Incentivizing Relay Participation for Securing IoT Communication

Xiaonan Zhang, Pei Huang, Linke Guo, and Mo Sha
Department of Electrical and Computer Engineering, Binghamton University,
State University of New York, Binghamton, NY 13902, USA
Email: {xzhan167, phuang13, lguo, msha}@binghamton.edu

***Abstract*—Internet of Things (IoT) has emerged as a new computing paradigm that promises to offer a fully connected "smart" world. However, due to the open nature of wireless medium, the information sensed, collected, and transmitted by IoT devices can be easily intercepted by adversaries, which becomes a serious concern in most IoT applications requiring sensitive data. In practice, cooperative communication approaches can effectively improve the security level for wireless communication under the presence of eavesdroppers with unbounded computational ability. In this paper, we apply the amplify-and-forward (AF) cooperative communication to increase the secrecy capacity of IoT systems by incentivizing relay IoT devices. Specifically, a Stackelberg game is designed to motivate the participation of the relay IoT devices for security enhancement. Extensive experimental results have demonstrated the feasibility and security of the proposed mechanism under both unknown and known channel state information (CSI) models.**

***Index Terms*—IoT, Cooperative Communication, Stackelberg Game, Physical-layer Security**

I. Introduction

Internet of Things (IoT) is expected to enable ubiquitous connectivity and information exchange among billions of everyday necessities. Although the deployment of smart connected objects has become a reality in our daily activities, serious concerns are raised as follows. On the one hand, over 60% of IoT applications are required to achieve low power consumption, long battery life, high data rate, and wide coverage simultaneously [1]. Although the newly proposed NB-IoT and LoRa protocols would be able to address some of the above requirements, the low data rate (approx. 50-250 kbps) becomes the main bottleneck to hinder their wide deployment in many applications. For some existing wireless technologies (e.g., Bluetooth Low Energy and 802.15.4/ZigBee), the low power feature limits the communication range, and thus they are unable to be deployed in industrial applications, such as environmental sensing and machinery weakness monitoring. On the other hand, the disclosure of sensitive information, including machinery data, patients' health data, or financial files, collected by many IoT applications is unacceptable. Unfortunately, data communication is *de facto* vulnerable to the eavesdropping attack due to the heterogeneous wireless environment in the IoT system [2, 3].

The work of Dr. L. Guo is partially supported by National Science Foundation (NSF) under grants ECCS-1710996, CNS-1744261, and IIS-1722731. The work of Dr. M. Sha is partially supported by NSF under grant CNS-1657275.

Cooperative communication is a perfect fit to tackle the above challenges with its advantages on wide coverage, energy efficiency, and high interference mitigation capability. While being thoroughly investigated in the Wireless Sensor Network (WSN), it could play a more significant role in the IoT system of enhancing the reliability and security. Specifically, the cooperative communication will introduce inherent randomness of wireless channels, which could prevent eavesdroppers from intercepting the transmitted message. However, the major challenge that deters the deployment of cooperative communication on improving the security level is the limited battery life of wireless sensors.

In this paper, we propose a novel cooperative IoT system consisting of multiple relay IoT nodes to enhance the reliability and security. Different to that in WSN, many Commercial off-the-shelf (COTS) IoT nodes are able to collect energy from renewable resources in ambient environments, such as vibration, solar and, wind energy [4]. Such characteristics give relay IoT nodes more opportunities, and they mainly play two roles: 1) forwarding the data from each source node to the destination node to ensure the reliable communication; 2) preventing data information from being intercepted by the eavesdropper to secure the IoT communication. Although the proposed paradigm enlightens a new methodology for reliable IoT communication, how to incentivize relay IoT nodes to help data forwarding becomes a challenging issue, because each relay IoT node has to consume its own energy for relaying. Therefore, we propose a game-theoretical solution to motivate the participation of relay IoT nodes with joint consideration on both channel state information (CSI) and energy consumption. We highlight our contributions as follows,

- We propose a novel cooperative IoT system to ensure the reliability and security of data communication specifically for IoT applications.
- Relay IoT nodes can help improve the secrecy capacity by participating in the cooperative communication continuously given their current energy limitation.
- To demonstrate the practicality, two "two-stage" Stackelberg games under both the wiretap-link CSI unknown and known cases are formulated between the source and relay IoT nodes.
- Simulations and the experiments using real-world dataset show the feasibility of the proposed scheme.

The rest of this paper is organized as follows. We briefly review related work in Sec. II. A detailed description of the system model and the Stackelberg game formulation are given in Sec. III. In Sec. IV, we introduce the proposed Stackelberg game in the wiretap-link CSI unknown case in detail. An extension to the wiretap link CSI known case, which is more complex, is discussed in Sec. V. In Sec. VI, complexity is analyzed and performance evaluation is demonstrated for both cases, followed with a conclusion in Sec. VII.

II. Related Work

A. Cooperative Communication in IoT

Cooperative communication aims at improving energy efficiency, overall throughput, power control, and resource allocation in wireless networks [5–8]. It has been widely deployed in many IoT applications. Omar *et al.* in [9] use cooperative communications in a smart metering system to relay data in a multi-hop fashion to far-off aggregation points. The experimental results verify cooperative communication can increase network range, prolong network lifetime, and reduce energy consumption. It is also deployed in cluster-based industrial IoT network to optimize both energy efficiency and QoS in [5, 10]. In the context of large-scale IoT, Bader *et al.* in [11] use blind cooperative transmission in conjunction with multi-hop networking to minimize underlying protocol overhead and therefore allows for scalability. However, securing cooperative IoT system receives less attention.

B. Physical-layer Security

Physical-layer security mechanism exploits the property of the wireless channel for secure communication [3, 12–14]. It has shown great potential in providing information-theoretically unbreakable secrecy [2]. Many transmission strategies, such as cooperative transmission [15], artificial noise [16], and secure beamforming [17], are proposed to enhance physical layer security. Among all those strategies, cooperative communication is of great significance to the IoT communication due to its low power and wide coverage requirements. A comprehensive overview of physical layer security in wireless cooperative relay networks is provided in [18]. The performance of secure transmission is improved by employing multiple relays in [15, 19]. Specifically, Xu *et al.* in [2] prove that the proper use of relay transmission enhances the secrecy throughput and extends the secure coverage range. However, without proper benefits, relay IoT nodes will not participate in the cooperative communication.

C. Stackelberg Game

Stackelberg game [20] models and analyzes the interactions among independent decision makers, which has been applied in a broad field of wireless communications and networks [21–25]. Particularly, A single-leader single-follower Stackelberg game is proposed in [26] for physical layer security and energy efficiency enhancement. However, it does not support multiple relay nodes case. A single-leader multiple-followers Stackelberg game is deployed to coordinate multiple relays for physical-layer security improvement in [13], where the fairness among relay nodes is considered. However, due to the different CSIs on the wiretap link between the eavesdropper and each relay node, each relay node contributes differently to physical layer security. The EWS-based algorithm in [13] is also not a proper method for physical-layer security enhancement.

III. System Overview

A. System Model

An IoT application shown in Fig.1 describes our system model. Assume that K energy constrained source devices (nodes) $\mathcal{S} = \{S_1, S_2, \cdots, S_K\}$ transmit data to a distant destination node (e.g., gateway) D (e.g., IoT gateway) through orthogonal channels in the presence of an eavesdropper E near the destination node D. Nodes D and E are out of the transmission range of the source nodes. To enable data transmission and prevent them from being intercepted, an amplified-and-forward (AF) cooperative protocol is employed with the help of N mobile relay IoT devices (nodes) $\mathcal{R} = \{R_1, R_2, \cdots, R_N\}$. Each R_i collects extra energy from the ambient environment when it does not work for the source nodes. Besides, all the nodes including the eavesdropper are assumed to know the existence of the relay nodes and the cooperative protocol, which is a common assumption in physical-layer security protocols [26]. Since the eavesdropper cannot receive data information from $\mathcal{S}$, it monitors the data transmission from R_i to D and attempts to interpret the data.

