

RESEARCH

Open Access



A novel secure relay selection strategy for energy-harvesting-enabled Internet of things

Yan Huo^{*} , Mi Xu, Xin Fan and Tao Jing

Abstract

In this article, we focus on the problem of relay selection for the cooperative cognitive radio-based Internet of things. In such systems, a pair of primary user devices (PUs) can only communicate with each other through a relay. The relay is selected from a set of multi-slot energy-harvesting (EH)-enabled secondary user devices (SUs). The charging and discharging process of an SD's battery is formulated as a finite state Markov chain, and we can derive the corresponding analytical expression of steady-state distribution. Consider the non-authority of SUs, we analyze the outage performance when SUs are trusted and untrusted. When SUs are trusted, we provide the theoretical analysis expression and the lower bound expression for the outage probability. On the contrary, we propose a destination-assisted jamming strategy to secure primary communication if SUs are untrusted. In addition, we propose a Vickrey auction-based EH-enabled relay selection strategy which can be applied to the secondary system. For this auction strategy, SUs without direct links can transmit signals by selecting an EH-enabled SU as a relay. The winning SU in the process of auction can earn reward. Finally, the simulation results verify that the EH-based transmission can obtain excellent system performance without consuming excess energy, and we also study the effect of different parameters on system outage performance.

Keywords: Energy harvesting, Physical layer security, Outage probability, Markov chain, Cooperative cognitive radio networks

1 Introduction

Internet of things (IoT) is emerging as a new paradigm to achieve network convergence in 5G mobile communications. It definitely requires mass data exchanging and sharing among numerous mobile nodes, e.g., machine-to-machine (M2M) and device-to-device (D2D), and forms a data volume that is far greater than the traditional mobile communication and wireless access [1]. Therefore, the shortage of spectrum resources becomes a bottleneck for the IoT development. A reliable and efficient technology, called as the cooperative cognitive radio (CCR), greatly improves the spectral efficiency of IoT applications. In CCR-based IoT, a secondary user (SU) is asked to assist primary users (PUs) to achieve primary signal transmission. In return, the SU can get a certain spectrum as a reward to transmit its own data [2, 3]. In this case, the opportunistic access for SUs can promote spectrum utilization significantly [4, 5].

Yet, an IoT system contains a large number of low-cost devices that may only be powered by batteries [6, 7]. These energy-limited devices, usually in the edge of a network [8], may cause cooperative communication to not work properly. Accordingly, some works introduce energy-harvesting (EH) technology to solve such restriction and achieve better energy efficiency [9, 10]. This technology can realize the reuse of energy resources. An SU with EH technology can harvest energy from the ambient environment [11, 12], e.g., solar energy, thermal energy, and sound energy. Additionally, it can also harvest energy from the surrounding electromagnetic field generated by other communication nodes, which is defined as the wireless powered communication (WPC) technology [13]. The WPC-enabled SU is powered by radio frequency (RF) signals in the electromagnetic field and can convert the RF signals into a direct current that can be used in subsequent communications. As a result, the EH technology may increase the battery life of SUs by replenishing energy from various energy sources [14] and SUs can assist PUs without consuming additional

*Correspondence: yhuo@bjtu.edu.cn

School of Electronics and Information Engineering, Beijing Jiaotong University, Shangyuan, Beijing 100044, People's Republic of China

energy to achieve secure and reliable cooperative data transmission.

The WPC technology is widely used in wireless communication systems. One of the most popular research topics is the application of simultaneous wireless information and power transfer (SWIPT) technology to relay networks. Specifically, for a two-hop cooperative network, a relay employs a part of the received source signals for energy harvesting in the first phase of communication and the remaining is forwarded in the second phase. However, the harvested energy of the relay may be very limited due to the constraints of time slot and low EH conversion efficiency. Thus, this model can only be applied to near field communications. In order to use more energy for cooperative communications, multi-slot EH technology can be utilized. In the multi-slot mode, the energy harvested in each time slot can be accumulated in a battery and used for data transmission when the battery's energy exceeds a certain threshold. Thus, primary data transmission can be assisted by using multiple multi-slot EH-enabled SUs.

In this paper, we study the optimal single-relay selection problem for the energy-limited CCR-based IoT and then analyze the outage performance of PUs. To the best of our knowledge, this is the first time to discuss a relay selection strategy based on multi-slot EH for CCR-based IoT. Compared with traditional relay selection strategies, our proposed strategy is based on both SUs' channel state information (CSI) and battery state information (BSI). In addition, the selected SU as a relay adopts the amplify-and-forward (AF) mode rather than the decode-and-forward (DF) model in [15–18]. Different from the assumption of the infinite battery capacity in [19], we set the SUs' battery capacity is limited to satisfy the actual requirements. In our analysis, we formulate the accumulation process of SUs' battery energy as a finite state Markov chain to obtain the steady-state probability of BSI. However, we cannot fully guarantee the credibility and integrity of primary data forwarding due to the existing non-authorized SUs. An untrusted SU may spoof PUs by pretending to be a relay in exchange for its own data opportunistic transmit [20]. In this case, the outage probability of primary transmission may increase significantly. More seriously, the untrusted SU may cause various malicious behaviors, e.g., poisoning signals injection [21, 22], phishing attacks [23, 24], or private information leakage [25, 26]. Therefore, we analyze the outage probability of our relay selection strategy for the scenarios of trusted and untrusted SUs. When SUs are untrusted, we design a destination-assisted jamming strategy to ensure secure primary communication, and provide a Vickrey auction-based secondary system relay selection strategy to encourage SUs cooperation [27].

The main contributions of the paper are summarized as follows.

- We propose a relay selection strategy based on CSI and BSI. This strategy can select an SU from several multi-slot EH-enabled SUs as a relay to assist primary data transmission. Modeling the energy accumulation process of SU's battery as a finite state Markov chain, we can finally achieve PUs' reliable transmission without consuming SUs' additional energy.
- We analyze the outage probability of primary data transmission in the case of trusted and untrusted SUs. When SUs are trusted, we derive the theoretical analysis expression and the lower bound expression of outage probability. For the untrusted SUs, we propose a destination-assisted jamming strategy to ensure secure communication.
- For the EH-enabled secondary system in CCR-based IoT, we propose a Vickrey auction-based relay selection strategy. SUs without direct links can employ other EH-enabled SUs as relays to conduct secondary data transmission. These EH-enabled SUs bid as relays to gain rewards.
- The experiments of this paper is carried out on MATLAB platform. The relevant parameters are set according to the real wireless environment. The observation demonstrate excellent outage probability in both trusted and untrusted scenarios when using our strategy. This paper further exploits similar network parameters to analyze the secondary data forwarding rate based on the Vickrey auction and verifies the personal rationality of secondary users.

The rest of the paper is organized as follows. In Section 2, we review the related work, and then, the network model and necessary preliminaries are presented in Section 3. The relay selection strategy and the Markov model of SU's battery are illustrated in Section 4. Next, Section 5 analyzes the outage probability of the system. In Section 6, we propose a Vickrey-auction-based relay selection strategy for secondary systems. Finally, we analyze and discuss the performance of our work in Sections 7 and 8, and conclude our work in Section 9.

Notations: In this paper, we denote upper-case and lower-case bold letters as matrices and vectors, respectively. $\sqrt{\cdot}$ and $|\cdot|$ stand for the square root and the absolute value of a vector. $E[\cdot]$ represents the statistical expectation of random variables.

2 Related work

WPC technology generally appears in three basic network models, namely wireless power transfer networks (WPTNs), wireless powered communication networks (WPCNs), and SWIPT-enabled networks. In WPTNs,

there exists a dedicated RF transmitter to power the EH-enabled devices. These devices can receive sufficient and uninterrupted power. Obviously, this mode should be applied to the network with high system performance requirements [28]. And in WPCNs, a dedicated RF transmitter powers an EH-enabled device and the device uses the harvested energy to communicate with the RF transmitter. In addition, another SWIPT-based mode is the upsurge of current research. Since the RF signal carries information and energy at the same time, this mode can harvest energy from part of the received signals and use this energy to forward the remaining part of the received signals.

For the SWIPT technology, there exist two practical relay policies to achieve energy harvesting and information processing, i.e., power splitting relaying (PSR) and time switching relaying (TSR). Gao in [29] suggested selecting a SWIPT-enabled SU as a relay to maximize system throughput with the energy constraint and the requirement of the signal to interference plus noise ratio (SINR). In [30], Salem and Hamdi analyzed the secrecy capacity of an AF multi-antenna network with a SWIPT-enabled relay. The authors in [31] provided the maximal secrecy rate with the assistance of several SWIPT-enabled relays which are capable of simultaneous interference. Furthermore, Raghuvanshi et al. [32] discussed the secrecy performance of a dual-hop cognitive radio network (CRN) with a SWIPT-enabled relay.

Yet, the assumptions of existing EH-based works are too idealized. They always assume that only one time slot is used to harvest energy and the EH efficiency is high. In practice, the energy harvested in one time slot is very limited, and the EH efficiency is very low¹. Therefore, it is difficult to ensure the reliability of the system with EH-enabled relays or jammers for the single-slot harvesting mode. Instead of using the energy harvested in one transmission slot to immediately send data, we store the harvested energy with the help of a battery and adaptively used for transmissions. This mode is called as the multi-slot EH technology that have investigated in many articles [15–18, 33]. In [15], Zhou et al. proposed a multi-slot EH-based PSR strategy with distributed beamforming for wireless powered multi-relay cooperative networks. Intuitively, relay (jammer) selection based on the energy status in multi-slot EH-based networks is a question worth exploring. In [16], the authors separately studied the problem of single-relay and multi-relay selection in a distributed wireless powered cooperative communication (WPCC) network. They formulated the energy accumulation process of relays as a two-state Markov chain and analyzed the outage performance of the system. Unlike [16], the authors in [17] studied the outage performance of a multi-relay selection strategy based on an energy threshold in a WPCC network. They modeled the relay energy

accumulation process as a finite state Markov chain. Actually, the single-relay optimal selection is more reasonable and environment-friendly than the multi-relay selection in the energy-limited WPCC networks. Therefore, the authors in [18] studied the single-relay selection problem in a basic two-hop communication model. In addition, most articles analyzed the DF relay selection problem in WPCC networks. Nevertheless, the AF mode requires lower processing power and complexity at the relay node than the DF mode, but little works discussed the AF single relay selection problem [33], which inspired the work of this article.

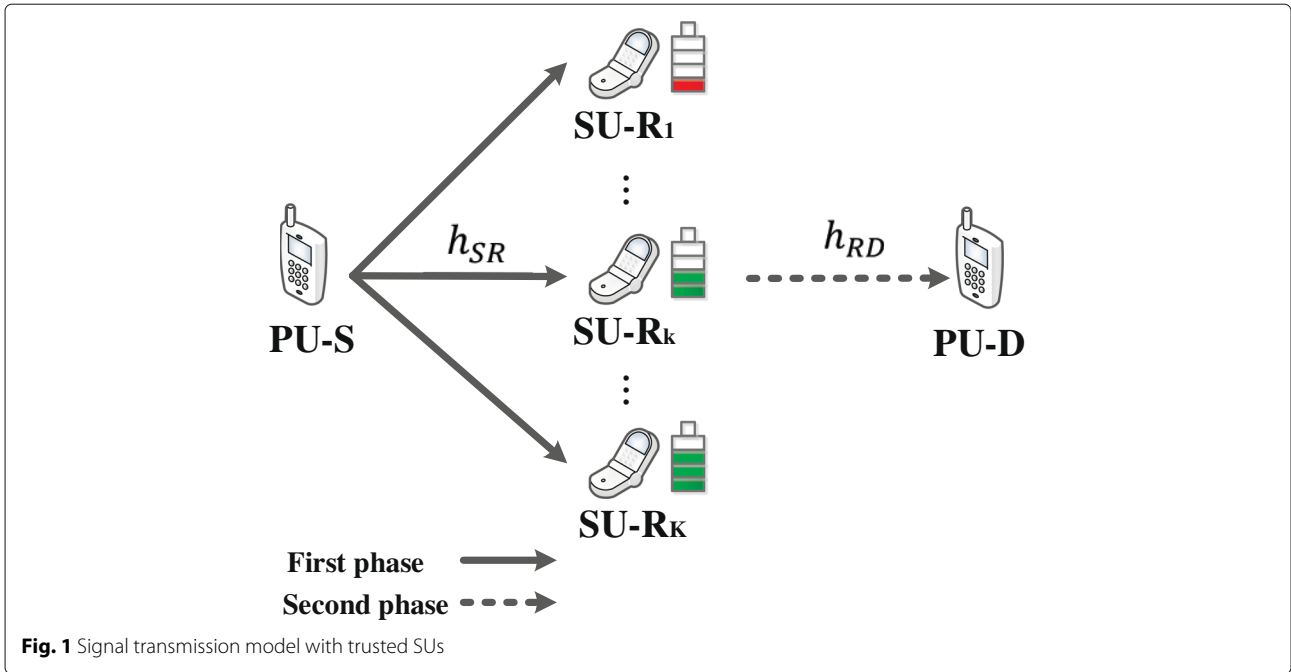
3 Network model

In this paper, we consider a CCR-based IoT that consists of a pair of PUs and K SUs as depicted in Figs. 1 and 3. All nodes are equipped with a single antenna and operate in half-duplex mode. We assume that the direct link between two PUs does not exist due to deep fading or obstacles. One PU as a source, abbreviated as $PU - S$, can only communicate with its destination, i.e., $PU - D$, via a relay ($SU - R$) selected from the K SUs. Here, SUs are considered as low-power devices and they can be powered by RF signals sent by $PU - S$. Each SU equipped with a RF-EH circuitry can convert the received RF power into direct current that can be recharged in a finite-size battery. For simplicity, all batteries have unified capacity of E_{\max} energy units. We consider two scenarios, namely trusted SUs and untrusted SUs, and introduce them separately in the following subsections.

