because the channel quality difference between the legitimate link and the eavesdropping link will finally become the bottleneck and dominate the secrecy outage probability.

C. SECRECY THROUGHPUT

The ST definition adopted in our paper corresponds to the average secrecy rate achieving a reliable and secure transmission at the destination [29], given by

$$\eta^\star = R_s\left(1-P_{out}^\star\right), \tag{25}$$

where $\star \in \{OS, TS, RS\}$.

Remark 3: Given the result of (25), we numerically find that if R_s is small, even though the secrecy outage probability is low, the ST is still small; if R_s is large, the secrecy outage probability will be close to one and therefore the value of ST remains small. This observation is of practical significance for designers to determine a suitable value of target secrecy rate which achieves the maximal ST. The design problem can be formulated as

$$\max_{R_s} \eta^\star. \tag{26}$$

An explicit expression for R_s is intractable. Instead, the optimal solutions can be evaluated by numerical calculations, e.g., the gradient-based search techniques.

D. SECURE ENERGY EFFICIENCY

In fact, the security improvement is often accompanied with high power consumption. From the perspective of the sustainability, greedily pursuing secrecy performance may be disadvantageous for IoT users, which generally have significant energy constraints. For the IoT devices, secure communications should work in a green manner to improve unit energy efficiency. Therefore, the SEE is adopted here as the preferred metric to achieve physical layer security and energy efficiency simultaneously, which is defined as the ratio of secrecy throughput to the total power consumption. Mathematically, the SEE is expressed as

$$\xi^\star = \frac{R_s\left(1-P_{out}^\star\right)}{P_{total}}, \tag{27}$$

where $P_{total} = \frac{2P}{\kappa} + P_c$ with κ being the power amplifier efficiency and P_c being the all other circuit power except power amplifier [19].

Remark 4: Due to a tradeoff between security and reliability imposed by the untrusted relay, the secrecy outage probability of the three proposed schemes become saturated in the high transmit power region. However, the denominator of SEE is an increasing function of the transmit power. Thus, overload transmit power will incur a negative effect on the SEE. On the other hand, from (26) and (27), the SEE is also a convex function of the target secrecy rate. Thus, the optimization problem can be expressed as

$$\max_{R_s,\lambda} \xi^\star. \tag{28}$$

Likewise, a rigorous analysis of optimal exact expressions for R_s and λ is not tractable. Instead, with the aid of searching methods, simulations and numerical calculations can be used again to find the optimal R_s and λ. It is highlighted that the optimization problem (28) is of more practical operational significance for the IoT communications.

IV. NUMERICAL RESULTS

In this section, Monte Carlo simulation results are provided to validate the theoretical analysis derived in the previous sections. Unless otherwise stated, the simulation parameters are set as $\kappa = 0.38$, $P_c = 100mW$, $R_s = 0.2\ bit/s/Hz$, $\gamma_T = 1.2$, $\bar{\gamma}_{SR} = \bar{\gamma}_{SD} = \bar{\gamma}_{RD} = 0dB$, and $N_0 = 1$. In each figure, the theoretical curves and simulation points match precisely with each other in all regions, which confirms the accuracy of our derivations.

Figs. 2, 3, and 4 plot the impact of λ, N and γ_T on the SOP of the OS, TS and RS schemes, respectively. We observe that the SOP first decreases and then reaches an error floor with increasing transmit SNR for a given number of sources. This is due to the fact that any increasing in the transmit power is beneficial for both the destination and the untrusted relay. We further observe that the outage probability of the OS scheme decays linearly as the number of sources increases, which indicates it is an effective method to enhance the secrecy performance under the OS scheme by increasing the number of sources. Moreover, the decline rate of the TS scheme is slower than the OS scheme, and the SOP of the RS scheme is independent of the number of sources. In addition, we observe that the performance of the TS scheme

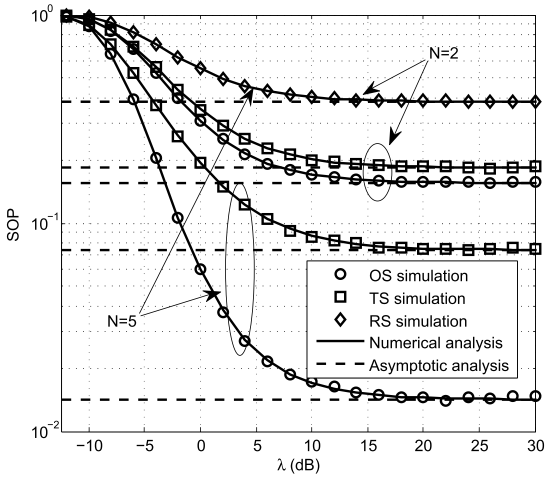

FIGURE 2. SOP vs transmit SNR.