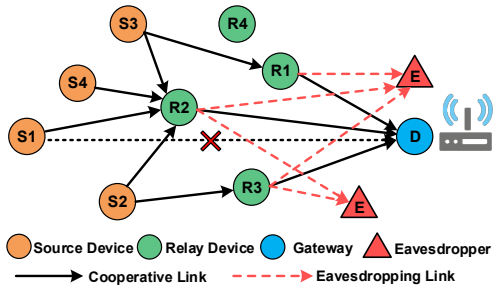


Fig. 1: System Model

B. Cooperative IoT System

We consider a flat Rayleigh fading channel in the proposed cooperative IoT system. The fading amplitude between S_k and R_i is denoted as $h_{S_k R_i}$, whereas that between R_i and D is represented by $h_{R_i D}$. Meanwhile, we denote the fading amplitude between R_i and E as $h_{R_i E}$. Without loss of generality, $n_{S_k R_i}$, $n_{R_i D}$ and $n_{R_i E}$ are the corresponding additive white Gaussian noise (AWGN) with the same distribution $\mathcal{CN}(0, \sigma^2)$, where σ^2 is one-sided power spectral density. Similar to [13], we assume that source nodes can get global CSI of the main links, and the local information can be obtained by the relay nodes. Generally, data transmission is divided into two steps: **Step 1**: S_k broadcasts its encoded signal s_k $(E\left(|s_k|^2\right) = 1)$ with the power P_{S_k}. The signal received at R_i is,

$$y_{S_k R_i} = \sqrt{P_{S_k}} h_{S_k R_i} s_k + n_{S_k R_i}. \tag{1}$$

Step 2: R_i normalizes and amplifies the received signal $y_{S_kR_i}$ with the power $P_{R_i}^{S_k}$ and sends it to D. Then, D receives,

$$y_{S_kR_iD} = \sqrt{P_{R_i}^{S_k}} h_{R_iD} \frac{y_{S_kR_i}}{|y_{S_kR_i}|} + n_{R_iD} \tag{2}$$

where the power $P_{R_i}^{S_k}$ consists of two parts: the power provided by the relay IoT node itself and harvested from the ambient environment. Similarly, S_k' signal forwarded by R_i can also be received by E, where

$$y_{R_iE} = \sqrt{P_{R_i}^{S_k}} h_{R_iE} \frac{y_{S_kR_i}}{|y_{S_kR_i}|} + n_{R_iE} \tag{3}$$

Substitute (1) into (2), the signal-to-noise radio (SNR) $\Gamma_{S_kR_iD}$ on the main link (S_k-R_i-D) becomes,

$$\Gamma_{S_kR_iD}(P_{R_i}^{S_k}) = \frac{P_{S_k} P_{R_i}^{S_k} \gamma_{S_kR_i} \gamma_{R_iD}}{1 + P_{S_k}\gamma_{S_kR_i} + P_{R_i}^{S_k}\gamma_{R_iD}} \tag{4}$$

where $\gamma_{S_kR_i} = |h_{S_kR_i}|^2/\sigma^2$ and $\gamma_{R_iD} = |h_{R_iD}|^2/\sigma^2$.

Similarly, based on (1) and (3), the SNR $\Gamma_{S_kR_iE}$ on the wiretap link (S_k-R_i-E) related to the relay node R_i is,

$$\Gamma_{S_kR_iE}(P_{R_i}^{S_k}) = \frac{P_{S_k} P_{R_i}^{S_k} \gamma_{S_kR_i} \gamma_{R_iE}}{1 + P_{S_k}\gamma_{S_kR_i} + P_{R_i}^{S_k}\gamma_{R_iE}} \tag{5}$$

in which $\gamma_{R_iE} = |h_{R_iE}|^2/\sigma^2$, $i = 1, 2, \cdots, N$.

To maximize the receiving SNR, we deploy Maximum Radio Combination (MRC) at both D and E, representing the theoretically optimal combiner over fading channels [27]. As a result, the corresponding channel capacities on the main link and wiretap link are,

$$C_D^{S_k}(P_{\mathbf{R}}^{S_k}) = W \log_2(1 + \sum\nolimits_{i=1}^{N} \Gamma_{S_kR_iD}) \tag{6}$$

and

$$C_E^{S_k}(P_{\mathbf{R}}^{S_k}) = W \log_2(1 + \sum\nolimits_{i=1}^{N} \Gamma_{S_kR_iE}) \tag{7}$$

respectively, where $P_{\mathbf{R}}^{S_k} = \{P_{R_1}^{S_k}, P_{R_2}^{S_k}, \cdots, P_{R_N}^{S_k}\}$ denotes the power each relay node consumes to forward the signal S_k.

DEFINITION 1. *(Secrecy Capacity) The secrecy capacity [28] related to S_k, defined as the difference between the capacity of the main link (S_k-$\mathcal{R}$-D) and that of the wiretap link (S_k-$\mathcal{R}$-E), is written as,*

$$C^{S_k}(P_{\mathbf{R}}^{S_k}) = \max\{C_D^{S_k}(P_{\mathbf{R}}^{S_k}) - C_E^{S_k}(P_{\mathbf{R}}^{S_k}), 0\} \tag{8}$$

It represents the maximum transmission rate of the main link that the eavesdropper is unable to decode any information.

Therefore, in order to enhance the IoT system security, it is necessary to maximize the secrecy capacity of S_k with the help of multiple relay IoT nodes given the source node power P_{S_k} and the CSI of both the main link and the wiretap link,

$$\max\nolimits_{P_{\mathbf{R}}^{S_k}} C^{S_k}(P_{\mathbf{R}}^{S_k}) \tag{9}$$

We denote $P_{R_i}^{max}$ as the maximized power the relay node R_i uses to forward the data from all the source nodes. Hence, we have the following constraint,

$$0 \le \sum\nolimits_{k=1}^{K} P_{R_i}^{S_k} \le P_{R_i}^{max}, i = 1, 2, \cdots, N. \tag{10}$$

C. Stackelberg Game Formulation

To incentivize the relay participation, we propose a game-theoretical approach to choose proper relay IoT nodes for data forwarding. In contrast to treating source nodes equally from relay IoT nodes' perspectives, S_k intends to select the most beneficial R_i because R_i has different performance on enhancing the secrecy capacity due to the different CSIs and available power. To maximize the benefits of both the source nodes and the relay nodes, we formulate their interactions as a two-stage multi-buyer multi-seller Stackelberg game. Particularly, we discuss the Stackelberg game under the wiretap-link CSI h_{R_iE} unknown and known cases.