Moreover, other network parameters are defined as follows. The wireless channel between nodes i and j experience a quasi-static Rayleigh block fading with the channel fading coefficient $h_{i,j}$. In other words, these channels remain constant within a time slot and obey independent complex Gaussian distribution, e.g., $h_{i,j} \in CN(0, d_{i,j}^{-\alpha})$. Thus, the channel gain $g_{i,j} = |h_{i,j}|^2$ is exponentially distributed with mean $\bar{g}_{i,j} = 2d_{i,j}^{(-\alpha)}$, where $d_{i,j}$ is the Euclidean distance between nodes i and j , and α represents the path loss factor. Assuming SUs are located closely, we have $\bar{g}_{S,R_i} = \bar{g}_{S,R}$, $\bar{g}_{D,R_i} = \bar{g}_{R_i}$, $D = \bar{g}_{D,R}$.

3.1 Network model with trusted SUs

The network model with trusted SUs is depicted as Fig. 1. When all SUs are trustworthy, the time slot T of entire transmission duration is divided into two phases, as shown in Fig. 2. Without loss of generality, we consider a normalized transmission time slot (i.e., $T = 1$). In the first phase, $PU - S$ transmits its private signals s_1 to SUs. The selected $SU - R$, e.g., $SU - R_l$, receives the signals, and the other SUs harvest energy from the received signals. In the second phase, $SU - R_l$ employs the AF mode



to forward the signals to $PU - D$, and the other SUs keep in idle mode².

According to the description of our transmission model, we provide mathematical expressions of signal transmission in two phases.

In the first phase, the received signals at $SU - R_k$ can be expressed as follows,

$$y_{R_k} = h_{S,R_k} s_1 + n_{R_k}, \tag{1}$$

where n_{R_k} is the additive white Gaussian noise (AWGN) at $SU - R_k$. If an SU not be selected as a relay, it is in the EH mode, and the amount of harvested energy at the $SU - R_k$ can be expressed as:

$$E_k = \frac{\eta}{2} P_S g_{S,R_k}, \tag{2}$$

where $P_S \triangleq E[s_1^2]$ is the transmit power of $PU - S$, and $0 \leq \eta \leq 1$ denotes energy harvesting efficiency which depends on the EH circuitry and the rectification process.

If an SU is selected as the best relay (i.e. $SU - R_l$), it is in the signal processing mode.

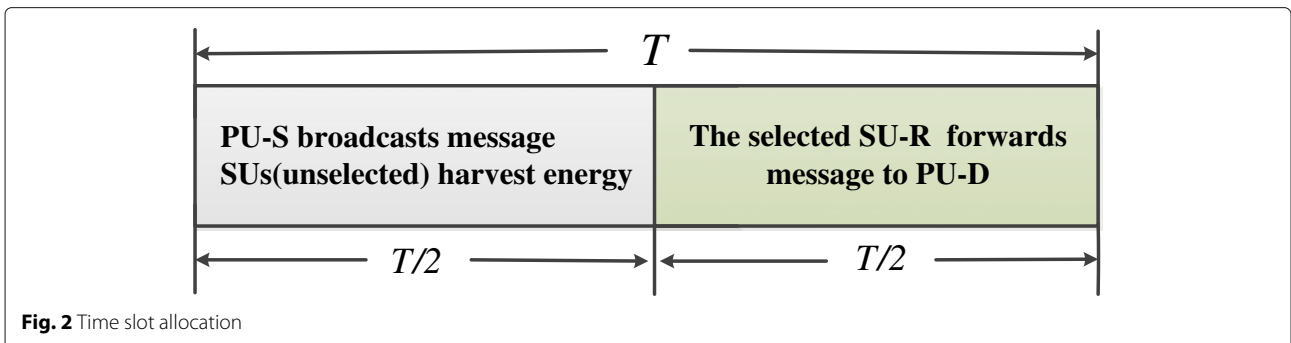
In the second phase, the selected relay is in the information forward (IF) mode. $SU - R_l$ amplifies and forwards signals $s_2 = \rho y_{R_l}$ to $PU - D$. Here, ρ is an amplification factor that can be defined as below:

$$\rho = \sqrt{\frac{P_R}{P_{S,R_l} + \sigma^2}}. \tag{3}$$

Therefore, the received signals at $PU - D$ is as follows:

$$\begin{aligned} y_D &= h_{R_l,D} \rho y_{R_l} + n_D \\ &= h_{R_l,D} \rho (h_{S,R_l} s_1 + n_{R_l}) + n_D, \end{aligned} \tag{4}$$

where $P_R \triangleq E[s_2^2]$ represents transmit power of $SU - R_l$ and $n_D^{(2)} \sim CN(0, \sigma^2)$ is AWGN at $PU - D$. According to the received signals of the second phase in (4), the corresponding SINR at $PU - D$ can be calculated by:



$$\gamma_D = \frac{\delta_{R_l,D} \delta_{S,R_l}}{\delta_{R_l,D} + \delta_{S,R_l} + 1}, \tag{5}$$

where $\delta_{i,j} = \frac{P_i g_{i,j}}{\sigma^2}$ is the signal to noise ratio (SNR). Thus, the channel rate is given by:

$$R_D = \frac{1}{2} \log_2 (1 + \gamma_D). \tag{6}$$

3.2 Network model with untrusted SUs

The network model with untrusted SUs has been slightly modified on the previous model, which is described in Fig. 3. Since SUs are non-authorized users, in many cases, we cannot ensure that they are completely reliable. As we know, the confidentiality of signals transmitted by $PU - S$ may be very high, and the SUs has no authority to know specific messages. Like many untrusted relay network definitions, in general, SUs are assumed trusted at the service level [34–37] but untrusted at the data level. Thus, the SU selected as relay may be able to eavesdrop the PU’s signals and other unselected SUs harvest energy³. Therefore, different from [16, 18], the selected SU exploits the AF mode in our network model. In addition, there is another reason that we have to exploit the AF mode is that the DF mode may greatly increase the risk of eavesdropping due to the decoding signals.

In order to avoid malicious behaviors (e.g., eavesdropping), we employ cooperative jamming schemes to deal with the untrusted relay. Signals to achieve cooperative jamming can be classified into the source-assisted method, friendly jammer-assisted one, and the destination-assisted one. The first one is designed based

on the principle that the legitimate signals and jamming signals are sent at the source simultaneously [38, 39]. The precondition for this method to be feasible is that the destination is aware of jamming signals. This requires additional channel resources to negotiate before communication. Then, the second one is to transmit jamming signals that only degrade the reception quality of eavesdroppers when the source or the relay transmits the legitimate signals [40, 41]. The disadvantage of this method is that the cooperative jamming-based secure transmission must have a trusted jammer. It may be difficult to achieve in reality due to selfishness of network nodes. In our work, we exploit the third one, i.e., the destination-assisted jamming methods, to design an anti-eavesdropping mechanism [42]. Here, we assume that $PU - D$ sends artificial noise (AN) to prevent eavesdropping when $PU - S$ sends legitimate signals.

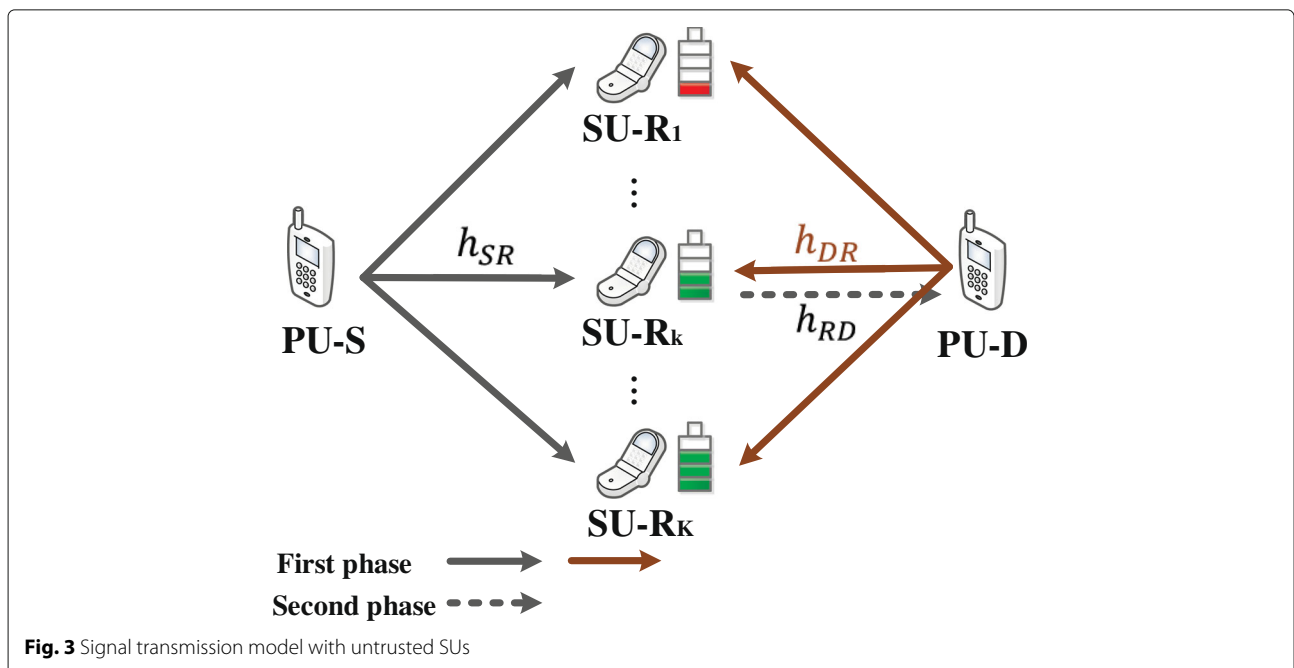
The time slot allocation in the untrusted scenario is shown in Fig. 4. In the first phase, $PU - S$ transmits its private signals s_1 to SUs, and $PU - D$ broadcasts AN v to prevent eavesdropping and provides additional energy sources simultaneously.

Specifically, the received signals in the first phase at $SU - R_k$ can be expressed as:

$$y_{R_k}^{(1)} = h_{S,R_k} s_1 + h_{D,R_k} v + n_{R_k}^{(1)}. \tag{7}$$

Thus, the amount of harvested energy at $SU - R_k$ can be derived as follows:

$$E_k = \frac{\eta}{2} (P_{S G_{S,R_k}} + P_{D G_{D,R_k}}), \tag{8}$$



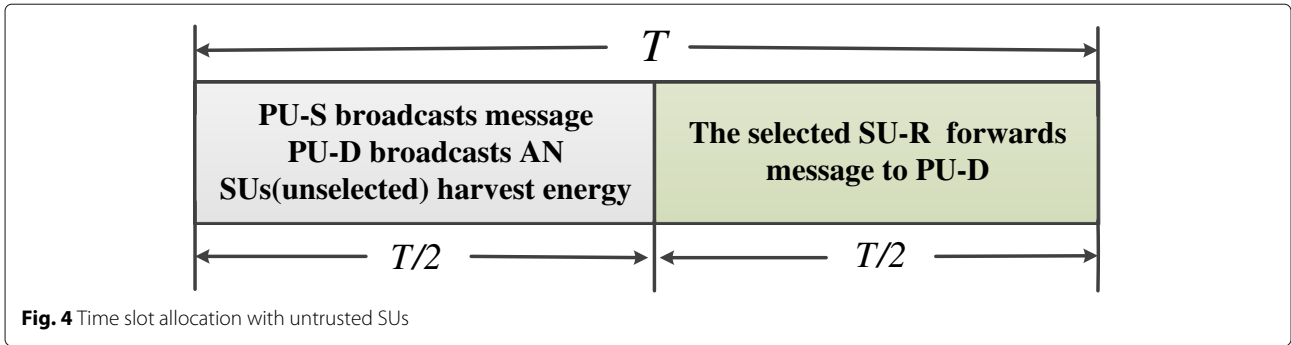


Fig. 4 Time slot allocation with untrusted SUs

where $P_S \triangleq E[s_1^2]$ and $P_D \triangleq E[v^2]$ are the transmit power of $PU-S$ and $PU-D$. According to (7), the SINR at $SU-R_l$ in the first phase is defined as:

$$\gamma_{R_l}^{(1)} = \frac{\delta_{S,R_l}}{\delta_{D,R_l} + 1}. \tag{9}$$

Similar to the trusted case, $SU - R_l$ will forward signals $s_2 = \rho y_{R_l}^{(1)}$ to $PU - D$ and the other SUs keep in the idle mode in the second phase. Thus, ρ can be defined as:

$$\rho = \sqrt{\frac{P_R}{P_{Sg_{S,R_l}} + P_{Dg_{D,R_l}} + \sigma^2}}. \tag{10}$$