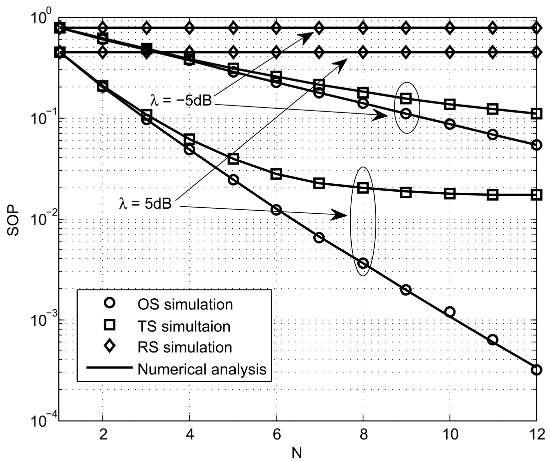

FIGURE 3. SOP vs the number of sources.

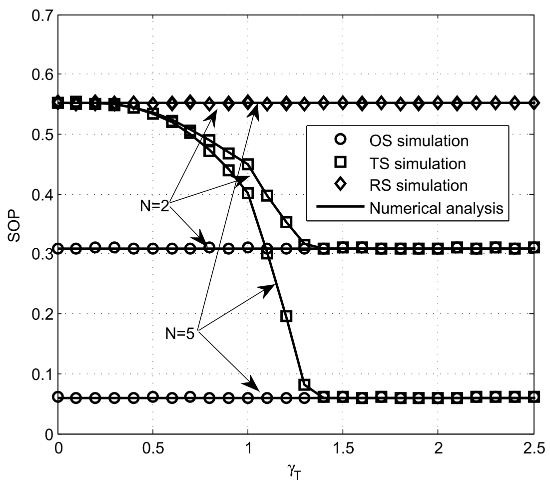

FIGURE 4. SOP vs γ_T.

switches between the RS scheme and the OS scheme as the predefined threshold increases. This is because when the predefined threshold is too small, only the first source node is selected for data transmission, which is equivalent to the RS scheme. On the other hand, when the predefined threshold is sufficiently large, the user maximizing the secrecy rate is scheduled for transmission, which is equal to the OS scheme. Therefore, we know that a good tradeoff between implementation complexity and secrecy performance is introduced by the TS scheme.

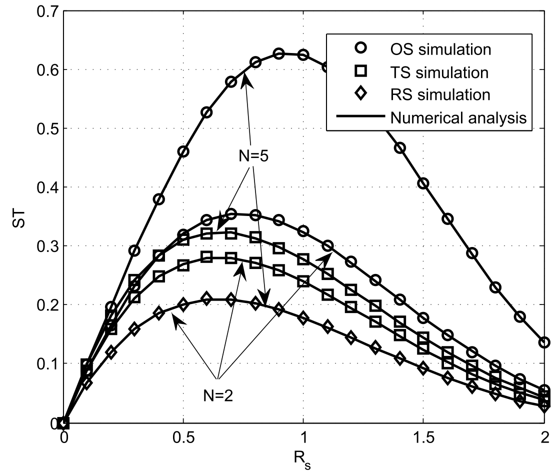

FIGURE 5. ST vs R_S with $\lambda = 10dB$.

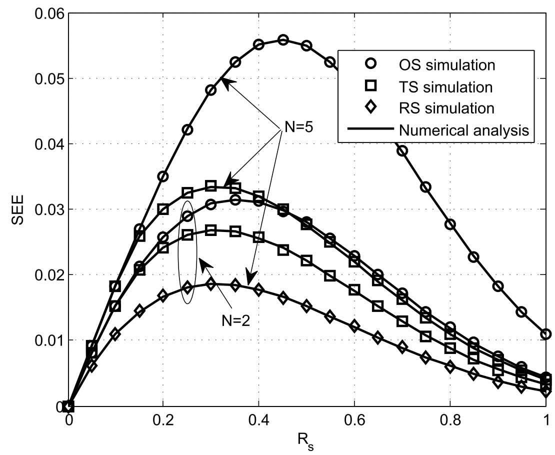

FIGURE 6. SEE vs R_S with $\lambda = 0dB$.