1) CSI-Unknown Stackelberg Game (CUS Game): Assuming the eavesdropper only listens without transmitting, the CSI on the wiretap link $h_{R_iE}, i = 1, 2, \cdots, N$ is unknown. The source node S_k cannot select qualified relay IoT nodes and purchase power to enhance the secrecy performance. Motivated by [13], we replace the capacity on the wiretap link with its supreme $\overline{C_E^{sup}}$, which is obtained based on a period of monitoring. We define the multi-buyers multi-sellers Stackelberg game as,

DEFINITION 2. *(CUS Game)*

- ***Stage I (Unit Pricing)*** *Each relay IoT node $R_i \in \mathcal{R}$ sells its power to maximize the benefit U_i with a unit price q_i^*,*

$$q_i^* = \arg\max (q_i - c_i) \sum\nolimits_{k=1}^{K} P_{R_i}^{S_k}, i = 1, 2, \cdots, N \tag{11}$$

- ***Stage II (Power Purchased)*** *Each source node $S_k \in \mathcal{S}$ buys an amount of power $P_{R_i}^{S_k}$ from R_i to maximize its utility,*

$$\mathbf{P_R^{S_k}}^* = \arg\max U^{S_k}(\mathbf{P_R^{S_k}}^*, \mathbf{q}), k = 1, 2, \cdots, K \tag{12}$$

In the CUS game, R_i sells its power to $S_k, k = 1, 2, \cdots, K$ to maximize the utility with a unit price q_i,

$$U_{R_i}(P_{R_i}^{S_1}, P_{R_i}^{S_2}, \cdots, P_{R_i}^{S_K}, q_i) = (q_i - c_i) \sum\nolimits_{k=1}^{K} P_{R_i}^{S_k} \tag{13}$$

with its current power constraint (10). c_i denotes its own cost. The unit price of each relay node composes a price vector $\mathbf{q} = \{q_1, q_2, \cdots, q_N\}$. As for each S_k, when the relay nodes help forward the data, it gets the utility,

$$U^{S_k}(\mathbf{P_R^{S_k}}, \mathbf{q}) = \alpha(C_D^{S_k}(\mathbf{P_R^{S_k}}) - \overline{C_E^{sup}}) - \sum\nolimits_{i=1}^{N} q_i P_{R_i}^{S_k} \tag{14}$$

where α denotes the gain per unit of secrecy capacity.

2) CSI-Known Stackelberg Game (CKS Game): A receiving node can play as a legitimate destination node for some data transmission while still performing as an eavesdropper for others. Therefore, the CSI on the wiretap link is obtained. We extend the above CUS game to the CKS game. At this time, the utility of each source node becomes,

$$U^{S_k}(\mathbf{P_R^{S_k}}, \mathbf{q}) = \alpha C^{S_k}(\mathbf{P_R^{S_k}}) - \sum\nolimits_{i=1}^{N} q_i P_{R_i}^{S_k} \tag{15}$$

In addition, a secrecy capacity constraint is added to ensure data transmission security,

$$C^{S_k}(\mathbf{P_R^{S_k}}) > C_0 \tag{16}$$

where C_0 is the minimum secrecy capacity limitation. The Stackelberg game formulation and utility with power constraint for each relay node keeps unchanged. Note that the utilities for all the source/relay nodes are nonnegative.

IV. Utility Maximization in CUS Game

In the proposed CUS game, we deploy the backward induction [29] to find the optimal power strategies that no source node deviates based on the unit price each relay node charges. For each relay node in Stage I, we are interested in the pricing strategy that maximizes its benefit given the source nodes' optimal strategies in Stage II, which yields the concept of power equilibrium.

DEFINITION 3. *(Power Equilibrium) For any price p_i given in Stage I, the power equilibrium (PE) in Stage II is a strategy profile $P_{R_i}^{S_k*}$ such that S_k cannot improve its utility by unilaterally changing the power purchased from R_i, i.e.,*

$$\mathbf{P_R^{S_k}}^* = \arg\max_{\mathbf{P_R^{S_k}}} U^{S_k}(\mathbf{P_R^{S_k}}, \mathbf{q}), i = 1, 2, \cdots, N \quad (17)$$

A. Stage II: Power Equilibrium

Since source nodes transmit the data on the orthogonal channels and are equally treated by each relay node, we consider the power equilibrium for the S_k. Based on (4), (6) and (14), its utility becomes,

$$\begin{aligned} U^{S_k}(\mathbf{P_R^{S_k}}, \mathbf{q}) &= \alpha W \log_2(1 + \textstyle\sum_{i=1}^{N} \frac{P_{S_k} P_{R_i}^{S_k} \gamma_{S_k R_i} \gamma_{R_i D}}{1 + P_{S_k}\gamma_{S_k R_i} + P_{R_i}^{S_k}\gamma_{R_i D}}) \\ &\quad - \overline{C_E^{sup}} - \textstyle\sum_{i=1}^{N} q_i P_{R_i}^{S_k} \\ &= \alpha W \log_2(1 + \sum_{i=1}^{N} \frac{A_{S_k R_i} P_{R_i}^{S_k}}{B_{S_k R_i} + P_{R_i}^{S_k}}) - \overline{C_E^{sup}} - \sum_{i=1}^{N} q_i P_{R_i}^{S_k} \end{aligned} \quad (18)$$

where $A_{S_k R_i} = P_{S_k}\gamma_{S_k R_i}$, $B_{R_k S_i} = (1 + P_{S_k}\gamma_{S_k R_i})/\gamma_{R_i D}$. The constant $\overline{C_E^{sup}}$ transforms the utility maximization problem on the secrecy capacity to that on the channel capacity on the main link. Such transformation is an approximation to the original problem. Only when the supreme secrecy capacity equals to the channel capacity on the wiretap link are the two utility maximization problems equal [21].

Using the utility function (18), by setting the derivative $\partial U^{S_k}(\mathbf{P_R^{S_k}}, \mathbf{q})/P_{R_i}^{S_k} = 0$ as the first-order condition and solving the equation set, we get the optimal power strategies,

$$P_{R_i}^{S_k*} = \sqrt{\frac{A_{S_k R_i} B_{S_k R_i}}{q_i}} \frac{Y_k + \sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}{2X_{S_k}} - B_{S_k R_i} \quad (19)$$

where $X_{S_k} = 1 + \sum_{i=1}^{N} A_{S_k R_i}$ and $Y_{S_k} = \sum_{i=1}^{N} \sqrt{q_i A_{S_k R_i} B_{S_k R_i}}$. Meanwhile, since the utility function (18) is joint concave in $\{P_{R_i}^{S_k}\}_{i=1}^{N}$, $P_{R_i}^{S_k*}$ is the power equilibrium purchased from R_i given its unit price p_i.

B. Stage I: Optimal Pricing

Different to the scenario in [21], CUS game is played between multiple source nodes and relay nodes. From (13), we see that the utility of each relay IoT node depends on the power sold to all the source nodes. To obtain the optimal price of R_i, we set the derivative $\partial U_{R_i}/\partial q_i = 0$ according to (13) and obtain,

$$q_i = I_i(\mathbf{q}) = c_i - \frac{\sum_{k=1}^{K} P_{R_i}^{S_k*}}{\partial \sum_{k=1}^{K} P_{R_i}^{S_k*}/\partial q_i} \quad (20)$$

Denote $\mathbf{I}(\mathbf{q}) = \{I_1(\mathbf{q}), I_2(\mathbf{q}), \cdots, I_N(\mathbf{q})\}$. We have,

THEOREM 1. *The optimal price is obtained by continuously updating the price of each relay node as follows,*

$$\mathbf{q} = \mathbf{I}(\mathbf{q}). \quad (21)$$

Proof: To prove the convergence, we show that $\mathbf{I}(\mathbf{q})$ is a standard function [30], which means that $\mathbf{I}(\mathbf{q})$ needs to satisfy positivity, scalability, and monotonicity. We describe the utility maximization process for both the source and relay nodes in Algorithm 1, which is convergent according to Theorem 1.