Therefore, the received signals at $PU - D$ is as follows,

$$\begin{aligned} y_D^{(2)} &= h_{R_l,D} \rho y_{R_l}^{(1)} + n_D^{(2)} \\ &= h_{R_l,D} \rho (h_{S,R_l} s_1 + h_{D,R_l} v + n_{R_l}^{(1)}) + n_D^{(2)}, \end{aligned} \tag{11}$$

where $P_R \triangleq E[s_2^2]$ represents transmit power of $SU - R_l$ and $n_D^{(2)} \sim CN(0, \sigma^2)$ is AWGN at $PU - D$. Since v in $y_{R_l}^{(1)}$ is the AN transmitted by $PU - D$ itself in the first phase, we assume that $PU - D$ can easily remove the interference by self-interference cancelation (SIC) technology. As a result, (11) can be rewritten as follows:

$$y_D^{(2)} = h_{R_l,D} \rho (h_{S,R_l} s_1 + n_{R_l}^{(1)}) + n_D^{(2)}. \tag{12}$$

Then, the corresponding SINR at $PU - D$ can be calculated by:

$$\gamma_D^{(2)} = \frac{\delta_{R_l,D} \delta_{S,R_l}}{\delta_{R_l,D} + \delta_{S,R_l} + \delta_{D,R_l} + 1}. \tag{13}$$

According to [43], the secrecy rate is defined as the difference between the main channel rate and the eavesdropping channel rate. Thus, we can obtain the secrecy rate as follows:

$$R_S = [R_D - R_E]^+ = \frac{1}{2} \left[\log_2 \left(\frac{1 + \gamma_D^{(2)}}{1 + \gamma_{R_l}^{(1)}} \right) \right]^+, \tag{14}$$

where $[x]^+ = \max\{0, x\}$.

4 Relay selection and energy storage model

In this section, we propose a relay selection strategy when an SU is trusted or untrusted. Then, the charging and discharging process of an SU's battery is modeled as a finite state Markov chain and the analytical expression for steady-state distribution is derived.

4.1 Relay selection strategy

Unlike traditional relay selection (RS) strategies in [44, 45], our proposed RS strategy based on the CSI of wireless channels and SUs' BSI. At the beginning of a transmission time slot, each SU checks if the remaining energy of its battery reaches a energy threshold. Here, the energy threshold is defined as $E_{th} = P_R/2^4$. Then, SUs that satisfy the threshold condition constitute a subset Ω with cardinality $|\Omega|$. The subset Ω is defined as follows:

$$\Omega = \{SU_k | e_k \geq E_{th}, \forall k \in \{1, \dots, K\}\}, \tag{15}$$

where e_k donates the remaining energy of SU_k 's battery at the beginning of the transmission time slot.

Each SU in the subset Ω may send a pilot signal to $PU - S$, which contains their CSI⁵. According to the CSI, $PU - S$ can select the best SU as a relay to obtain the maximum channel rate R_D or the secrecy rate R_S . Therefore, $PU - S$ will notify all SUs the number of the selected SU when it broadcasts signals. And the selected SU will be in the IF mode, while the other SUs will be in the EH mode. In the trusted scenario, the selected SU can be expressed as:

$$SU - R_l = \arg \max_{SU_i \in \Omega} \{R_{D,i}\}. \tag{16}$$

And in the untrusted scenario, the selected SU can be expressed as:

$$SU - R_l = \arg \max_{SU_i \in \Omega} \{R_{S,i}\}. \tag{17}$$

With the proposed RS strategy, we can guarantee secure and reliable communication of PUs without using the additional energy of SUs. As we know, many works put forward various multi-relay selection methods. They will achieve more secure transmission performance at the cost of higher energy consumption. Obviously, they cannot achieve in the

limited energy CCR-based IoT due to the scarce energy. In addition, the multi-relay forwarding strategy need to apply the beamforming technology [17, 46]. This means that more resources need to be consumed to complete time synchronization and beamforming vector design, which will greatly increase the computational complexity. Therefore, in this paper, our RS strategy is designed to select one optimal relay.

4.2 Markov model of the SU's battery

In our battery model, the process of charging and discharging of the battery of an SU is an important part to achieve cooperative communication. In general, the charging or discharging behavior of an SU is a discrete-time stochastic process. Therefore, the battery life of SU_k at the beginning of each transmission time slot can be modeled as a finite-state discrete-time Markov chain (MC). Different from two states of the battery life (empty or full) mentioned in [16], we assume a finite state space $S = \{s_0, \dots, s_L\}$, where L denotes the number of discrete energy levels. We defined that $s_0 = 0$ and $s_1 = E_{max}/L$, which are referred as energy levels. The remaining energy of SU_k 's battery is $e_k = i \cdot s_1$ if SU_k is in state s_i . Moreover, the energy threshold is defined as $E_{th} = s_{th} = th \cdot s_1$, where $th \in \{1, \dots, L\}$.

The transition probability matrix of SU_k 's MC is defined as $\mathbf{P}^k = [p_{ij}^k]_{(L+1) \times (L+1)}$. Next, we provide the analysis of the transition probability from s_i to s_j of an arbitrary SU. For the sake of simplicity, we employ p_{ij} instead of p_{ij}^k in the following analysis.

4.2.1 The battery's state remains unchanged

$$(s_0 \leq s_i = s_j < s_L)$$

There are two reasons a battery's energy may remain unchanged.

- An SU belongs to subset Ω ($s_i \geq s_{th}$) but is not selected as a relay. Then, the SU is in EH mode and the energy harvested at this time slot is less than an energy level s_1 .
- An SU does not belong to subset Ω ($s_i < s_{th}$) and the energy harvested of the SU at this time slot is less than an energy level s_1 .

Thus, the transition probability is given by:

$$p_{i,i} = \begin{cases} \Pr[(SU \neq SU - R_l) \cap (s_i \leq s_i + E < s_{i+1})], & s_i \geq s_{th} \\ \Pr[s_i \leq s_i + E < s_{i+1}], & s_i < s_{th} \end{cases} \quad (18)$$

where E denotes the harvested energy of SU_k which is given by (2) and (8).

On one hand, we assume that each SU in Ω has an equal chance to be selected as the best relay with probability $\frac{1}{|\Omega|}$

if $s_i \geq s_{th}$. Here, we replace $\frac{1}{|\Omega|}$ by the lower-bound $\frac{1}{K}$ for simplicity. Therefore, the probability of a not selected SU in set Ω is $\frac{K-1}{K}$. The transition probability $p_{i,i}$ can be further derived as follows:

$$\begin{aligned} p_{i,i} &= \Pr[(SU \neq SU - R_l) \cap (s_i \leq s_i + E < s_{i+1})] \\ &= \Pr[SU \neq SU - R_l] \Pr[s_i \leq s_i + E < s_{i+1}] \\ &= \frac{K-1}{K} \Pr[0 \leq E < s_1] \\ &= \frac{K-1}{K} F_E(s_1), \end{aligned} \quad (19)$$

where $F_E(\cdot)$ is the cumulative distribution function (CDF) of variable E . The specific expression of $F_E(\cdot)$ is given by Lemma 1.

Lemma 1 For the trusted scenario, the CDF of E can be expressed as:

$$F_E(t) = 1 - e^{-\frac{t}{\bar{g}_S}}. \quad (20)$$

And that of E for the untrusted scenario is:

$$F_E(t) = 1 - \frac{\bar{g}_S}{\bar{g}_S - \bar{g}_D} e^{-\frac{t}{\bar{g}_S}} - \frac{\bar{g}_D}{\bar{g}_D - \bar{g}_S} e^{-\frac{t}{\bar{g}_D}}. \quad (21)$$

Proof Please see Appendix A. \square

On the other hand, when $s_i < s_{th}$, we can also derive the transition probability $p_{i,i}$ as follows:

$$\begin{aligned} p_{i,i} &= \Pr[s_i \leq s_i + E < s_{i+1}] \\ &= \Pr[0 \leq E < s_1] \\ &= F_E(s_1). \end{aligned} \quad (22)$$

4.2.2 The empty battery is partially charged

$$(s_0 = s_i < s_j < s_L)$$

When an SU's battery is in state s_0 , the SU must not belong to subset Ω , i.e., $s_i < s_{th}$. In this case, an empty battery is partially charged to level s_j only if the SU is in EH mode and the energy harvested at this time slot is between s_j and s_{j+1} . The transition probability can be calculated as follows:

$$\begin{aligned} p_{i,j} &= \Pr[s_j \leq s_i + E < s_{j+1}] \\ &= \Pr[s_j \leq E < s_{j+1}] \\ &= F_E(s_{j+1}) - F_E(s_j). \end{aligned} \quad (23)$$

4.2.3 The non-full battery is partially charged

$$(s_0 < s_i < s_j < s_L)$$

Similar to the unchanged state described in 4.2.1, there are two cases for this result.

- An SU belongs to subset Ω ($s_i \geq s_{th}$) but is not selected as a relay. Then, the SU is in EH mode and the energy harvested at this time slot is between $s_j - s_i$ and $s_{j+1} - s_i$.

- An SU does not belong to subset Ω ($s_i < s_{th}$), and the energy harvested of the SU at this time slot is between $s_j - s_i$ and $s_{j+1} - s_i$.

Thus, the transition probability is:

$$p_{i,i} = \begin{cases} \Pr[(SU \neq SU - R_l) \cap (s_j \leq s_i + E < s_{i+1})], & s_i \geq s_{th} \\ \Pr[s_j \leq s_i + E < s_{j+1}], & s_i < s_{th} \end{cases} \quad (24)$$

If $s_i \geq s_{th}$, the SU must belong to subset Ω . Similar to (19), the transition probability $p_{i,i}$ can be further expressed as:

$$\begin{aligned} p_{i,j} &= \Pr[(SU \neq SU - R_l) \cap (s_j \leq s_i + E < s_{j+1})] \\ &= \frac{K-1}{K} \Pr[s_{j-i} \leq E < s_{j+1-i}] \\ &= \frac{K-1}{K} (F_E(s_{j+1-i}) - F_E(s_{j-i})). \end{aligned} \quad (25)$$

And if $s_i < s_{th}$, the transition probability $p_{i,j}$ can be further expressed as:

$$\begin{aligned} p_{i,j} &= \Pr[s_j \leq s_i + E < s_{j+1}] \\ &= \Pr[s_{j-i} \leq E < s_{j+1-i}] \\ &= F_E(s_{j+1-i}) - F_E(s_{j-i}). \end{aligned} \quad (26)$$

4.2.4 The non-full battery is fully charged ($s_0 < s_i < s_j = s_L$)
A non-full battery is fully charged, there are two cases for this result.

- An SU belongs to subset Ω ($s_i \geq s_{th}$) but is not selected as a relay. Then, the SU is in EH mode and the energy harvested at this time slot is larger than $s_L - s_i$.
- An SU does not belong to subset Ω ($s_i < s_{th}$), and the energy harvested of the SU at this time slot is larger than $s_L - s_i$.