Figs. 5 and 6 plot the ST and SEE of the three proposed schemes versus R_s, respectively. We observe that both ST and SEE first increase with the target secrecy rate R_s increasing and then decrease when R_s increases beyond a unique value for a given number of sources, which is consistent with the Remark 3 and Remark 4. Focusing on the peaks of the ST and SEE, we also observe that the optimal R_s of the OS scheme increases as the number of sources increases. This is due to the fact that a larger N leads to a better secrecy capacity of the considered system, thereby, a larger R_s we set to maximize the ST.

Fig. 7 plots the SEE of the OS, RS and TS schemes versus transmit SNR. It is clearly seen that when the transmit SNR is either extremely small or large, the SEE approaches to

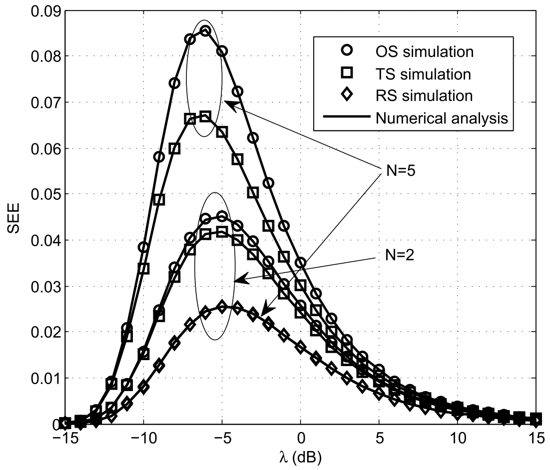

FIGURE 7. SEE vs transmit SNR.

zero. This is because when the transmit SNR is too small, it is difficult to establish a reliable and secure link from the sources to the destination which of course will lead to the poor SEE. When transmit SNR is too large, too much power is wasted unnecessarily, consequently, also deteriorates the SEE. Therefore, we conclude that the transmit power can be optimized to maximize the SEE of IoT communications with an untrusted relay. In addition, we observe that increasing the number of source nodes has a positive impact on the SEE for the OS and TS schemes. The reason is that the more number of source nodes, the better secrecy throughput at a fixed transmit power.

V. CONCLUSION

In this paper, physical layer security and multiuser diversity techniques were investigated jointly in an untrusted-relay-aided IoT network. By taking both the relay and direct links into account, we designed three different scheduling schemes, e.g., OS scheme, TS scheme, and RS scheme, to cope with the implementation complexity of user scheduling in IoT communications. The exact SOP, ST and SEE were derived to characterize the security and energy efficiency of the considered system. Our numerical results indicated that it is favorable to put more nodes in the cluster of source, which produces the improvement of security and energy efficiency for the OS scheme. Moreover, a good tradeoff between implementation complexity and secrecy performance is introduced by the TS scheme.

APPENDIX A

The conditional CDF of Z_n can be formulated as

$$F_{Z_n}(z|v) \approx \Pr\left(\frac{1+\lambda\left|h_{S_nD}\right|^2+\lambda\min\left(\left|h_{S_nR}\right|^2, v\right)}{1+\lambda\left|h_{S_nR}\right|^2}<z\right)$$
$$=\underbrace{\Pr\left(1+\frac{\lambda\left|h_{S_nD}\right|^2}{1+\lambda\left|h_{S_nR}\right|^2}<z,\left|h_{S_nR}\right|^2<v\right)}_{\varphi_1}$$
$$+\underbrace{\Pr\left(\frac{1+\lambda\left|h_{S_nD}\right|^2+\lambda v}{1+\lambda\left|h_{S_nR}\right|^2}<z,\left|h_{S_nR}\right|^2>v\right)}_{\varphi_2} \quad (29)$$

where the approximation is widely adopted by the fact that $\frac{XY}{X+Y+1}\approx\min(X,Y)$ [11]. In the following, the terms of φ_1 and φ_2 can be derived into two cases, e.g., $z\geq 1$ and $0<z<1$.