Algorithm 1: Utility Maximization in CUS Game

Input: convergence threshold ξ
Output: $\mathbf{P_{R_i}^{S_k}}^*, \mathbf{q}^*$
Set the initial price $q_{i(0)} = c_i, i = 1, 2, \cdots, N$;
Set the initial power $P_{R_i}^{S_k} = 0, i = 1, 2, \cdots, N, k = 1, 2, \cdots, K$;
while $\mathbf{1}^T|\mathbf{q}_{(n+1)} - \mathbf{q}_{(n)}| \leq \xi$ **do**
  Compute $P_{R_i}^{S_k}$ based on (19) for $k = 1, 2, \cdots, K, i = 1, 2, \cdots, N$;
  Update $\mathbf{q_{(n+1)}}$ according to (21);
end
Compute $P_{R_i}^{S_k}$ given $\mathbf{q}_{(n)}$;
return $\mathbf{q}^* = \mathbf{q}_{(n)}$, $\mathbf{P_R^{S_k}}^* = \mathbf{P_R^{S_k}}$;

Positivity: $\mathbf{I}(\mathbf{q}) > 0$. From (19), for each relay node,

$$\begin{aligned} \frac{\partial \sum_{k=1}^{K} P_{R_i}^{S_k*}}{\partial q_i} &= -\frac{1}{2q_i}\left(1 - \frac{\sqrt{q_i A_{S_k R_i} B_{S_k R_i}}}{\sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}\right) \\ &\quad \times \sum_{k=1}^{K}\left(\sqrt{\frac{A_{S_k R_i} B_{S_k R_i}}{q_i}} \frac{Y_{S_k} + \sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}{2X_{S_k}}\right) < 0 \end{aligned} \quad (22)$$

Hence, $I_i(\mathbf{q})$ in (20) is positive under the condition that both c_i and $\sum_{k=1}^{K} P_{R_i}^{S_k*}$ are larger than 0.

Scalability: We show that for all $\vartheta > 1$, $\vartheta\mathbf{I}(\mathbf{q}) > \mathbf{I}(\vartheta\mathbf{q})$.

$$\begin{aligned} \vartheta\mathbf{I}(\mathbf{q}) - \mathbf{I}(\vartheta\mathbf{q}) &= (\vartheta - 1)c_i + \\ \vartheta\left(\frac{\sum_{k=1}^{K} P_{R_i}^{S_k*}(\vartheta\mathbf{q})}{\partial \sum_{k=1}^{K} P_{R_i}^{S_k*}(\vartheta\mathbf{q})/\partial q_i} - \frac{\sum_{k=1}^{K} P_{R_i}^{S_k*}(\mathbf{q})}{\partial \sum_{k=1}^{K} P_{R_i}^{S_k*}(\mathbf{q})/\partial q_i}\right) &> 0. \end{aligned} \quad (23)$$

The key is to see whether the second part in (23) is positive. Denote $Z_{R_i}(W) = \frac{\sum_{k=1}^{K} P_{R_i}^{S_k*}(\mathbf{q})}{\partial \sum_{k=1}^{K} P_{R_i}^{S_k*}(\mathbf{q})/\partial q_i}$. Based on (19),

$$\begin{aligned} P_{R_i}^{S_k*}(\vartheta\mathbf{q}) &= \sqrt{\frac{A_{S_k R_i} B_{S_k R_i}}{\vartheta q_i}} \frac{\sqrt{\vartheta} Y_{S_k} + \sqrt{\vartheta Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}{2X_{S_k}} - B_{S_k R_i} \\ &= \sqrt{\frac{A_{S_k R_i} B_{S_k R_i}}{q_i}} \frac{Y_{S_k} + \sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{\vartheta In2}}}{2X_{S_k}} - B_{S_k R_i} \end{aligned} \quad (24)$$

Instead of $\mathbf{q}$, ϑ puts an effect to W in (24). Hence,

$$\frac{\sum_{k=1}^{K} P_{R_i}^{S_k*}(\vartheta\mathbf{q})}{\partial \sum_{k=1}^{K} P_{R_i}^{S_k*}(\vartheta\mathbf{q})/\partial q_i} = Z_{R_i}(W/\vartheta) \quad (25)$$

The scalability problem becomes to see whether $Z_{R_i}(W/\vartheta) - Z_{R_i}(W)$ is positive, where $Z_{R_i}(W)$ equals to

$$\frac{-2q_i \sum_{k=1}^{K}\left(\sqrt{\frac{A_{S_k R_i} B_{S_k R_i}}{q_i}} \frac{Y_{S_k} + \sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}{2X_{S_k}} - B_{S_k R_i}\right)}{\sum_{k=1}^{K}\left(1 - \frac{\sqrt{q_i A_{S_k R_i} B_{S_k R_i}}}{\sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}\right)\left(\sqrt{\frac{A_{S_k R_i} B_{S_k R_i}}{q_i}} \frac{Y_{S_k} + \sqrt{Y_{S_k}^2 + 4X_{S_k}\frac{\alpha W}{In2}}}{2X_{S_k}}\right)} \quad (26)$$

Through deduction, we conclude that $Z_{R_i}(W)$ in (26) is monotonic decreasing. $Z_{R_i}(W/\vartheta) > Z_{R_i}(W/\vartheta)$ for $i = 1, 2, \cdots, N$, the scalability of $\mathbf{I}(\mathbf{q})$ is proved.

Monotonicity: If $\mathbf{q} \geq \mathbf{q}^{'}, \mathbf{I}(\mathbf{q}) \geq \mathbf{I}(\mathbf{q}^{'})$. $\mathbf{q} \geq \mathbf{q}^{'}$ denotes that there at least exists a R_i such that $q_i \geq q_i^{'}$. For any $j \neq i$,

$$I_i(q_i, \mathbf{q_{-i}}) \geq I_i(q_i^{'}, \mathbf{q_{-i}}) \tag{27}$$

and

$$I_j(q_i, \mathbf{q_{-i}}) \geq I_j(q_i^{'}, \mathbf{q_{-i}}) \tag{28}$$

where $\mathbf{q_{-i}}$ denotes the price of other relay nodes except R_i. From (27) and (28), we see that the problem becomes to show that $\partial I_i(\mathbf{q})/\partial q_i \geq 0$ and $\partial I_j(\mathbf{q})/\partial q_i \geq 0$. We conclude that above inequalities are satisfied after deduction process. Therefore, monotonicity property is proved. □

V. Utility Maximization in CKS Game

In this section, we consider the CKS game. According to (5), (7) and (8), instead of being a constant, the capacity of the wiretap link is affected by its CSI. Therefore, the algorithm applied in CUS game cannot be used here to get the optimal strategies for the source and relay nodes.

A. Relay Selection

Since relay nodes have different local CSIs and ask for different unit prices for helping the same source node, each source node has its own preference on the relay nodes.

Denote $\theta_i = |h_{R_iD}|^2/|h_{R_iE}|^2 = \gamma_{R_iD}/\gamma_{R_iE}$ as the ratio of the power gain between the R_i-D and R_i-E links. When the secrecy capacity is positive, C^{S_k} in (8) is rewritten as,

$$\begin{aligned} C^{S_k} &= W\log_2(1+\textstyle\sum_{i=1}^{N}\frac{P_{S_k}P_{R_i}^{S_k}\gamma_{S_kR_i}\theta_i\gamma_{R_iE}}{1+P_{S_k}\gamma_{S_kR_i}+P_{R_i}^{S_k}\theta_i\gamma_{R_iE}}) - \\ &\quad W\log_2(1+\textstyle\sum_{i=1}^{N}\frac{P_{S_k}P_{R_i}^{S_k}\gamma_{S_kR_i}\gamma_{R_iE}}{1+P_{S_k}\gamma_{S_kR_i}+P_{R_i}^{S_k}\gamma_{R_iE}}) \end{aligned} \tag{29}$$

By setting the C^{S_k}'s derivative with respect to θ_i,

$$\begin{aligned} \frac{\partial C^{S_k}}{\partial\theta_i} &= \frac{W}{\ln 2}\frac{1}{(1+\sum_{i=1}^{N}\frac{P_{S_k}P_{R_i}^{S_k}\gamma_{S_kR_i}\theta_i\gamma_{R_iE}}{1+P_{S_k}\gamma_{S_kR_i}+P_{iS_k}\theta_i\gamma_{R_iE}})}\times \\ &\quad \frac{P_{S_k}P_{R_i}^{S_k}\gamma_{S_kR_i}\gamma_{R_iE}(1+P_{S_k}\gamma_{S_kR_i})}{(1+P_{S_k}\gamma_{S_kR_i}+P_{R_i}^{S_k}\theta_i\gamma_{R_iE})^2} > 0. \end{aligned} \tag{30}$$

We see C^{S_k} is increasing with θ_i and $C^{S_k} = 0$ only if $\theta_i = 1, i = 1, 2, \cdots, N$. Thus, to secure the data transmission, relay IoT nodes with a higher power gain on the wiretap link will be discarded. The remaining relay IoT nodes form a new set $\mathcal{L} = \{R_1, R_2, \cdots R_L\}$.