Thus, the transition probability is given by:

$$p_{i,i} = \begin{cases} \Pr[(SU \neq SU - R_l) \cap (s_L \leq s_i + E)], & s_i \geq s_{th} \\ \Pr[s_L \leq s_i + E], & s_i < s_{th} \end{cases} \quad (27)$$

When $s_i \geq s_{th}$, the SU must belong to subset Ω . The transition probability $p_{i,i}$ can be further expressed as:

$$\begin{aligned} p_{i,j} &= \Pr[(SU \neq SU - R_l) \cap (s_L \leq s_i + E)] \\ &= \frac{K-1}{K} \Pr[s_{L-i} \leq E] \\ &= \frac{K-1}{K} (1 - F_E(s_{L-i})). \end{aligned} \quad (28)$$

When $s_i < s_{th}$, the transition probability $p_{i,j}$ can be further expressed as:

$$\begin{aligned} p_{i,j} &= \Pr[s_L \leq s_i + E] \\ &= \Pr[s_{L-i} \leq E] \\ &= 1 - F_E(s_{L-i}). \end{aligned} \quad (29)$$

4.2.5 The empty battery is fully charged ($s_0 = s_i < s_j = s_L$)
This case happens only when an SU is in EH mode and the energy harvested at this time slot is larger than level s_L . Thus, the transition probability is given by:

$$p_{i,j} = \Pr[s_L \leq s_i + E] = \Pr[s_L \leq E] = 1 - F_E(s_L). \quad (30)$$

4.2.6 The battery remains fully charged ($s_0 < s_i = s_j = s_L$)
This case happens only when an SU belongs to subset Ω ($s_i \geq s_{th}$) but is not selected as the best relay. Thus, the transition probability can be given as:

$$p_{i,j} = \Pr[SU \neq SU - R_l] = \frac{K-1}{K}. \quad (31)$$

4.2.7 The battery is discharged ($s_0 < s_j < s_i \leq s_L$)
The battery discharge occurs only when an SU belongs to subset Ω ($s_i \geq s_{th}$) and is selected as the best relay. Additionally, it is true only when $s_j = s_i - s_{th}$ and the probability of everything else case is 0. Then, we can derive the transition probability for this case as follows:

$$p_{i,i} = \begin{cases} \Pr[SU = SU - R_l] = \frac{1}{K}, & s_i \geq s_{th} \cap s_j = s_i - s_{th} \\ 0, & s_i < s_{th} \cup (s_i \geq s_{th} \cap s_j \neq s_i - s_{th}) \end{cases} \quad (32)$$

Through the above analysis of all possible cases, we can easily obtain the transition probability matrix $\mathbf{P} \triangleq [p_{i,j}]_{(L+1) \times (L+1)}$ of any SU. In addition, through the above analysis, we can find that the transition probability matrix of each SU is consistent. The reason is that all the channels related to SUs are distributed identically, e.g., $\bar{g}_{S,R_i} = \bar{g}_{S,R}$ and $\bar{g}_{R_i,D} = \bar{g}_{D,R_i} = \bar{g}_{R,D}$. Since the above MC model is finite-state, irreducible, and positive recurrent, \mathbf{P} is irreducible and row stochastic. We define that $\boldsymbol{\pi} = (\pi_0, \pi_1, \dots, \pi_L)$ is the steady-state distribution vector of SU_k . With reference to [17], $\boldsymbol{\pi}$ can be found by solving a set of balance equations $\boldsymbol{\pi} = \mathbf{P}\boldsymbol{\pi}$ and the normalization equation $\sum_0^L \pi_i = 1$. Furthermore, we can obtain the unique steady-state distribution vector $\boldsymbol{\pi}$ by solving the following equation,

$$(\boldsymbol{\pi})^T = ((\mathbf{P})^T - \mathbf{I} + \mathbf{B})^{-1} \mathbf{b}, \quad (33)$$

where \mathbf{I} is a $(L+1) \times (L+1)$ unit matrix, \mathbf{B} is a $(L+1) \times (L+1)$ matrix with all elements are one, and \mathbf{b} is a $(L+1) \times 1$ vector with all elements are one.

5 Outage performance analysis

In order to evaluate the secrecy performance of our proposed model, we use the outage probability to evaluate system performance.

5.1 Outage analysis for the trusted scenario

When SUs are trusted, there may be only two cases in which an outage event occurs, i.e.,

- At the beginning of the transmission, there are no SU that satisfies the energy threshold. The subset Ω is empty, namely, $|\Omega| = 0$.
- The subset Ω is not empty, but the channel rate R_D achieved by using the selected relay is less than a certain rate R_{th} .

Hence, the outage probability can be expressed as follows:

$$P_{out} = \Pr[|\Omega| = 0] + \Pr[R_{D,i}^* < R_{th}|\Omega] \Pr[|\Omega| = k], \quad (34)$$

where $R_{D,i}^* = \max_{SU_i \in \Omega} R_{D,i}$ is the channel rate achieved by using the optimal relay in the set Ω . Here, $R_{D,i}$ is given by (6). The first item to the right of the above equation can be calculated as:

$$\Pr[|\Omega| = 0] = \left(\sum_{i=0}^{th-1} \pi_i \right)^K, \quad (35)$$

and the second item to the right can be given by:

$$\Pr[R_{D,i}^* < R_{th}|\Omega] \Pr[|\Omega| = k] = \sum_{k=1}^K \binom{K}{k} \left(\sum_{i=0}^{th-1} \pi_i \right)^{K-k} \left(\sum_{i=th}^L \pi_i \right)^k \{\Pr[R_D < R_{th}]\}^k, \quad (36)$$

where K is the total number of SUs. $\Pr[R_D < R_{th}]$ is the traditional outage probability, i.e., the channel rate R_D is less than the predetermined channel rate R_{th} . Obviously, $\Pr[R_D < R_{th}]$ can be converted to $\Pr[\gamma_D < \theta] = F_{\gamma_D}(\theta)$. Here, γ_D is given by (5), $\theta = 2^{2R_{th}} - 1$, and $F_{\gamma_D}(t)$ is the CDF of γ_D .

We aim to find the optimal SU that can achieve the maximum $\gamma_{D,i}$ in set $\Gamma = \{\gamma_{D,i}, i = 1, 2, 3 \dots k, k = |\Omega|\}$. Because the variables in Γ are independently and identically distributed, the equations of $f_{\gamma_{D,i}}(\theta) = f_{\gamma_D}(\theta)$ and $F_{\gamma_{D,i}}(\theta) = F_{\gamma_D}(\theta)$ hold, where $f_{\gamma_{D,i}}(\theta)$ is the probability density function (PDF) of $\gamma_{D,i}$. According to Section 2.2.2 in [47], we exploit the knowledge of order statistics to provide the PDF of the j^{th} smallest order statistics of Γ as follows,

$$f_{\Gamma}(\theta) = \frac{j!}{(j-1)!(k-j)!} \{F_{\gamma_D}(\theta)\}^{j-1} \{1 - F_{\gamma_D}(\theta)\}^{k-j} f_{\gamma_D}(\theta). \quad (37)$$

The maximum value means the k^{th} smallest value. If we define $j = k$, we can get the PDF of the maximum statistics, i.e.,

$$f_{\Gamma_{max}}(\theta) = k \{F_{\gamma_D}(\theta)\}^{k-1} f_{\gamma_D}(\theta). \quad (38)$$

And the CDF of the maximum order statistics of Γ can be easily derived by integrating the PDF in (42), which is given by:

$$F_{\Gamma_{max}}(\theta) = \{F_{\gamma_D}(\theta)\}^k. \quad (39)$$

And finally, we have:

$$\begin{aligned} \Pr[R_i^* < R_{th}|\Omega] &= \Pr \left[\max_{\substack{SU_i \in \Omega \\ |\Omega|=k}} R_{D,i} < R_{th} \right] \\ &= \Pr \left[\max_{\substack{SU_i \in \Omega \\ |\Omega|=k}} \gamma_{D,i} < \theta \right] = \{F_{\gamma_D}(\theta)\}^k \\ &= \{\Pr[R_D < R_{th}]\}^k. \end{aligned} \quad (40)$$

Next, we will provide an integral form, a closed-form, and a lower bound of $\Pr[R_D < R_{th}]$.

For the sake of simplicity, we define $X = \delta_{R_i, D} = \frac{P_{R_i} g_{R_i, D}}{\sigma^2}$ and $Y = \delta_{S, R_i} = \frac{P_{S} g_{S, R_i}}{\sigma^2}$. Since $g_{R_i, D}$ and g_{S, R_i} are random variables that obey exponential distribution, X and Y are exponentially distributed with mean $\bar{x} = \frac{P_{R_i} \bar{g}_{R_i, D}}{\sigma^2}$ and $\bar{y} = \frac{P_S \bar{g}_{S, R_i}}{\sigma^2}$. Thus, we can easily derive that $\gamma_D = \frac{XY}{X+Y+1}$. And the integral form of $\Pr[R_D < R_{th}]$ can be expressed as follows:

$$\begin{aligned} &\Pr[R_D < R_{th}] \\ &= \Pr \left[\frac{XY}{X+Y+1} < \theta \right] \\ &= \Pr \left[X < \frac{\theta Y + \theta}{Y - \theta} \right] \\ &= \int_0^{+\infty} F_X \left(\frac{\theta y + \theta}{y - \theta} \right) \cdot f_Y(y) dy \\ &= \frac{1}{\bar{y}} \int_0^{+\infty} \left[1 - \exp \left(-\frac{\theta y + \theta}{y \bar{x} - \theta \bar{x}} \right) \right] \cdot \exp \left(-\frac{y}{\bar{y}} \right) dy \\ &= 1 - \frac{1}{\bar{y}} \int_0^{+\infty} \exp \left(-\frac{\theta y + \theta}{y \bar{x} - \theta \bar{x}} - \frac{y}{\bar{y}} \right) dy, \end{aligned} \quad (41)$$

where $F_X(\cdot)$ is the CDF of X and $f_Y(\cdot)$ is the PDF of Y .

However, (41) is extremely complicated for actual calculations. It is difficult to obtain the final result using

existing mathematical calculation software. To cope with this challenge, we can derive the PDF and the CDF of γ_D according to [48], i.e.,

$$\begin{aligned}
 f_{\gamma_D}(\gamma_D) &= \frac{2}{\bar{x} \cdot \bar{y}} e^{-\frac{\gamma_D(\bar{x}+\bar{y})}{\bar{x}\bar{y}}} \\
 &\times \left[\left(\sqrt{\frac{\bar{y}}{\bar{x}}} + \sqrt{\frac{\bar{x}}{\bar{y}}} \right) \sqrt{\gamma_D(\gamma_D + 1)} \right. \\
 &\times K_1 \left(2\sqrt{\frac{\gamma_D(\gamma_D + 1)}{\bar{x} \cdot \bar{y}}} \right) \\
 &\left. + (2\gamma_D + 1) \times K_0 \left(2\sqrt{\frac{\gamma_D(\gamma_D + 1)}{\bar{x} \cdot \bar{y}}} \right) \right], \tag{42}
 \end{aligned}$$

and

$$\begin{aligned}
 F_{\gamma_D}(\gamma_D) &= 1 - 2e^{-\frac{\gamma_D(\bar{x}+\bar{y})}{\bar{x}\bar{y}}} \\
 &\times \sqrt{\frac{\gamma_D(\gamma_D + 1)}{\bar{x} \cdot \bar{y}}} \cdot K_1 \left(2\sqrt{\frac{\gamma_D(\gamma_D + 1)}{\bar{x} \cdot \bar{y}}} \right), \tag{43}
 \end{aligned}$$

where $K_0(\cdot)$ and $K_1(\cdot)$ are the zero-order and the first-order modified Bessel function of the second kind. The specific solution of (42) and (43) is to first obtain the PDF and CDF of γ_D under Nakagami- m fading. And let the fading factor of x and y equal to 1 ($m_x = m_y = 1$); then, Nakagami- m fading becomes Rayleigh fading. Accordingly, we can get the above formulas by substituting $m_x = m_y = 1$ into the PDF and CDF of γ_D under Nakagami- m fading. The closed-form of $\Pr[R_D < R_{th}]$ is as follows:

$$\Pr[R_D < R_{th}] = \Pr[\gamma_D < \theta] = F_{\gamma_D}(\theta). \tag{44}$$

Furthermore, we provide the closed-form expression of the lower bound of $\Pr[R_D < R_{th}]$ in Lemma 2.

Lemma 2 We assume that P_{out}^{LB} is the lower bound of $\Pr[R_D < R_{th}]$, i.e.,

$$P_{out}^{LB} = 1 - 2e^{-\frac{\theta(\bar{x}+\bar{y})}{\bar{x}\bar{y}}} \times \theta \sqrt{\frac{1}{\bar{x} \cdot \bar{y}}} \cdot K_1 \left(2\theta \sqrt{\frac{1}{\bar{x} \cdot \bar{y}}} \right). \tag{45}$$

Proof Please see Appendix B. □

5.2 Outage analysis for the untrusted scenario

When SUs are untrusted, the reason for the interruption time is the same as the above. Hence, the outage probability can be expressed as follows:

$$P_{out} = \Pr[|\Omega| = 0] + \Pr[R_{S,i}^* < R_{th}|\Omega] \Pr[|\Omega| = k], \tag{46}$$

where $R_{S,i}^* = \max_{SU_i \in \Omega} R_{S,i}$ is the channel rate achieved by using the optimal relay in the set Ω . Here, $R_{D,i}$ is given by (14). The first term to the right of (46) is the same as that of (35), and the second term to the right of (46) can be given by:

$$\begin{aligned}
 &\Pr[R_{S,i}^* < R_{th}|\Omega] \Pr[|\Omega| = k] = \\
 &\sum_{k=1}^K \binom{K}{k} \left(\sum_{i=0}^{th-1} \pi_i \right)^{K-k} \left(\sum_{i=th}^L \pi_i \right)^k \{\Pr[R_S < R_{th}]\}^k, \tag{47}
 \end{aligned}$$

where $\Pr[R_S < R_{th}]$ denotes that the secrecy rate R_S is less than the predetermined secrecy rate R_{th} . Obviously, it is very difficult to get an integral form or a closed-form expression of $\Pr[R_S < R_{th}]$ because there exist three random variables in R_S . We will give the results in subsequent simulations results section.