1) Case of $z\geq 1$: It is easy to write φ_1 as

$$\varphi_1=\frac{1}{\bar{\gamma}_{SR}}\int_0^v\left(1-e^{-\frac{z-1+\lambda(z-1)x}{\lambda\bar{\gamma}_{SD}}}\right)e^{-\frac{x}{\bar{\gamma}_{SR}}}dx$$
$$=1-e^{-\frac{v}{\bar{\gamma}_{SR}}}-\frac{\bar{\gamma}_{SD}e^{-\frac{z-1}{\lambda\bar{\gamma}_{SD}}}}{\bar{\gamma}_{SD}+(z-1)\bar{\gamma}_{SR}}\left(1-e^{-\left(\frac{1}{\bar{\gamma}_{SR}}+\frac{z-1}{\bar{\gamma}_{SD}}\right)v}\right). \quad (30)$$

Similarly, φ_2 in (29) can be expressed as

$$\varphi_2=\frac{1}{\bar{\gamma}_{SR}}\int_v^\infty\left(1-e^{-\frac{z-1-\lambda v+z\lambda x}{\lambda\bar{\gamma}_{SD}}}\right)e^{-\frac{x}{\bar{\gamma}_{SR}}}dx$$
$$=e^{-\frac{v}{\bar{\gamma}_{SR}}}-\frac{\bar{\gamma}_{SD}e^{-\left(\frac{z-1}{\lambda\bar{\gamma}_{SD}}+\frac{v}{\bar{\gamma}_{SR}}+\frac{(z-1)v}{\bar{\gamma}_{SD}}\right)}}{\bar{\gamma}_{SD}+z\bar{\gamma}_{SR}}. \quad (31)$$

2) Case of $0<z<1$: In this case, $1+\frac{\lambda\left|h_{S_nD}\right|^2}{1+\lambda\left|h_{S_nR}\right|^2}<z$ can not hold, such that we have $\varphi_1=0$. Now, φ_2 can be written as

$$\varphi_2=\frac{1}{\bar{\gamma}_{SR}}\int_{\frac{1+\lambda v-z}{z\lambda}}^\infty\left(1-e^{-\frac{z-1-\lambda v+z\lambda x}{\lambda\bar{\gamma}_{SD}}}\right)e^{-\frac{x}{\bar{\gamma}_{SR}}}dx$$
$$=\frac{z\bar{\gamma}_{SR}}{\bar{\gamma}_{SD}+z\bar{\gamma}_{SR}}e^{-\frac{1-z}{z\lambda\bar{\gamma}_{SR}}-\frac{v}{z\bar{\gamma}_{SR}}}. \quad (32)$$

Then, the conditional CDF of Z_n can be derived by summarizing results of (30), (31) and (32).

APPENDIX B

According to (9) and (11), we know that three cases, e.g., $\gamma_T\geq\gamma_{th}$, $1\leq\gamma_T<\gamma_{th}$ and $0<\gamma_T<1$, have to be discussed for calculating the exact expression of P_{out}^{TS}.

1) Case of $\gamma_T\geq\gamma_{th}$: In this case, it is easy to have $P_{out}^{TS}=P_{out}^{OS}$.

2) Case of $1\leq\gamma_T<\gamma_{th}$: In this case, based on lemma 1, the SOP can be rewritten as

$$P_{out}^{TS}=\frac{1}{\bar{\gamma}_{RD}}\int_0^\infty\left(a_1+a_2e^{-a_3v}-a_6-a_7e^{-a_8v}\right)e^{-\frac{v}{\bar{\gamma}_{RD}}}dv$$
$$+\sum_{k=2}^{N}\frac{1}{\bar{\gamma}_{RD}}\int_0^\infty\left(a_6-a_7e^{-a_8v}\right)^{k-1}$$
$$\cdot\left(a_1+a_2e^{-a_3v}-a_6-a_7e^{-a_8v}\right)e^{-\frac{v}{\bar{\gamma}_{RD}}}dv$$
$$+\frac{1}{\bar{\gamma}_{RD}}\int_0^\infty\left(a_6+a_7e^{-a_8v}\right)^Ne^{-\frac{v}{\bar{\gamma}_{RD}}}dv \quad (33)$$

Then, the closed-form expression can be easily derived with the help of probability theory and binomial theorem.

3) Case of $0 < \gamma_T < 1$: In this case, the SOP can be expressed as

$$P_{out}^{TS} = \frac{1}{\bar{\gamma}_{RD}} \int_0^{\infty} \left(a_1 + a_2 e^{-a_3 v} - a_9 e^{-\frac{v}{\gamma_T \bar{\gamma}_{SR}}} \right) e^{-\frac{v}{\bar{\gamma}_{RD}}} dv + \sum_{k=2}^{N} \frac{1}{\bar{\gamma}_{RD}} \int_0^{\infty} a_9^{k-1} e^{-\frac{v(k-1)}{\gamma_T \bar{\gamma}_{SR}}} \cdot \left(a_1 + a_2 e^{-a_3 v} - a_9 e^{-\frac{v}{\gamma_T \bar{\gamma}_{SR}}} \right) e^{-\frac{v}{\bar{\gamma}_{RD}}} dv + \frac{a_9^N}{\bar{\gamma}_{RD}} \int_0^{\infty} e^{-\left(\frac{N}{\gamma_T \bar{\gamma}_{SR}} + \frac{1}{\bar{\gamma}_{RD}}\right) v} dv \quad (34)$$

Following the same approach as in Case 2), the desired expression can be directly obtained after some simple mathematical manipulations.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[2] 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.