B. Stage II: Power Equilibrium

Similar to that in CUS game, the source node S_k is considered. Its secrecy capacity is ensured to be positive with selected feasible relay IoT nodes. Given the unit price $\mathbf{q}$, the utility maximization problem (15) in State II becomes,

$$\max_{\mathbf{P_R^{S_k}}} \alpha C^{S_k}(\mathbf{P_R^{S_k}}) - \textstyle\sum_{i=1}^{L} q_i P_{R_i}^{S_k} \tag{31}$$

$$\text{s.t.} \quad 0 \leq P_{R_i}^{S_k} \leq P_{R_i}^{max}/K, i = 1, 2, \cdots, L$$

$$C^{S_k}(\mathbf{P_R^{S_k}}) > C_0 \tag{32}$$

Motivated by [31], we combine the penalty function method and the differential convex programming (DC programming) to maximize (31), which is equivalent to,

$$\min_{\mathbf{P_R^{S_k}}} \textstyle\sum_{i=1}^{L} q_i P_{R_i}^{S_k} - \alpha C^{S_k}(\mathbf{P_R^{S_k}}) \tag{33}$$

1) Obtaining Exact Penalty: To simplify the minimization, penalty function method [32] is deployed to merge the constraint (32) into the objective function (33), which transforms the original problem to,

$$\begin{aligned} \min_{\mathbf{P_R^{S_k}}} \quad & \textstyle\sum_{i=1}^{N} q_i P_{R_i}^{S_k} - \alpha C^{S_k}(\mathbf{P_R^{S_k}}) + \beta_m C^{+}(\mathbf{P_R^{S_k}}) \\ & 0 \leq P_{R_i}^{S_k} \leq P_{R_i}^{max}/K, i = 1, 2, \cdots, L \end{aligned} \tag{34}$$

where the penalty function $C^{+}(\mathbf{P_{r_k}})$ is constructed as,

$$C^{+}(\mathbf{P_R^{S_k}}) = \max\{-C^{S_k}(\mathbf{P_R^{S_k}}) + C_0, 0\}. \tag{35}$$

β_m is a suitable penalty factor. Based on [31], there exists $\beta > 0$ such that for every $\beta_m > \beta$ the problem in (33) is equivalent to the penalty problem in (34), which can be solved given β_m using DC programming. Since a larger β_m may increase the difficulty to solve the penalty problem, we start β_m with a small value and scale it up by a scaling factor $d > 1$ to make the problems (33) and (34) equivalent. The algorithm to obtain the exact penalty factor is as follows.

Algorithm 2: Obtaining Exact Penalty

Input: Pricing $\mathbf{q}$, convergence threshold ϵ, the index of update m, and the maximum allowed number of m, M_ϵ
Output: $\mathbf{P_R^{S_k}}(\mathbf{q})$

```
Choose an initial value β_0, set m = 0 and C^+(P_R^{S_k})^{(β_0)} = R_0;
while β_m C^+(P_R^{S_k})^{(β_m)} < ε and m < M_ε do
    Given β_m, using DC Programing algorithm to solve (34) to otain the
      optimal P_R^{S_k (β_m)};
    Calculate β_m C^+(P_R^{S_k})^{(β_m)};
    β_{m+1} = dβ_m;
    m = m + 1;
end
return P_R^{S_k}(q) = P_R^{S_k (β_m)};
```

THEOREM 2. *Algorithm 2 is convergent.*

Proof: Assume (34) is solvable. Then $\mathbf{P_R^{S_k}}^{(\beta_m)}$ and $\mathbf{P_R^{S_k}}^{(\beta_{m+1})}$ are the optimal solutions of (34) given β_m and β_{m+1}, respectively. We have,

$$\begin{aligned} &\sum_{i=1}^{L} q_i P_{R_i}^{S_k(\beta_m)} - \alpha C^{S_k}(\mathbf{P_R^{S_k}})^{(\beta_m)} + \beta_m C^{+}(\mathbf{P_R^{S_k}})^{(\beta_m)} \leq \\ &\sum_{i=1}^{L} q_i P_{R_i}^{S_k(\beta_{m+1})} - \alpha C^{S_k}(\mathbf{P_R^{S_k}})^{(\beta_{m+1})} + \beta_m C^{+}(\mathbf{P_R^{S_k}})^{(\beta_{m+1})}, \\ &\sum_{i=1}^{L} q_i P_{R_i}^{0} S_k(\beta_{m+1}) - \alpha C^{S_k}(\mathbf{P_R^{S_k}})^{(\beta_{m+1})} + \beta_{m+1} C^{+}(\mathbf{P_R^{S_k}})^{(\beta_{m+1})} \\ &\leq \sum_{i=1}^{L} q_i P_{R_i}^{S_k(\beta_m)} - \alpha C^{S_k}(\mathbf{P_R^{S_k}})^{(\beta_m)} + \beta_{m+1} C^{+}(\mathbf{P_R^{S_k}})^{(\beta_m)} \end{aligned}$$

respectively. By adding the above two inequalities, we get,

$$C^{+}(\mathbf{P_R^{S_k}})^{(\beta_{m+1})} \leq C^{+}(\mathbf{P_R^{S_k}})^{(\beta_m)} \tag{36}$$

where $C^{+}(\mathbf{P_R^{S_k}})^{(\beta_m)}$ is decreasing with β_m. Since $C^{+}(\mathbf{P_R^{S_k}})$ is decreasing, Algorithm 2 is convergent. □

2) Solving Penalty Problem: Given the penalty factor β_m, we introduce an auxiliary variable $t \in \mathbb{R}$ and reformulate (34),

$$\begin{aligned}\min_{\mathbf{P_R^{S_k}}} U'_{S_k}(\mathbf{P_R^{S_k}}) = &\sum_{i=1}^{N} q_i P_{R_i}^{S_k} - \alpha C^{S_k}(\mathbf{P_R^{S_k}}) + \\ &\beta_m(t + C_E^{S_k}(\mathbf{P_R^{S_k}})) \\ \text{s.t.} - &C_E^{S_k}(\mathbf{P_R^{S_k}}) + C_0 \le t \\ - &C_E^{S_k}(\mathbf{P_R^{S_k}}) \le t \\ &0 \le P_{R_i}^{S_k} \le P_{R_i}^{max}/K, i = 1, 2, \cdots, L\end{aligned}$$

For convenience, we denote the feasible set as,

$$\begin{aligned}\mathcal{S} = \{(\mathbf{P_R^{S_k}}, t) : &-C_D^{S_k}(\mathbf{P_R^{S_k}}) + C_0 \le t, -C_E^{S_k}(\mathbf{P_R^{S_k}}) \le \\ &t, 0 \le P_{R_i}^{S_k} \le P_{R_i}^{max}/K, i = 1, 2, \cdots, L, t \in R\}\end{aligned} \quad (37)$$

By dividing the objective function $U'_{S_k}(\mathbf{P_R^{S_k}})$ into two convex functions, we have

$$U^{S'_k}(\mathbf{P_R^{S_k}}, t) = U_1^{S_k}(\mathbf{P_R^{S_k}}, t) - U_2^{S_k}(\mathbf{P_R^{S_k}}) \quad (38)$$

where

$$U_1^{S_k}(\mathbf{P_R^{S_k}}, t) = \sum_{i=1}^{N} q_i P_{R_i}^{S_k} - \alpha C_D^{S_k}(\mathbf{P_R^{S_k}}) + \beta_m t \quad (39)$$

and

$$U_2^{S_k}(\mathbf{P_R^{S_k}}) = -(\beta_m + \alpha) C_E^{S_k}(\mathbf{P_R^{S_k}}) \quad (40)$$