6 Vickrey auction-based secondary system relay selection strategy

After assisting a PU, the selected SU will obtain a certain amount of time to occupy the PU's spectrum to achieve its own data transmission. In our work, we not only consider the above transmission strategy of PUs in energy-limited CCR-based IoT, but also investigate the secure and reliable transmission strategy of SUs. In the former case, PUs employ an SU as a relay to assist their communication, and the spectrum resource is used as a reward for the SU. However, in the latter case, the SUs are all rational users, and they do not voluntarily consume limited energy to assist other SUs in their transmission. In general, cooperation among them should be based on the improvement of their own earnings. Thus, we will propose a secondary system relay selection strategy based on Vickrey auction in this section.

In general, the Vickrey auction combines advantages of the English auction and the sealed price auction [27]. Theoretically, it is an effective auction mechanism because the optimal strategy for each candidate is based on the valuation of the subject matter. This is obviously a trading method that conforms to the principle of incentive compatibility. Moreover, since an auction is ultimately obtained by the bidder with the highest willingness to pay, it is also a configuration mechanism that enables the buyer and the seller to achieve Pareto optimality.

In our system, the secondary system is decentralized. We exploit Bitcoin mechanism to achieve an auction incentive. The original intention of this approach is that Bitcoin is a decentralized peer-to-peer(P2P) digital currency [49]. With the idea of blockchain in Bitcoin [50, 51], we can implement decentralized credit-based P2P transactions in distributed systems without mutual trust, by means of data encryption, time stamping, distributed consensus, and economic incentive. Thus, the blockchain

technology ensures the normal and reliable circulation of Bitcoin.

Introducing the Bitcoin mechanism, in our work, the secondary system model is composed of a pair of SUs (SU-S and SU-D) that need to communicate with each other and K energy-limited relays (SU-Rs). Similar to the description in primary system, SU-S wants to communicate with SU-D. Yet, there does not exist a direct link between SU-S and SU-D due to deep fading or obstacles. Thus, it is necessary to employ another SU to be a relay to assist the secondary pair users communication. In our system, relays are all EH-enabled SUs and their battery energy should be harvested from the surrounding RF signals. The calculation process of the system channel rate is similar to Section 3.1, where the results are given directly below,

$$\begin{aligned} R_D^{SU} &= \frac{1}{2} \log_2 \left(1 + \gamma_D^{SU} \right) \\ &= \frac{1}{2} \log_2 \left(1 + \frac{\delta_{R,D}^{SU} \delta_{S,R}^{SU}}{\delta_{R,D}^{SU} + \delta_{S,R}^{SU} + 1} \right), \end{aligned} \quad (48)$$

where $\delta_{i,j}^{SU} = \frac{p_i^{SU} g_{i,j}^{SU}}{\sigma^2}$ is the corresponding SNR.

In the Vickrey auction, the bidder that submits the lowest bid wins the auction, but the auctioneer pays the second-lowest amount bid to the winner. Here, we define that the auctioneer is SU-S and the bidders are K candidate relays. And the characteristic of bidders are the CSI between SU-S and SU-D, e.g., $g_{S,R}^{SU}$ and $g_{R,D}^{SU}$. Then, we provide the valuation of bidder R_i as follows:

$$v_i = E_i | \left(R_{D,i}^{SU} = R_{D,th}^{SU} \right), \quad (49)$$

where $R_{D,i}^{SU}$ denotes the channel rate of SU-D when using R_i as a relay and $R_{D,th}^{SU}$ is the expected channel rate of SU-D. E_i represents the energy that the relay R_i needs to consume when satisfying the channel rate requirement of SU-S. Each relay calculates the corresponding bid b'_i according to its own E_i based on a certain unit price rule, and:

$$b_i = \begin{cases} 0, & \text{if } E_i > e_i \\ 0, & \text{if } E_i \leq e_i \text{ and } b'_i > b_0, \\ b'_i, & \text{if } E_i \leq e_i \text{ and } b'_i \leq b_0 \end{cases}, \quad (50)$$

where e_i indicates the remaining battery energy of the R_i at this time and b_0 is the upper payment of SU-S. Therefore, $B = \{b_1, b_2 \cdots b_K\}$ is the bidding set of relays.

In auctions, we need to ensure both the user's integrity and the user's personal rationality. Integrity means that regardless of other bidders' bid, the user's optimal strategy is given the honest bid, and false prices cannot improve their own utility. Intuitively, integrity is used to ensure that the auction process is fair and effective. Personal rationality means that the auctioneer's and bidder's utilities are positive. It is used to ensure the enthusiasm of the auction

parties in participating in the auction. We will explain the details of this two requirements separately below.

Integrity: Vickrey auction guarantees the integrity of the auction users. In other words, for the relay selection strategy proposed by this section based on the Vickrey auction, the only dominant strategy is that all relays honestly bid. Next, we will give the corresponding proof. According to the principle of Vickrey auction, we assume that R_i 's bid b_i is the lowest price, and R_j 's bid b_j is the second lowest price (where the relay whose bid is 0 does not participate in the bid because its energy is not enough). Thus, R_i is the winning relay and its utility function can be expressed as:

$$m_i = \begin{cases} \min\{b_0, b_j\} - b_i, & \text{if } b_i = \min\{b_1, b_2 \cdots b_K\} \\ 0, & \text{otherwise} \end{cases}. \quad (51)$$

Accordingly, there exist different behaviors of relays in various situations.

- When $b_i \neq b'_i$ and R_i loses the auction, the utility of R_i is 0.
- When $b_i > b'_i$ and R_i wins the auction, the utility of R_i is $b_j - b_i$ which is lower than $b_j - b'_i$, and R_i lost $b_i - b'_i$ compared to honest bid.
- When $b_i < b'_i$ and R_i wins the auction, the utility of R_i still $b_j - b'_i$, because R_i really consumes the energy of the corresponding value b'_i . Thus, the utility of R_i has not been improved. And even if R_j adopts the strategy of $b_j < b'_j$, the utility of R_i will decrease.

Personal rationality: From (51), we can see that relays always have non-negative utilities. Then, we can get the utility function of SU-S as:

$$R = \begin{cases} R_{D,th}^{SU}, & \forall b_i > 0, b_i \in B \\ 0, & \exists b_i = 0, b_i \in B \end{cases}. \quad (52)$$

Obviously, we can also find that SU-S always have a non-negative utility. Therefore, our auction strategy can guarantee the personal rationality of the auction parties. Next, we will specify the steps of the proposed relay selection strategy as follows.

- SU-S determines the expected channel rate $R_{D,th}^{SU}$, broadcasts it to all relays, and then waits for response.
- All candidate relays calculate their own E_i based on (48) and compare it to their own battery's remaining energy e_i . If $E_i > e_i$, the candidate may set its own bid $b_i = 0$. Otherwise, it calculates the corresponding bid b'_i according to a certain unit price rule. For b'_i , the candidate will set $b_i = 0$ if $b'_i > b_0$ and set $b_i = b'_i$ otherwise. Then, all relays sent their bids to SU-S.
- After receiving K bids, SU-S will perform the decision-making process. If all bids are 0, the transmission is terminated; if only one non-zero bid b_i , R_i is the winner and SU-S will pay R_i b_0 ; if there

are more than one non-zero bid, the candidate relay with the lowest bid is the winner and SU-S pays the second lowest price;

- SU-S broadcasts its messages which contains the number of the selected relay, and all relays will receive the messages. In this case, the winner assists SU-S to forward messages and others will harvest energy or complete its own services.

7 Numerical results

7.1 Analysis of PUs' outage performance

In this subsection, we will present numerical results via Monte Carlo simulation to evaluate the outage performance of PUs in CCR-based IoT. This network consists of a pair of PUs and some energy-harvesting-enabled SUs. For simplicity, unless otherwise noted, the simulation parameters are set in Table 1.

Figure 5a and b depict the outage performance of system with trusted SUs under different numbers of SUs and discrete energy levels. In the legend of these two figures, "Sim" indicates the results obtained by Monte Carlo simulation, "Ana" denotes the theoretical values obtained by (43), and "LB" represents the lower bound value given by Lemma 2. In these two figures, the results of exact analysis and the lower bound closely match the simulated results. Figure 5a demonstrates that the outage probability decreases gradually as the number of SUs increases. In addition, we can also find that the higher battery capacity E_{max} , the lower outage probability can be achieved. When $E_{max} = 20$ mW, the ideal outage performance (less than 10^{-4}) can be achieved if the number of SUs K is greater than 6. Yet, when $E_{max} = 10$ mW, the same performance can be achieved only when $K > 9$. In Fig. 7, we set $th = L/2 + 1$ and $E_{th} = E_{max}/2$. The result shows that the outage probability gradually decreases and tends to be

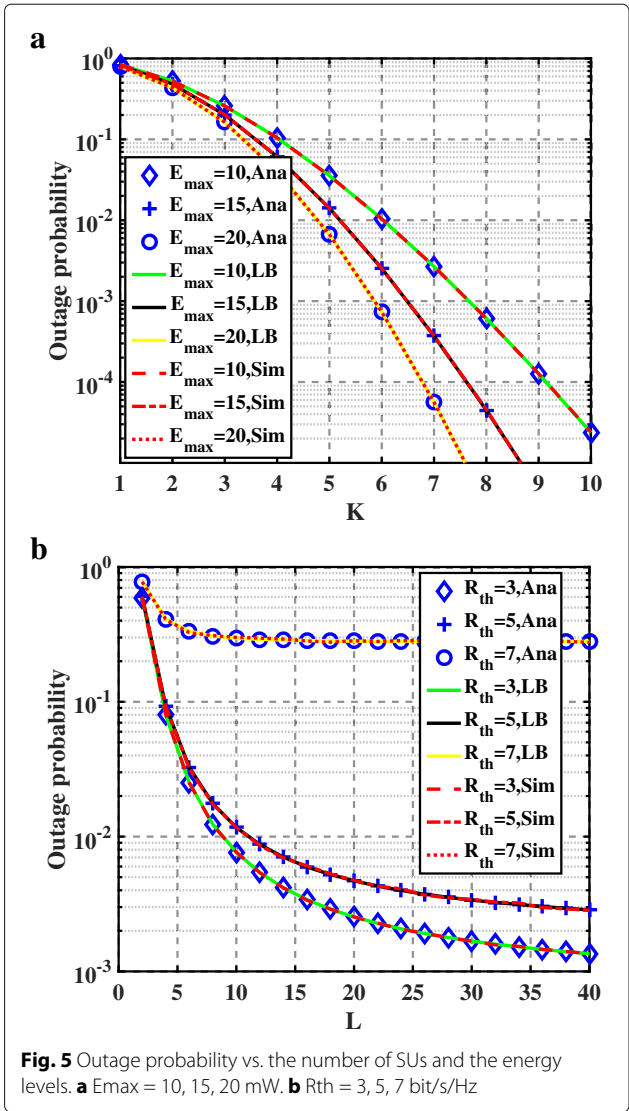


Fig. 5 Outage probability vs. the number of SUs and the energy levels. a $E_{max} = 10, 15, 20$ mW. b $R_{th} = 3, 5, 7$ bit/s/Hz

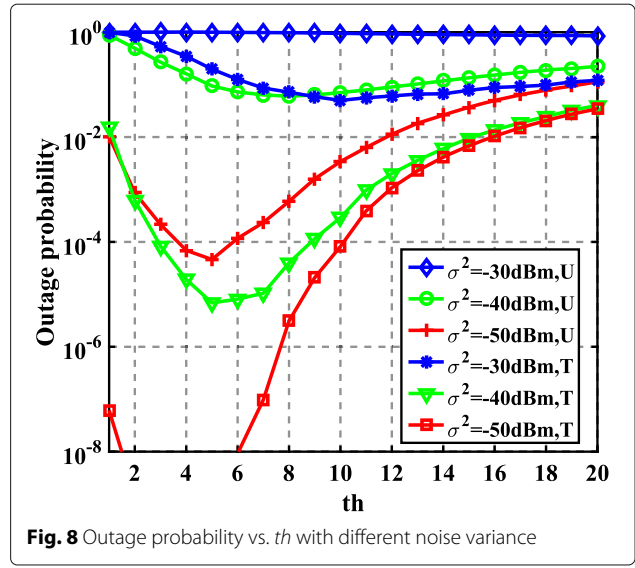
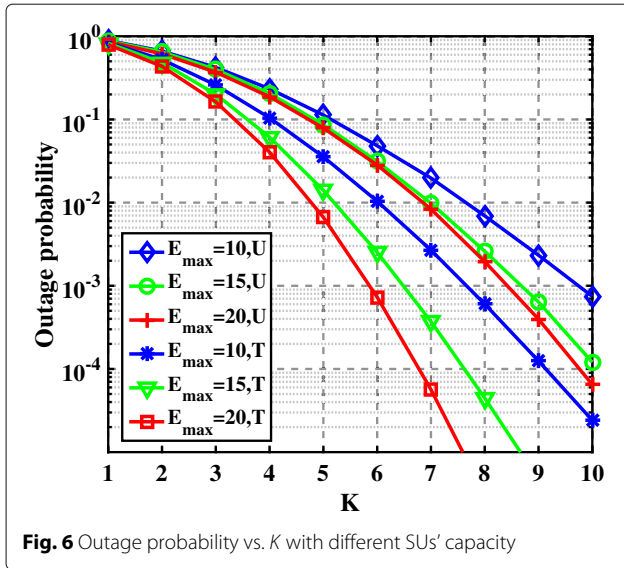
Table 1 Simulation parameters

Simulation parameter	Value
The transmit power for trusted scenario, P_S	200 mW
The transmit power for untrusted scenario, P_S	100 mW
The transmit power for untrusted scenario, P_D	100 mW
The noise variance, σ^2	-50 dBm
The number of SUs, K	6
The discrete energy levels, L	20
The unified capacity of SUs, E_{max}	15 mW
The energy-harvesting efficiency, η	0.5
The energy threshold, th	11
The distance between two PUs	10 m
The distance between $PU - S$ and $SU - R$, D_{SR}	4 m
The path loss factor, α	3
The predetermined rate, R_{th}	3 bit/s/Hz

stable as the energy discrete levels L increases. And the outage probability will increase as the predetermined rate R_{th} increases. When the given rate reaches 7 bit/s/Hz, the system outage is too high to work.