[3] B. Chen *et al.*, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.

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

[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] 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.

[7] W. Yang, W. Mou, X. Xu, W. Yang, and Y. Cai, "Energy efficiency analysis and enhancement for secure transmission in SWIPT systems exploiting full duplex techniques," *IET Commun.*, vol. 10, no. 14, pp. 1712–1720, 2016.

[8] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[9] F. Ding, H. Wang, S. Zhang, and M. Dai, "Multiuser untrusted relay networks with joint cooperative jamming and opportunistic scheduling under perfect and outdated CSI," *Electron. Lett.*, vol. 52, no. 23, pp. 1925–1927, 2016.

[10] D. Deng, X. Li, L. Fan, W. Zhou, R. Hu, and Z. Zhou, "Secrecy analysis of multiuser untrusted amplify-and-forward relay networks," *Wireless Commun. Mobile Comput.*, vol 2017, Jan. 2017, Art. no. 9580639.

[11] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 463–466, Mar. 2015.

[12] A. A. Zewail and A. Yener, "Multi-terminal two-hop untrusted-relay networks with hierarchical security guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2052–2066, Sep. 2017.

[13] D. Feng, C. Jiang, G. Lim, L. J. Cimini, J. G. Feng, and G. Y. Li, "A survey of energy-efficient wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 167–178, 1st Quart., 2013.

[14] M. Ozmen and M. C. Gursoy, "Secure transmission of delay-sensitive data over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2036–2051, Sep. 2017.

[15] J. Huang, Q. Duan, C.-C. Xing, and H. Wang, "Topology control for building a large-scale and energy-efficient internet of things," *IEEE Wireless Commun.*, vol. 24, no. 1, pp. 67–73, Feb. 2017.

[16] M. El-Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1909–1920, Sep. 2013.

[17] W. Xu, J. Liu, S. Jin, and X. Dong, "Spectral and energy efficiency of multi-pair massive MIMO relay network with hybrid processing," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3794–3809, Sep. 2017.

[18] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[19] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

[20] X. Xu, J. Bao, H. Cao, Y.-D. Yao, and S. Hu, "Energy-efficiency-based optimal relay selection scheme with a BER constraint in cooperative cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 191–203, Jan. 2016.

[21] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861–1874, May 2016.

[22] J. Farhat, G. Brante, and R. D. Souza, "On the secure energy efficiency of TAS/MRC with relaying and jamming strategies," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1228–1232, Aug. 2017.

[23] D. Chen, Y. Cheng, W. Yang, J. Hu, and Y. Cai, "Physical layer security in cognitive untrusted relay networks," *IEEE Access*, to be published, doi: 10.1109/ACCESS.2017.2762738.

[24] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4874–4883, Dec. 2013.

[25] L. Sun, T. Zhang, Y. Li, and N. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[26] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2703–2709, Jun. 2015.

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

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

[29] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.

DECHUAN CHEN received the M.S. degree in information and communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2017, where he is currently pursuing the Ph.D. degree in information and communications engineering. His research interests include cooperative communications, physical-layer security, energy harvesting, and cognitive radio systems.

WEIWEI YANG (S'08–M'12) received the B.S., M.S., and Ph.D. degrees from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively. His research interests include orthogonal frequency-domain multiplexing systems, signal processing in communications, cooperative communications, wireless sensor networks, and network security.

JIANWEI HU (S'14) received the B.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2012, where he is currently pursuing the Ph.D. degree in communications and information system. His research interests include MIMO systems, cooperative communications, and network security.

YUEMING CAI (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982, and the M.S. degree in micro-electronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include MIMO systems, OFDM systems, signal processing in communications, cooperative communications, and wireless sensor networks.

XUANXUAN TANG received the B.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2014, where he is currently pursuing the Ph.D. degree in information and communications engineering. His current research interests include cooperative communications, wireless sensor networks, the Internet of Things, physical-layer security, energy harvesting, full-duplex, and cognitive radio systems.