The problem in (34) is a standard DC programming problem now. We solve it iteratively with a sequential convex program,

$$\begin{aligned}\min_{(\mathbf{P_R^{S_k}}, t) \in \mathcal{S}} &U_1^{S_k}(\mathbf{P_R^{S_k}}, t) - U_2^{S_k}(\mathbf{P_{R\,(n)}^{S_k}}) - \\ &< \nabla U_2^{S_k}(\mathbf{P_{R\,(n)}^{S_k}}), \mathbf{P_R^{S_k}} - \mathbf{P_{R\,(n)}^{S_k}} >\end{aligned} \quad (41)$$

In particular, $\nabla U_2^{S_k}(\mathbf{P_R^{S_k}}) = \left(\frac{\partial U_2^{S_k}}{\partial P_{R_1}^{S_k}}, \frac{\partial U_2^{S_k}}{\partial P_{R_2}^{S_k}}, \cdots, \frac{\partial U_2^{S_k}}{\partial P_{R_N}^{S_k}}\right)$ in (41) represents the gradient with respect to $\mathbf{P_R^{S_k}}$, where

$$\frac{\partial U_2^{S_k}}{\partial P_{R_i}^{S_k}} = -\frac{W(\beta_m + \alpha)}{\ln 2} \frac{\frac{\gamma_{S_k R_i} \gamma_{R_i E} P_{S_k} (1 + \gamma_{S_k R_i} P_{S_k})}{(1 + \gamma_{S_k R_i} P_{S_k} + \gamma_{R_i E} P_{R_i}^{S_k})^2}}{\left(1 + \sum_{i=1}^{L} \frac{P_{S_k} P_{R_i}^{S_k} \gamma_{S_k R_i} \gamma_{R_i E}}{1 + P_{S_k} \gamma_{S_k R_i} + P_{R_i} S_k \gamma_{R_i E}}\right)^2} \quad (42)$$

We propose Algorithm 3 to minimize the objective function in (41). According to [31], the $U^{S'_k}(\mathbf{P_{R\,(n+1)}^{S_k}})$ obtained is decreasing, and thus Algorithm 3 is convergent.

Algorithm 3: DC Programing Algorithm

Input: P_{S_k}, β_m, convergence threshold ξ, N_ξ
Output: $\mathbf{P_R^{S_k}}^{(\beta_m)}$

Set the initial value $\mathbf{P_{R\,(n)}^{S_k}} = \mathbf{c}$ and $n = 0$;
Compute $U^{S'_k}(\mathbf{P_{R\,(0)}^{S_k}})$;
while $|U^{S'_k}(\mathbf{P_{R\,(n+1)}^{S_k}}) - U^{S'_k}(\mathbf{P_{R\,(n)}^{S_k}})| \le \xi$ *and* $n < N_\xi$ **do**
  Based on $U^{S'_k}(\mathbf{P_{R\,(n)}^{S_k}})$, solving (41) to obtain $\mathbf{P_{R\,(n+1)}^{S_k}}$ using convex programming;
  Calculate $U^{S'_k}(\mathbf{P_{R\,(n+1)}^{S_k}})$;
  $n = n + 1$;
end
return $\mathbf{P_R^{S_k}}^{(\beta_m)} = \mathbf{P_{R\,(n)}^{S_k}}$;

Since both Algorithm 2 and Algorithm 3 are convergent, the power equilibrium for each source node is obtained given the price of relay nodes.

C. Stage I: Optimal Pricing

Similar to that in the CUS game, we update the price of each relay node as in (20). In practice, each selected relay node R_i listens to the instantaneous feedback information about $P_{R_i}^{S_k *}$ and $\partial P_{R_i}^{S_k *}/\partial p_i$ from the source node. In addition, it is natural for each relay node to regulate the unit price of its power as $q_i = c_i$, because a lower price q_i will result in a negative utility U_i while a higher price q_i would be at the risk of being excluded by the source node at the beginning.

VI. Performance Analysis and Evaluation

In this section, we analyze the complexity for both the CUS and CKS game and evaluate their performance by both the simulations and experiments using real-world dataset.

A. Complexity Analysis

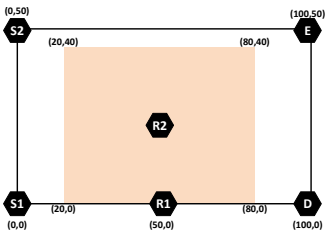
1) CUS Game (CUSG): The problem of obtaining the strategies for both the source nodes and relay IoT nodes can be divided into two subproblems iteratively. First, for the utility maximization of source nodes, the optimal power is easily obtained according to Algorithm 1. Second, for the utility maximization of relay IoT nodes, the key to the price update is to calculate the partial derivative with respect to the unit price. Even if there are multiple relay IoT nodes, the source node updates the price for relay IoT nodes at one time and does not have to interact with each relay IoT node individually [21]. Hence, the expense of the communication between the source and relay IoT nodes is largely reduced.

2) CKS Game (CKSG): The problem of obtaining the strategies for both the source and relay nodes is divided into three subproblems hierarchically. From Algorithm 2, Algorithm 3, and the Eq (20), the computational complexity of the proposed utility maximization method heavily depends on the DC programming and the derivatives with respect to the unit price of each relay IoT node. Since the convex subproblem in DC programming can be solved by many standard convex optimization methods, the utility maximization problem for the source node given the unit price can be easily solved.

B. Performance Evaluation Settings

To demonstrate the feasibility of our proposed game-theoretical approaches, we conduct both simulations and experiments using real-world datasets under both wiretap-link CSI known and unknown cases. In the wiretap-link CSI known case, we mainly consider the secrecy capacity performance, while the price, the power, and utilities of the source/relay nodes are focused in the wiretap-link CSI unknown case.

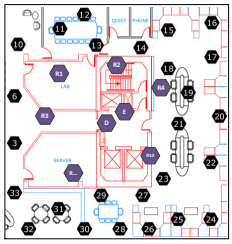
1) Simulation Setting: We mainly consider the following three cases, Single-Source Single-Relay (SSSR), Single-Source Multiple-Relay (SSMR), and Multiple-Source Multiple-Relay (MSMR), where we choose 2 nodes in the multiple source/relay cases. Note that these can be easily extended into the scenario with more than two source/relay nodes. The simulation settings are given in Fig. 2a and Tab. 2b.