Figures 6, 7, and 8 compare the outage probability in the case of trusted and untrusted scenarios. In these figures, "T" indicates the trusted SUs, while "U" denotes the untrusted ones. Figure 6 shows the impact of the number of SUs K and the battery capacity E_{max} on the outage performance in the two scenarios. Obviously, the outage probability decreases gradually with the number of SUs increases. And we can increase the battery capacity E_{max} to improve the system performance.

The impact of EH efficiency η on outage probability is studied in Fig. 7 with different predetermined rate R_{th} . With the increase of η , the outage probability gradually decreases. Moreover, it can be seen that the outage

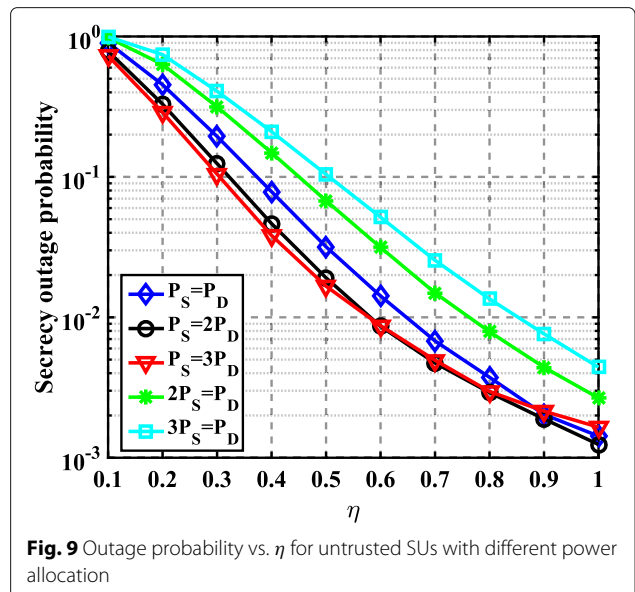
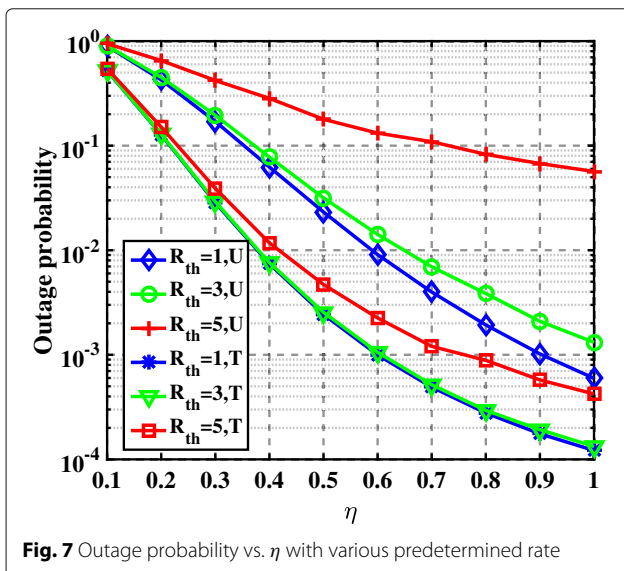


probability increases accordingly by increasing the predetermined rate R_{th} . In the case of trusted SUs, the curves for $R_{th} = 1$ bit/s/Hz and $R_{th} = 3$ bit/s/Hz are almost coincident. This can be interpreted as the effect of the predetermined rate R_{th} on the outage performance is very small at low predetermined rate case.

Figure 8 plots the effect of threshold energy levels th on outage performance in both cases. In this figure, we set different noise power $\sigma^2 = -30, -40, -50$ dBm. From the figure, we can see that the system is almost outage in untrusted SUs case when $\sigma^2 = -30$ dBm. In addition to the curve of $\sigma^2 = -30$ dBm, we can find the optimal value th on the other curves to achieve the lowest outage probability. And the optimal th also gradually decreases as the noise power decreases. The reason is that

the same secure performance can be achieved by using lower transmit power when noise power is lower. Thus, we can conclude that the outage performance achieved by trusted SUs is superior to that of untrusted SUs when consuming the same energy. This is because part of the system power has to be used to broadcast AN due to eavesdropping. Yet, according to our cooperative jamming strategy, we can still achieve excellent performance by adjusting the corresponding parameters when SUs are untrusted

Next, in Figs. 9 and 10, we study the effect of EH efficiency η on outage performance under different power allocations for the trusted and untrusted SUs. From Fig. 9, it can be observed that the outage performance achieved by different power allocation strategies is slightly different.



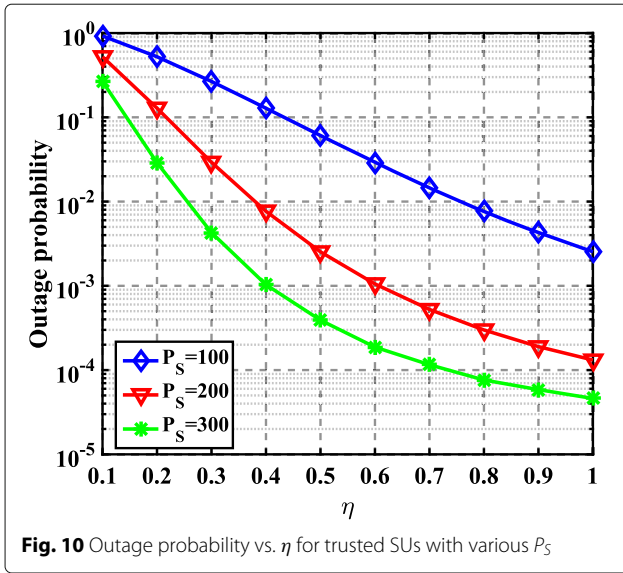


Fig. 10 Outage probability vs. η for trusted SUs with various P_S

When η is relatively small, we should exploit higher P_S to achieve lower outage probability. On the contrary, properly increasing P_D can achieve better outage performance when η is larger. However, we should allocate more energy to broadcast messages instead of AN because η is still relatively small in practice. And when SUs are fully trusted, all system power is used to transmit messages. Thus, the larger the P_S , the lower outage probability can be achieved, which can be showed in Fig. 10.

Finally, we provide the the impact of SNR on outage performance with different the distance between PU-S and SUs in Fig. 11. Here, we assume that $SNR = P/\sigma^2$ with $P = 20$ dBm and $\sigma^2 = 10 \sim -70$ dBm⁶. From this figure, we know that the system is completely outage if

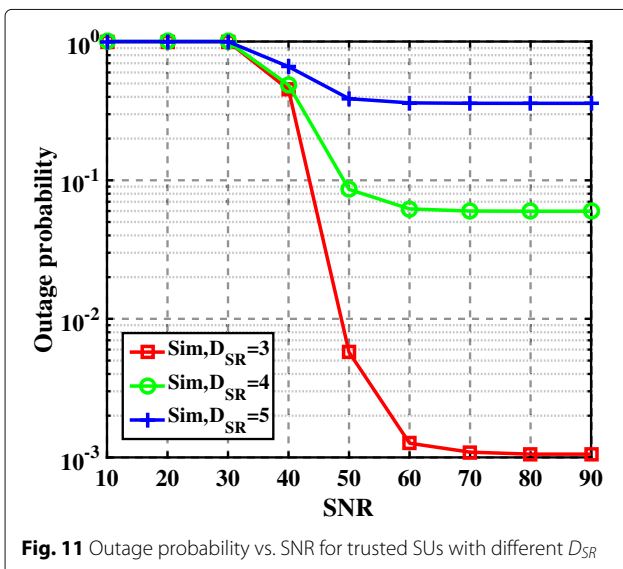


Fig. 11 Outage probability vs. SNR for trusted SUs with different D_{SR}

SNR is less than 30 dBm, and the outage probability gradually decreases and tends to be stable along with increasing SNR. In addition, we can also find that the closer the distance between SUs and PU-S is, the lower outage probability can be reached. Also, the larger SNR can obtain the more stable outage probability. This is because when an SU is closer to PU-S, it can harvest energy faster, which leads to the lower probability of energy shortage.

7.2 Analysis of Vickrey auction-based relay selection strategy

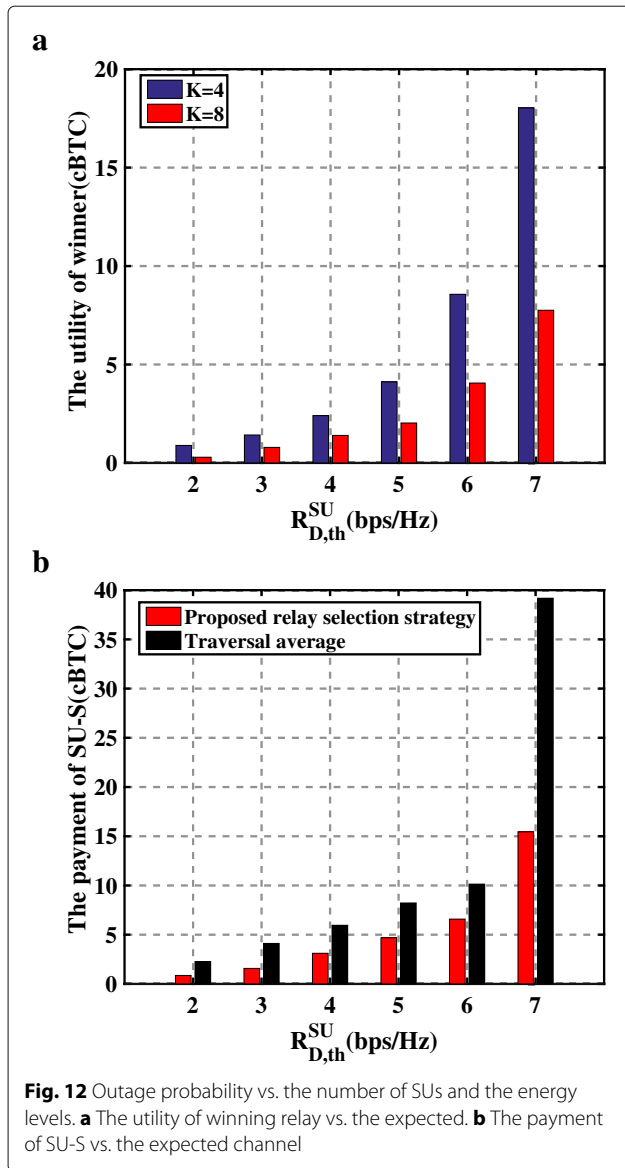
In this subsection, we analyze the performance of the secondary system with our proposed relay selection strategy based on Vickrey auction. This network consists of a pair of SUs and K energy-limited SU-Rs. The transmit power of SU-S and noise variance of the system are set to be 20 dBm and -50 dBm, respectively. In addition, the distance between two SUs is 10 m and the SU-Rs are located in the middle of two SUs. The path loss factor α is 3. For simplicity, we assume that the market price of 1 mW is 1 Bitcent in the following simulation figures⁷.

In Fig. 12a, the result shows the effect of the expected channel rate $R_{D,th}^{SU}$ of SU-S on the utility of the winning relay for different network scales. We can easily know that the utility of the winning relay is always positive no matter how the number of relays and the expected channel rate $R_{D,th}^{SU}$ change. This result also further verifies the personal rationality of bidders. Additionally, we can also find that when the number of relays increases, the utility of winning relay decreases. This result is quite reasonable because the auction competition becomes more intense when the number of relays increases, and the difference between the lowest bid and the second lowest bid is smaller. Furthermore, the utility of the winning relay also gradually increases along with increasing $R_{D,th}^{SU}$. This can be explained by the fact that when SU-S needs higher requirements, the difference between relays appear to be more pronounced, which may lead to different energy consumption.

The effect of the expected channel rate $R_{D,th}^{SU}$ on the auctioneer SU-S's payment is shown in Fig. 12b. In order to evaluate our proposed strategy, we define an average payment that is computed by traversing all relays. According to the figure, we know that the SU-S's payment may be growth when the expected channel rate $R_{D,th}^{SU}$ grows. Also, we can draw the conclusion that SU-S's payment is much smaller than the average one of traversal all the relays.

8 Discussion

According to the analysis of numerical results in Section 7, it is obviously to observe that the proposed strategy enables the CCR-based IoT the ability to cope with the secure forwarding problem and limited energy problem simultaneously. We can obtain excellent outage



performance of primary communication without consuming additional energy of selected secondary users. Therefore, this strategy is valuable for data transmission among low-end devices in IoT networks.

The experiments in this paper is carried out on MATLAB platform, and we exploit relevant parameters similar to a real wireless environment. Regardless of whether the trusted or untrusted SU acts as a relay node, the outage probability is only slightly different. The reason is that we employ different power allocation strategies for various scenarios. This observation may provide a unique vision to study data secure sharing among low-end devices with different attribute. In addition, it is worth noting that there is still an issue about secondary data exchanging due to the

lack of legal spectrum licences for low-end devices. Then, we analyze the effect of the expected secondary data rate on the utility of the winning relay based on the Vickrey auction. The results demonstrate the positive utility of the winner and also prove the personal rationality of a bidder during the auction.

Yet, the efficiency of energy conversion is still a bottleneck in EH-enabled CCR-based IoT. In future work, we would like to focus on improving the conversion efficiency and design scalable cooperative secure relays to enhance unit energy utilization.

9 Conclusions and future works

A relay selection strategy based on CSI and BSI in EH-enabled CCR-based IoT is proposed in this paper. Some low-end devices treated as SUs with EH capabilities can be selected as helpers of a pair of primary users. The outage probability is used to analyze transmission performance of PUs in both trusted and untrusted SU scenarios. When an SU is selected as a relay, it will be in IF state and the unselected SUs harvest energy from signals transmitted by PU-S. For untrusted SUs, we adopt a destination-assisted jamming strategy to prevent eavesdropping. And we formulate the energy accumulation process of SUs' batteries as a finite state Markov chain and derive the corresponding steady-state probability. For energy-limited secondary systems, we propose a relay selection strategy based on Vickrey auction. According to numerical results, we know that many parameters have effects on the outage performance of CCR-based IoT. Specifically, the outage probability is inversely proportional to the maximum battery capacity, the number of relays, the channel rate threshold, and the EH efficiency. And there exist the optimal energy threshold that can minimize the outage probability. Moreover, the accuracy of the theoretical analysis and the lower bound analysis are also confirmed via simulation results.

In this article, we assume that all CSI is perfectly known by using a channel estimation scheme. Yet, it is difficult to acquire the accurate CSI in wireless data transmission because of defects of channel estimation algorithms or dynamic channel state. Thus, we further study a secure relay selection method for an EH-enabled CCR-based IoT with imperfect CSI. In addition, we will discuss the outage performance of the non-centralized distribution of SUs in the same scenario as well as the secure data sharing among SUs in this scenario.

Appendix A

For both trusted and untrusted SUs, the energy harvested via the EH mode in a time slot is given by (2) and (8), respectively. For convenience, we use E_1 and E_2 to represent the harvested energy in these two scenarios. In addition, we define $g_S = \frac{\eta}{2} P_{SGS,R_k}$, where g_{S,R_k} is a random variable that obeys exponential distribution. Thus, g_S is an

exponentially distribution with mean $\bar{g}_S = \frac{1}{2}P_S\eta\bar{g}_{S,R_k}$. And the PDF and CDF of g_S can be calculated as follows.

$$f_{G_S}(g_S) = \frac{1}{\bar{g}_S} \exp\left(-\frac{g_S}{\bar{g}_S}\right), \quad (53)$$

and

$$F_{G_S}(g_S) = 1 - \exp\left(-\frac{g_S}{\bar{g}_S}\right). \quad (54)$$

Then, the CDF of E_1 is the CDF of g_S , which can be expressed as:

$$F_{E_1}(t) = 1 - \exp\left(-\frac{t}{\bar{g}_S}\right). \quad (55)$$

Next, in order to obtain the CDF of E_2 , we first obtain its probability density function (PDF). Similarly, we define $g_D = \frac{\eta}{2}P_D g_{D,R_k}$ based on (8). Here, g_{D,R_k} is also a random variable that obeys exponential distribution, which will lead to g_D as an exponentially distribution with mean $\bar{g}_D = \frac{1}{2}P_D\eta\bar{g}_{D,R_k}$. Thus, E_2 is the sum of two exponential random variables. We first compute the joint probability distribution of g_S and g_D , which can be given by:

$$\begin{aligned} f(g_S, g_D) &\stackrel{(a)}{=} f_{G_S}(g_S)f_{G_D}(g_D) \\ &= \frac{1}{\bar{g}_S \cdot \bar{g}_D} \exp\left(-\frac{g_S}{\bar{g}_S} - \frac{g_D}{\bar{g}_D}\right), \end{aligned} \quad (56)$$

where $f_{G_S}(g_S)$ and $f_{G_D}(g_D)$ are PDFs of g_S and g_D . The equality (a) holds due to the independence of g_S and g_D . Because $E = g_S + g_D$, we can easily obtain that $g_S = E - g_D$. Considering the non-negativity of the exponential distribution, we know that the value range of g_S is $[0, E_2]$. Therefore, the PDF of E_2 can be calculated as follows.

$$\begin{aligned} f_{E_2}(e) &= \int_0^e f(g_S, e - g_S) dx \\ &= \int_0^e f_{G_S}(g_S)f_{G_D}(e - g_S) dx \\ &= \int_0^e \frac{1}{\bar{g}_S \cdot \bar{g}_D} \exp\left(-\frac{g_S}{\bar{g}_S} - \frac{e - g_S}{\bar{g}_D}\right) dx \\ &= \frac{1}{\bar{g}_S \cdot \bar{g}_D} \exp\left(-\frac{e}{\bar{g}_D}\right) \int_0^e \exp\left(\frac{g_S}{\bar{g}_D} - \frac{g_S}{\bar{g}_S}\right) dx \\ &= \frac{1}{\bar{g}_S - \bar{g}_D} \left[\exp\left(-\frac{e}{\bar{g}_S}\right) - \exp\left(-\frac{e}{\bar{g}_D}\right) \right]. \end{aligned} \quad (57)$$

Then, we can get the CDF of E_2 by integrating (57), which can be derived as follows.

$$\begin{aligned} F_{E_2}(t) &= \int_0^t f_{E_2}(e) de \\ &= \int_0^t \frac{\exp\left(-\frac{e}{\bar{g}_S}\right) - \exp\left(-\frac{e}{\bar{g}_D}\right)}{\bar{g}_S - \bar{g}_D} de \\ &= 1 - \frac{\bar{g}_S \cdot \exp\left(-\frac{t}{\bar{g}_S}\right) - \bar{g}_D \cdot \exp\left(-\frac{t}{\bar{g}_D}\right)}{\bar{g}_S - \bar{g}_D}. \end{aligned} \quad (58)$$

And the proof of Lemma 1 is completed.

Appendix B

Here, we utilize the inequality $\frac{q_1q_2}{q_1+q_2+1} < \frac{q_1q_2}{q_1+q_2}$. Thus, it is easy to see that γ_D in (5) is upper bounded by:

$$\gamma_D = \frac{XY}{X+Y+1} < \frac{XY}{X+Y} = \gamma. \quad (59)$$

Accordingly, P_{out}^{LB} can be rewritten as:

$$\begin{aligned} \Pr[R_D < R_{th}] &= \Pr\left[\frac{XY}{X+Y+1} < \theta\right] \\ &> \Pr\left[\frac{XY}{X+Y} < \theta\right] \\ &= P_{out}^{LB}, \end{aligned} \quad (60)$$

In order to get the lower bound P_{out}^{LB} , we need to get the CDF of γ . At first, we define that $X_1 = 1/X$ and $Y_1 = 1/Y$. Then, we can get the CDF of X_1 as:

$$\begin{aligned} F_{X_1}(x_1) &= \Pr\{X_1 < x_1\} = 1 - \Pr\left\{X < \frac{1}{x_1}\right\} \\ &= 1 - F_X\left(\frac{1}{x_1}\right) = \exp\left(-\frac{1}{\bar{x} \cdot x_1}\right), \end{aligned} \quad (61)$$

where $F_X(\cdot)$ is the CDF of X . Thus, the PDF of X_1 can be calculated by deriving x_1 for (61), which is as below.

$$f_{X_1}(x_1) = \frac{1}{\bar{x} \cdot x_1^2} \exp\left(-\frac{1}{\bar{x} \cdot x_1}\right). \quad (62)$$

And the PDF of Y_1 is:

$$f_{Y_1}(y_1) = \frac{1}{\bar{y} \cdot y_1^2} \exp\left(-\frac{1}{\bar{y} \cdot y_1}\right). \quad (63)$$

Similar to the calculation in [52], the moment generating function (MGF) of X_1 and Y_1 is as follows.

$$\begin{aligned} M_{X_1}(s) &= E_{X_1}(e^{-sx_1}) \\ &= \int_0^\infty e^{-sx_1} \cdot f_{X_1}(x_1) dx_1 = 2\sqrt{\frac{s}{\bar{x}}} K_1\left(2\sqrt{\frac{s}{\bar{x}}}\right), \end{aligned} \quad (64)$$

and

$$\begin{aligned} M_{Y_1}(s) &= E_{Y_1}(e^{-sy_1}) \\ &= \int_0^\infty e^{-sy_1} \cdot f_{Y_1}(y_1) dy_1 = 2\sqrt{\frac{s}{\bar{y}}} K_1\left(2\sqrt{\frac{s}{\bar{y}}}\right). \end{aligned} \quad (65)$$

Next, we further define that:

$$Z = \frac{X+Y}{XY} = \frac{1}{X} + \frac{1}{Y}. \quad (66)$$

Since X_1 and Y_1 are mutually independent random variables, the MGF of $Z = X_1 + Y_1$ is the product of the MGFs of x and y , which is given by:

$$\begin{aligned} M_Z(s) &= M_{X_1}(s) \cdot M_{Y_1}(s) \\ &= 4\sqrt{\frac{1}{\bar{x} \cdot \bar{y}}} s K_1\left(2\sqrt{\frac{s}{\bar{x}}}\right) K_1\left(2\sqrt{\frac{s}{\bar{y}}}\right). \end{aligned} \quad (67)$$

Then, we can easily obtain the CDF of γ as:

$$\begin{aligned} F_{\Upsilon}(\gamma) &= \Pr\{\Upsilon < \gamma\} = \Pr\left\{\frac{1}{\Upsilon} \geq \frac{1}{\gamma}\right\} \\ &= 1 - F_Z\left(\frac{1}{\gamma}\right), \end{aligned} \quad (68)$$

where $F_Z(\cdot)$ is the CDF of Z . Using the differential nature of the Laplace transform, $F_Z(\cdot)$ can be computed by performing an inverse Laplace transform on $M_Z(s)/s$. Thus, we can get the CDF of γ as follows.

$$\begin{aligned} F_{\Upsilon}(\gamma) &= 1 - L^{-1}\left[\frac{M_Z(s)}{s}\right] \\ &= 1 - L^{-1}\left[4\sqrt{\frac{1}{\bar{x}\cdot\bar{y}}}\text{K}_1\left(2\sqrt{\frac{s}{\bar{x}}}\right)\text{K}_1\left(2\sqrt{\frac{s}{\bar{y}}}\right)\right] \\ &= 1 - 2\exp\left[-\frac{\gamma(\bar{x}+\bar{y})}{\bar{x}\cdot\bar{y}}\right]\gamma\sqrt{\frac{1}{\bar{x}\cdot\bar{y}}}\text{K}_1\left(2\gamma\sqrt{\frac{1}{\bar{x}\cdot\bar{y}}}\right). \end{aligned} \quad (69)$$

And the proof of Lemma 2 is completed.

Endnotes

¹The EH efficiency is often assumed to reach 90% or even 100% in many articles.

²Unselected SUs may continue to harvest energy in the second phase. And the transmission power of the selected $SU - R$ is negligible compared with PU's transmission power in the first phase.

³The main task of an SU is to harvest energy to assist PU's communication. We assume that the unselected SUs will only be in the EH mode and will not eavesdrop on the PUs' messages.

⁴The reason we define the energy threshold is that the time for the relay to send signals is half a time slot, i.e., 1/2 in this paper.