(a) Location in CKSG

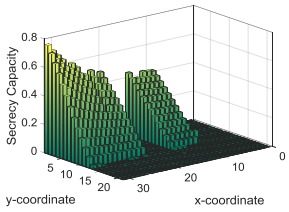
Simulation Parameter	Values
maximum power of the source node	10mW
maximum power of the relay IoT node	100mW
variance of the noise σ^2	10^{-8}
path loss of the static Rayleigh channel	2
transmission bandwidth W	1 (Normalization)
gain per unit of secrecy capacity α	0.01
unit cost of transmission power c_i	0.01
secrecy capacity constraint in CKSG	0.01bit/s/Hz
supreme secrecy capacity in CUSG	1bit/s/Hz

(b) System Parameters in Simulation

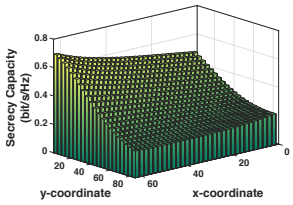


(c) Location in Dataset

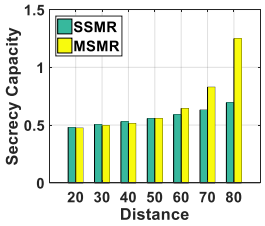
Fig. 2: System Settings



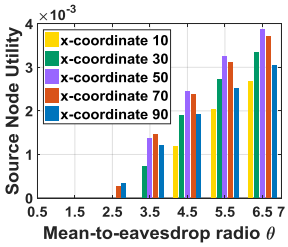
(a) SSSR



(b) SSMR

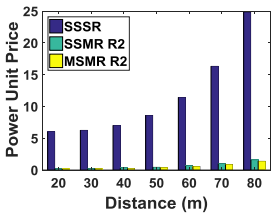


(c) MSMR

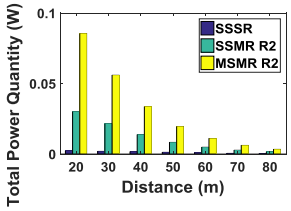


(d) Utility Vs. Power Gain (SSMR)

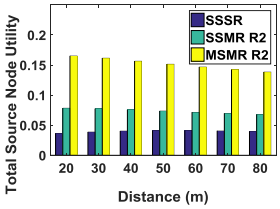
Fig. 3: Security Performance in CKSG



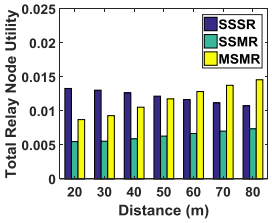
(a) Power Unit Price



(b) Total Power Quantity



(c) Total Source Node Utility



(d) Total Relay Node Utility

Fig. 4: Comparison between SSSR and SSMR in CUSG

2) Experiment Setting: We use the data from 54 sensors deployed in the Intel Berkeley Research lab [33] as shown in Fig. 2c. These sensors collect timestamped topology information, along with humidity, temperature, light and voltage values once every 31 seconds. We consider one of the circles surrounded by 26 nodes (No.3, No.6, and No.10-33). In addition, we assume there is a destination node D located at the center of the circle $(10m, 15m)$. An eavesdropper E $(12m, 18m)$ near the destination node attempts to intercept the sensed data information from all the source nodes.

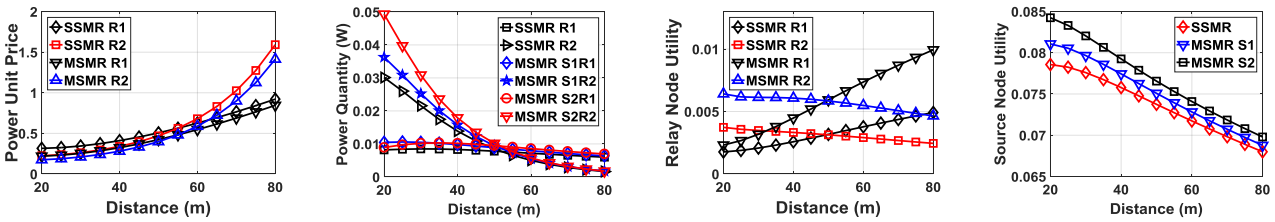
C. Security Performance in CKSG

The secrecy capacity performance in the CKSG simulation is demonstrated in Fig.3, where 'x-coordinate' and 'y-coordinate' in Fig.3a and Fig. 3b denote the location of relay nodes. The 'Distance' represents the horizontal location difference between the source node S_1 and relay nodes. For SSSR (S_1, R_2, D and E) scenario, S_1 is fixed and R_2 is moving in the red area in Fig.2a. For SSMR (S_1, R_1, R_2, D and E) scenario, a new relay IoT node R_1 is introduced, which is fixed at the location $(50m, 0m)$. Extending to MSMR (S_1, S_2, R_1, R_2, D and E) scenario, the source node S_2 is added and fixed at the location $(0m, 50m)$.

1) Effect of Multiple Relay Nodes: The location of R_2 has a strong effect on the secrecy capacity as shown in Fig.3a and Fig.3b. Particularly, when R_2 is near the destination node, the secrecy capacity is largely improved. This is because the power gain ratio between the relay-destination link and the relay-eavesdropper link increases as R_2 moves to the destination node. Besides, the comparison between Fig.3a and Fig.3b demonstrates that the introduction of R_1 increases the total secrecy capacity. Since R_1 close to the destination node D instead of the eavesdropper E, it can help forward the data from S_1 while preventing it from being intercepted by the eavesdropper. The security performance is improved.

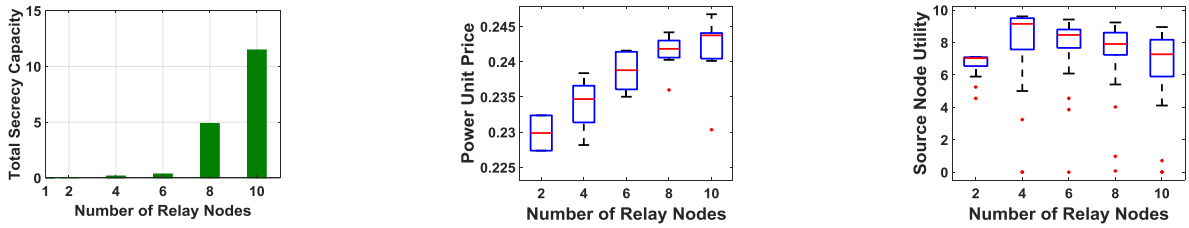
2) Effect of Multiple Source Nodes: Fig.3c compares the secrecy capacity performance under the SSMR and MSMR scenarios. When the relay node R_2 moves from the source node to the destination node, the power gain radio between the S_2-R_2-D link and the the S_2-R_2-E link becomes larger. The introduction of the new source node S_2 improves the total secrecy capacity as shown in Fig.3c.

3) Main-to-Eavesdropper Link Ratio Effect: We draw the relationship between the utility of the source node and the power gain ratio in SSMR scenario in Fig.3d, where y-coordinate of the relay node R_2 is assumed to be 0. In Fig.3d, the power gain ratio θ brings a positive effect to the source node utility. When $\theta \leq 1$, the utility of the source node keeps 0, which shows that the relay selection in the CKS game is infeasible. In addition, the source node's utility is still 0 even



(a) Power Unit Price (b) Total Power Quantity (c) Total Relay Node Utility (d) Total Source Node Utility

Fig. 5: Comparison between SSMR and MSMR in CUSG



(a) Secrecy Capacity in CKSG (b) Power Unit Price (CUSG) (c) Source Node Utility (CUSG)

Fig. 6: Experimental Results

if $\theta > 1$. Since the source node has to purchase the power from each relay node, it has to get a larger secrecy capacity in order to ensure its utility. In contrast to that in Fig.3b, the source node's utility gets maximized when R_2 is in the middle of the source and destination node. When R_2 is near to the destination node, it uses less power to forward the data. To get more benefits, R_2 requests a higher unit price, which decreases the utility of the source node. When R_2 is near the source node, it has to use more power for transmission. According to Eq.(15), the source node's utility is thus decreased.

D. Utility Performance in CUSG

In this subsection, we demonstrate the utility performance for both the source and relays nodes in CUSG. In particular, we keep the location of S_1, D and E while changing the location of S_2 and R_1 to $(0m, 25m)$ and $(50m, 25m)$, respectively, in both SSMR (S_1, R_1, R_2, D and E) and MSMR (S_1, S_2, R_1, R_2, D and E) scenarios. Meanwhile, we suppose R_1 in SSSR (S_1, R_1, D and E) scenario and R_2 in other scenarios are moving from $(20m, 25m)$ to $(80m, 25m)$ in a straight line to see the changes on the price, power and utility of both source and relay nodes.