⁵Here, we assume that the energy used to send the pilot signal can be negligible.

⁶In fact, the AWGN is not severe in practical applications. In order to illustrate the effectiveness of the proposed strategy, the noise power is set to be $\sigma^2 = 10^{-70}$ dBm here.

⁷For practical applications, energy can be expressed into different value according to different unit price rule.

Abbreviations

AF: Amplify-and-forward; AWGN: Additive white Gaussian noise; AN: Artificial noise; BSI: Battery state information; CCR: Cooperative cognitive radio; CDF: Cumulative distribution function; CRN: Cognitive radio network; CSI: Channel state information; D2D: Device-to-device; DF: Decode-and-forward; EH: Energy harvesting; IoT: Internet of things; M2M: Machine-to-machine; MGF: moment generating function; PDF: Probability density function; PSR: Power splitting

relaying; PU: Primary user; RS: Relay selection; SINR: Signal-to-interference-plus-noise ratio; SNR: Signal-to-noise ratio; SU: Secondary user; SWIPT: Simultaneous wireless information and power transfer; TSR: Time switching relaying; WPC: Wireless powered communication

Acknowledgements

Not applicable.

Funding

This work was financially supported by NSFC 61471028, 61871023, and 61572070 and the Fundamental Research Funds for the Central Universities 2017JBM004 and 2016JBZ003.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Authors' contributions

The authors have contributed jointly to the manuscript. All authors have read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 7 September 2018 Accepted: 31 October 2018

Published online: 16 November 2018

References

1. Z. Cai, X. Zheng, A private and efficient mechanism for data uploading in smart cyber-physical systems. *IEEE Trans. Netw. Sci. Eng.* 1–1 (2018)
2. T. Jing, S. Zhu, H. Li, X. Xing, X. Cheng, Y. Huo, R. Bie, T. Znati, Cooperative relay selection in cognitive radio networks. *IEEE Trans. Veh. Technol.* **64**(5), 1872–1881 (2015)
3. N. Zhang, N. Lu, N. Cheng, J. W. Mark, X. S. Shen, Cooperative spectrum access towards secure information transfer for CRNs. *IEEE J. Sel. Areas Commun.* **31**(11), 2453–2464 (2013)
4. W. Li, X. Cheng, T. Jing, X. Xing, in *2013 Proceedings IEEE INFOCOM*. Cooperative multi-hop relaying via network formation games in cognitive radio networks (IEEE, Turin, 2013), pp. 971–979
5. H. Li, X. Xing, J. Zhu, X. Cheng, K. Li, R. Bie, T. Jing, Utility-based cooperative spectrum sensing scheduling in cognitive radio networks. *IEEE Trans. Veh. Technol.* **66**(1), 645–655 (2017)
6. X. Fang, J. Luo, G. Luo, W. Wu, Z. Cai, Y.G. Pan, Big data transmission in industrial IoT systems with small capacitor supplying energy. *IEEE Trans. Ind. Inform.*, 1–1 (2018)
7. Y. Liu, Q. Chen, G. Liu, H. Liu, Q. Yang, Ecosense: A hardware approach to on-demand sensing in the Internet of Things. *IEEE Commun. Mag.* **54**(12), 37–43 (2016). <https://doi.org/10.1109/MCOM.2016.1600621CM>
8. X. An, X. Zhou, X. Lv, F. Lin, L. Yang, Sample selected extreme learning machine based intrusion detection in fog computing and MEC. *Wirel. Commun. Mob. Comput.* **2018**, 1–10 (2018). doi:10.1155/2018/7472095
9. Q. Chen, Y. Liu, G. Liu, Q. Yang, X. Shi, H. Gao, L. Su, Q. Li, Harvest energy from the water: A self-sustained wireless water quality sensing system. *ACM Trans. Embed. Comput. Syst.* **17**(1), 3–1324 (2017). <https://doi.org/10.1145/3047646>
10. D. Han, B. Zheng, Z. Chen, Sleep mechanism of base station based on minimum energy cost. *Wirel. Commun. Mob. Comput.* **2018**, 1–13 (2018). doi: 10.1155/2018/4202748
11. X. Lu, P. Wang, D. Niyato, D. I. Kim, Z. Han, Wireless networks with RF energy harvesting: A contemporary survey. *IEEE Commun. Surv. Tutor.* **17**(2), 757–789 (2015)
12. T. Shi, S. Cheng, Z. Cai, Y. Li, J. Li, Exploring connected dominating sets in energy harvest networks. *IEEE/ACM Trans. Netw.* **25**(3), 1803–1817 (2017)
13. S. Bi, Y. Zeng, R. Zhang, Wireless powered communication networks: an overview. *IEEE Wirel. Commun.* **23**(2), 10–18 (2016)
14. H. Ma, T. Jing, F. Zhang, X. Fan, Y. Lu, Y. Huo, in *Wireless Algorithms, Systems, and Applications*. Throughput analysis for energy harvesting

- cognitive radio networks with unslotted users (Springer Lecture Notes in Computer Science, Tianjin, 2018), pp. 345–356
15. Z. Zhou, M. Peng, Z. Zhao, W. Wang, R. S. Blum, Wireless-powered cooperative communications: Power-splitting relaying with energy accumulation. *IEEE J. Sel. Areas Commun.* **34**(4), 969–982 (2016)
 16. I. Krikidis, Relay selection in wireless powered cooperative networks with energy storage. *IEEE J. Sel. Areas Commun.* **33**(12), 2596–2610 (2015)
 17. Y. Gu, H. H. Chen, Y. Li, B. Vucetic, in *2016 IEEE International Conference on Communications (ICC)*. Distributed multi-relay selection in wireless-powered cooperative networks with energy accumulation (IEEE, Kuala Lumpur, 2016), pp. 1–6
 18. K. Liu, in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*. Selection cooperation using rf energy harvesting relays with finite energy buffer (IEEE, Istanbul, 2014), pp. 2156–2161
 19. K. Ishibashi, H. Ochiai, V. Tarokh, in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*. Energy harvesting cooperative communications (IEEE, Sydney, 2012), pp. 1819–1823
 20. F. Lin, Y. Zhou, X. An, I. You, K. R. Choo, Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of internet of things devices. *IEEE Consum. Electron. Mag.* **7**(6), 45–50 (2018). <https://doi.org/10.1109/MCE.2018.2851723>
 21. Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, Z. Liang, Man-in-the-browser-cache: Persisting https attacks via browser cache poisoning. *Comput. Secur.* **55**, 62–80 (2015). <https://doi.org/10.1016/j.cose.2015.07.004>
 22. Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, Y. Li, Cost-efficient strategies for restraining rumor spreading in mobile social networks. *IEEE Trans. Veh. Technol.* **66**(3), 2789–2800 (2017). <https://doi.org/10.1109/TVT.2016.2585591>
 23. J. Mao, W. Tian, P. Li, T. Wei, Z. Liang, Phishing-alarm: Robust and efficient phishing detection via page component similarity. *IEEE Access.* **5**, 17020–17030 (2017). <https://doi.org/10.1109/ACCESS.2017.2743528>
 24. X. Zheng, Z. Cai, J. Yu, C. Wang, Y. Li, Follow but no track: Privacy preserved profile publishing in cyber-physical social systems. *IEEE Internet Things J.* **4**(6), 1868–1878 (2017). <https://doi.org/10.1109/JIOT.2017.2679483>
 25. Z. Cai, Z. He, X. Guan, Y. Li, Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE Trans. Dependable Secure Comput.* **15**(4), 577–590 (2018). <https://doi.org/10.1109/TDSC.2016.2613521>
 26. X. Zheng, Z. Cai, Y. Li, Data linkage in smart internet of things systems: a consideration from a privacy perspective. *IEEE Commun. Mag.* **56**(9), 55–61 (2018). <https://doi.org/10.1109/MCOM.2018.1701245>
 27. Z. Duan, W. Li, Z. Cai, in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. Distributed auctions for task assignment and scheduling in mobile crowdsensing systems (IEEE, Atlanta, 2017), pp. 635–644
 28. Y. Zeng, R. Zhang, Optimized training design for wireless energy transfer. *IEEE Trans. Commun.* **63**(2), 536–550 (2015)
 29. Q. Gao, T. Jing, X. Xing, X. Cheng, Y. Huo, D. Chen, in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*. Simultaneous energy and information cooperation in MIMO cooperative cognitive radio systems (IEEE, Orleans, 2015), pp. 351–356
 30. A. Salem, K. A. Hamdi, K. M. Rabie, Physical layer security with RF energy harvesting in AF multi-antenna relaying networks. *IEEE Trans. Commun.* **64**(7), 3025–3038 (2016)
 31. H. Xing, K. Wong, A. Nallanathan, in *2015 IEEE International Conference on Communications (ICC)*. Secure wireless energy harvesting-enabled AF-relaying SWIPT networks (IEEE, London, 2015), pp. 2307–2312
 32. S. Raghuvanshi, P. Maji, S. D. Roy, S. Kundu, in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. Secrecy performance of a dual hop cognitive relay network with an energy harvesting relay, (2016), pp. 1622–1627
 33. K. Liu, Performance analysis of relay selection for cooperative relays based on wireless power transfer with finite energy storage. *IEEE Trans. Veh. Technol.* **65**(7), 5110–5121 (2016)
 34. L. Sun, P. Ren, Q. Du, Y. Wang, Z. Gao, Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Commun. Lett.* **19**(3), 463–466 (2015)
 35. G. Luo, J. Li, Z. Liu, X. Tao, F. Yang, in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. Physical layer security with untrusted relays in wireless cooperative networks (IEEE, San Francisco, 2017), pp. 1–6
 36. D. Wang, P. Ren, Y. Wang, Q. Du, L. Sun, in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*. Cooperative jamming with untrusted SUs for secure communication of two-hop primary system (IEEE, Dubrovnik, 2015), pp. 90–95
 37. B. Ali, N. Zamir, M. Fasih, U. Butt, S. X. Ng, in *2016 24th European Signal Processing Conference (EUSIPCO)*. Physical layer security: Friendly jamming in an untrusted relay scenario (IEEE, Budapest, 2016), pp. 958–962
 38. A. Mabrouk, A. E. Shafie, K. Tourki, N. Al-Dhahir, Adaptive secure transmission for RF-EH untrusted relaying with alien eavesdropping. *IEEE Commun. Lett.* **PP**(99), 1–1 (2017)
 39. L. Sun, P. Ren, Q. Du, Y. Wang, Z. Gao, Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Commun. Lett.* **19**(3), 463–466 (2015)
 40. D. Wang, P. Ren, Y. Wang, Q. Du, L. Sun, *Cooperative jamming with untrusted SUs for secure communication of two-hop primary system*. (2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 2015), pp. 90–95
 41. V. Gupta, S. S. Kalamkar, A. Banerjee, in *IEEE Global Communications Conference*. On secure communication using RF energy harvesting two-way untrusted relay (IEEE, Singapore, 2017)
 42. S. S. Kalamkar, A. Banerjee, Secure communication via a wireless energy harvesting untrusted relay. *IEEE Trans. Veh. Technol.* **66**(3), 2199–2213 (2017). <https://doi.org/10.1109/TVT.2016.2572960>
 43. A. D. Wyner, The wire-tap channel. *Bell Labs Tech. J.* **54**(8), 1355–1387 (1975)
 44. I. Krikidis, J. S. Thompson, S. Mclaughlin, Relay selection for secure cooperative networks with jamming. *IEEE Trans. Wirel. Commun.* **8**(10), 5003–5011 (2009)
 45. D. H. Ibrahim, E. S. Hassan, S. A. El-Dolil, Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks. *Comput. Secur.* **50**, 47–59 (2015)
 46. Y. Gu, H. Chen, Y. Li, Y. Liang, B. Vucetic, Distributed multi-relay selection in accumulate-then-forward energy harvesting relay networks. *IEEE Trans. Green Commun. Netw.* **2**(1), 74–86 (2018)
 47. D. Farnsworth, A first course in order statistics. *Technometrics.* **35**(4), 452–452 (1993)
 48. S. S. Soliman, N. C. Beaulieu, Exact analysis of dual-hop AF maximum end-to-end SNR relay selection. *IEEE Transactions on Communications.* **60**(8), 2135–2145 (2012)
 49. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008). <http://bitcoin.org/bitcoin.pdf>
 50. I. Eyal, A. E. Gencer, E. G. Sirer, R. V. Renesse, in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. Bitcoin-NG: A scalable blockchain protocol (ACM, Carlsbad, 2016), pp. 45–59
 51. G. Zyskind, O. Nathan, A. Pentland, in *2015 IEEE Security and Privacy Workshops*. Decentralizing privacy: Using blockchain to protect personal data (IEEE, San Jose, 2015), pp. 180–184
 52. M. O. Hasna, M. Alouini, End-to-end performance of transmission systems with relays over Rayleigh-fading channels. *IEEE Trans. Wirel. Commun.* **2**(6), 1126–1131 (2003)

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com