1) Effect of Multiple Relay Nodes: Fig.4 compares the performance in all ways between SSSR and SSMR scenarios. Particularly, we show the effect brought by the moving relay node R_2 in SSMR scenarios. Specifically, due to competition, introducing a new relay IoT node lowers the power unit price obviously as shown in Fig.4a. In the SSSR scenario, the source node purchases a smaller amount of power from the relay IoT node since the power is too expensive. Whereas in the SSMR and MSMR scenarios, the low power unit price stimulates the source nodes to purchase more power. Meanwhile, the relay IoT nodes can use their power to forward the data from the source nodes as much as possible as shown in Fig.4b. As a result, the power unit price and power quantity co-determine the utility of the source and relay nodes shown in Fig.4c and Fig.4d, where the introduction of the relay nodes increases the utility of source nodes and brings a slightly negative effect on other relay IoT nodes.

2) Mutual Effect among Relay Nodes: We mainly consider the SSMR scenarios, where R_1 is fixed at $(50m, 25m)$ and R_2 is moving. When R_2 is close to S_1, it uses more power to forward the S_1's data. Thus, a low power unit price is enough to get a high utility for R_2. Since S_1 buys less power from R_1, R_1 has to increase its unit price to maximize its utility. However, as R_2 is moving far away from S_1, it sells less power to S_1. R_2 has to increase the power unit price. Seeing that R_2 increases its unit price, R_1 also increases its own price as shown in Fig.5a. As a result, both R_1' power unit price and the power quantity sold to S_1 change even if it does not move as reflected in Fig.5a and Fig.5b. Obviously, the utility of R_2 is increasing when it is close to S_1 while becoming less as it is moving to D as shown in Fig.5c. Given less power and more unit price, the utility of the source node decreases as demonstrated in Fig.5d.

3) Effect of Multiple Source Nodes: The performance in all ways between SSMR and MSMR scenarios is compared in Fig.5, where Fig.5a and Fig. 5b show the changes of power unit price and quantity when introducing a new source node S_2. Suppose each relay node has enough harvested energy to forward the source nodes' data. Compared to the distance to S_1, R_2 is always close to S_2. R_2 sells more power to S_2 than to S_1. As R_2 continues moving, such distance difference becomes less. The power sold to S_1 and S_2 is almost the same. That is why the power quantity sold to S_1 and S_2 is similar for R_1. With more source nodes, the competition between relay IoT nodes becomes more fierce. Both relay nodes would like to sell more power to source nodes, which benefits source nodes' utilities. As shown in Fig.5d, the utility of each source node is more in MSMR scenario compared to that in SSMR scenario. Since each relay node sells more power with almost the same unit price, they get more utilities as shown in Fig.5c.

E. Real-world Experimental Results

To show the performance of CKSG and CUSG, we conduct the experiment using real-world dataset as shown in Fig.6. We first verify the effect brought by multiple relay IoT nodes in CKSG. The total secrecy capacity of all the 26 participating source nodes is illustrated in Fig.6a. Obviously, the introduction of more relay nodes indeed improves the security performance when the wire-tap link CSI is known. Note that we assume at most 10 relay IoT nodes help forward data. With more relay nodes, the interference among them would deteriorate the data transmission. In CUSG, the competition among relay nodes increases the power unit price as given in Fig.6b. As power unit price becomes larger, the source nodes will not purchase more power. Thus, the average source node utility is increasing and then decreasing as more relay IoT nodes help forward the data as shown in Fig.6c.

VII. Conclusion

In this paper, we design a cooperative IoT system for ensuring communication security. To benefit the relay nodes in forwarding the data to defend against the eavesdropping attack, we propose two Stackelberg games, namely CUS game and CKS game, working under the wiretap-link CSI unknown and known cases, respectively. Our simulation and experiment results show that the game-theoretical approach improves the utility of source nodes and defends against the eavesdropping attack, and thus enhances the security for IoT systems effectively.

References

[1] Y. Li, K. Chi, H. Chen, Z. Wang, and Y. h. Zhu, "Narrowband internet of things systems with opportunistic d2d communication," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2017.

[2] 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.

[3] X. Zhang, Q. Jia, and L. Guo, "Secure and optimized unauthorized secondary user detection in dynamic spectrum access," in *Communications and Network Security (CNS), 2017 IEEE Conference on*. IEEE, 2017, pp. 1–9.

[4] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, June 2015.

[5] L. Song, K. K. Chai, Y. Chen, J. Schormans, J. Loo, and A. Vinel, "Qos-aware energy-efficient cooperative scheme for cluster-based iot systems," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1447–1455, 2017.

[6] Z. He, X. Zhang, Y. Bi, W. Jiang, and Y. Rong, "Optimal source and relay design for multiuser mimo af relay communication systems with direct links and imperfect channel information," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2025–2038, 2016.

[7] W. Jiang, Z. He, X. Zhang, Y. Bi, and Y. Rong, "Joint transceiver design for amplify-and-forward multiuser mimo relay communication systems with source-destination links," *Journal of Communications*, vol. 10, no. 7, 2015.

[8] W. Xu, X. Zhang, J. Zhai, and J. Lin, "On the achievable rate of mimo cognitive radio network with multiple secondary users," in *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*. IEEE, 2014, pp. 1–5.

[9] M. S. Omar, S. A. R. Naqvi, S. H. Kabir, and S. A. Hassan, "An experimental evaluation of a cooperative communication-based smart metering data acquisition system," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 399–408, 2017.

[10] L. Song, K. K. Chai, Y. Chen, J. Loo, and J. Schormans, "Cooperative coalition selection for quality of service optimization in cluster-based capillary networks," *IEEE Systems Journal*, 2016.

[11] A. Bader and M.-S. Alouini, "Localized power control for multihop large-scale internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 503–510, 2016.

[12] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[13] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers stackelberg game scheme," *IEEE Transactions on Information Forensics and Security*, 2017.

[14] X. Zhang, P. Huang, Q. Jia, and L. Guo, "Cream: Unauthorized secondary user detection in fading environments," in *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2018, pp. 406–414.

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

[16] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.

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

[18] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, 2015.

[19] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[20] P. K. Dutta, *Strategies and games: theory and practice*. MIT press, 1999.

[21] B. Wang, Z. Han, and K. R. Liu, "Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game," *IEEE Transactions on Mobile Computing*, vol. 8, no. 7, pp. 975–990, 2009.

[22] N. C. Luong, P. Wang, D. Niyato, Y.-C. Liang, Z. Han, and F. Hou, "Applications of economic and pricing models for resource management in 5g wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, 2018.

[23] Z. Xiong, S. Feng, D. Niyato, P. Wang, A. Leshem, and Y. Zhang, "Game theoretic analysis for joint sponsored and edge caching content service market," *arXiv preprint arXiv:1808.04067*, 2018.

[24] X. Zhang, L. Guo, M. Li, and Y. Fang, "Motivating human-enabled mobile participation for data offloading," *IEEE Transactions on Mobile Computing*, vol. 17, no. 7, pp. 1624–1637, 2018.

[25] ——, "Social-enabled data offloading via mobile participation-a game-theoretical approach," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–6.

[26] H. Fang, L. Xu, and K.-K. R. Choo, "Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks," *Applied Mathematics and Computation*, vol. 296, pp. 153–167, 2017.

[27] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[28] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for wanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1117–1128, 2015.

[29] D. Fudenberg and J. Tirole, "Game theory," The MIT press, Tech. Rep., 1991.

[30] R. D. Yates, "A framework for uplink power control in cellular radio systems," *IEEE Journal on selected areas in communications*, vol. 13, no. 7, pp. 1341–1347, 1995.

[31] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in af relaying," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 740–752, 2016.

[32] M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, *Nonlinear programming: theory and algorithms*. John Wiley & Sons, 2013.

[33] "Intel lab data," http://db.csail.mit.edu/labdata/labdata.html.