Xu, Yang; Liu, Jia; Shen, Yulong; Liu, Jun; Jiang, Xiaohong; Taleb, Tarik

Incentive Jamming-Based Secure Routing in Decentralized Internet of Things

Published in:
IEEE Internet of Things Journal

DOI:
10.1109/JIOT.2020.3025151

Published: 15/02/2021

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Xu, Y., Liu, J., Shen, Y., Liu, J., Jiang, X., & Taleb, T. (2021). Incentive Jamming-Based Secure Routing in Decentralized Internet of Things. *IEEE Internet of Things Journal*, *8*(4), 3000-3013. Article 9199881. https://doi.org/10.1109/JIOT.2020.3025151

Incentive Jamming-based Secure Routing in Decentralized Internet of Things

Yang Xu, *Member, IEEE,* Jia Liu, *Member, IEEE,* Yulong Shen, *Member, IEEE,* Jun Liu, *Member, IEEE,* Xiaohong Jiang, *Senior Member, IEEE* and Tarik Taleb, *Senior Member, IEEE*

***Abstract*—This paper focuses on the secure routing problem in decentralized Internet of Things (IoT). We consider a typical decentralized IoT scenario composed of peer legitimate devices, unauthorized devices (eavesdroppers) and selfish helper jamming devices (jammers), and propose a novel incentive jamming-based secure routing scheme. For a pair of source and destination, we first provide theoretical modeling to reveal how the transmission security performance of a given route is related to the jamming power of jammers in the IoT. Then, we design an incentive mechanism with which the source pays some rewards to stimulate the artificial jamming among selfish jammers, and also develop a two-stage Stackelberg game framework to determine the optimal source rewards and jamming power. Finally, with the help of the theoretical modeling as well as the source rewards and jamming power setting results, we formulate a shortest weighted path-finding problem to identify the optimal route for secure data delivery between the source-destination pair, which can be solved by employing the Dijkstra's or Bellman-Ford algorithm. We prove that the proposed routing scheme is *individually rational*, *stable*, *distributed* and *computationally efficient*. Simulation and numerical results are provided to demonstrate the performance of our routing scheme.**

***Index Terms*—IoT security, routing, incentive mechanism, jamming, physical layer security.**

I. Introduction

THE rapid evolution of communication technologies has spawned the emergence of the Internet of Things (IoT). With the concept of "anything connected anytime" in IoT, billions of physical devices around the world are expected to be connected to the Internet via heterogeneous access technologies circa 2020 [1], [2]. Wireless communication is a critical enabling technology for connecting IoT devices, and there are two types of wireless connectivity: i) centralized connectivity such as cellular systems (e.g., LTE and 5G) and wireless wide-area networks (e.g., LoRaWAN), and ii) decentralized connectivity such as ad hoc, mesh and opportunistic networks. The majority of IoT devices employ short-range communication techniques like Bluetooth Low Energy and Zigbee. Therefore, the decentralized connectivity-based topology formation can play a pivotal role in achieving plug and play characteristics of IoT devices. This paper focuses on decentralized IoT.

Due to the inherent openness of wireless medium, data delivery through wireless communication is vulnerable to eavesdropping attacks by unauthorized devices (eavesdroppers), posing a serious threat to IoT security [3]. Conventionally, cryptography is widely used to protect communication security [4]. However, the secret key distribution and management are costly and complicated to be implemented in decentralized IoT. In addition, the cryptographic-based methods could be broken as the opponent's computing capability improves greatly, e.g., when quantum computing is available. These trigger an increasing review of physical layer security (PLS) technology recently, which exploits the natural characteristics of wireless channels to provide information-theoretic security, guaranteeing that eavesdroppers can never decode information from the transmitted data regardless of their computational capability [5], [6].

PLS technology has the advantages of low computational complexity, easy implementation in a decentralized manner, and no need to distribute/manage secret key, and thus employing it to protect data delivery security in various wireless communication systems (including IoT) has been attracting considerable academic attention [7]–[11]. To guarantee PLS performance in such systems, diverse mechanisms have been proposed in the literature. For example, the PLS enhancement based on the approaches of diversity, signal processing, and cross-layer optimization can be found in [12], [13] and [14], respectively. The works of [15], [16] indicated that coding schemes can be developed for ensuring PLS performance. Hu

This work was supported in part by the National Natural Science Foundation of China under Grant 61802292, in part by JSPS KAKENHI Grant Number JP20K14742, in part by the Project of Cyber Security Establishment with Inter University Cooperation, in part by the National Key R&D Program of China under Grant 2018YFE0207600 and Grant 2018YFB2100403, in part by Japan JSPS Grant No.18H03235, in part by the China NSFC under Grant 61972308 and Grant 61902214, in part by the Academy of Finland Project CSN under Grant Agreement 311654, in part by the 6Genesis project under Grant No. 318927, and in part by the Tsinghua University Initiative Scientific Research Program 2019Z08QCX19. *(Corresponding author: Jia Liu.)*

Yang Xu is with the School of Economics and Management, Xidian University, Xi'an 710071, China (email: yxu@xidian.edu.cn).

Jia Liu is with the Center for Cybersecurity Research and Development, National Institute of Informatics, Tokyo 101-8430, Japan (email: jliu@nii.ac.jp).

Yulong Shen is with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China (email: ylshen@mail.xidian.edu.cn).

Jun Liu is with the Institute of Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China, and also with Beijing National Research Center for Information Science and Technology (BNRist), Beijing, China (email: juneliu@tsinghua.edu.cn).

Xiaohong Jiang is with the School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan (email: jiang@fun.ac.jp).

Tarik Taleb is with the Department of Communications and Networking, School of Electrical Engineering, Aalto University, Finland (e-mail: tarik.taleb@aalto.fi). He is also with the Faculty of Information Technology and Electrical Engineering, Oulu University, and with the Department of Computer and Information Security, Sejong University, Seoul 05006, South Korea.

et al. [17] proposed a jamming-based scheme to improve PLS of downlink transmission in IoT. He *et al.* [18] put forward a link selection policy to optimize PLS-QoS tradeoffs in two-hop relay systems. In addition, the cooperative relaying and jamming strategies for PLS enhancement were comprehensively demonstrated in [19] and the references therein.

A. *Motivation and Our Main Contributions*

As mentioned before, devices in decentralized IoT usually adopt short-range communication due to the power limitation. Hence, data of a source may need to be forwarded by several intermediate devices to reach its destination when the distance between the source and destination is far. In this context, it is essential to leverage a routing scheme to establish the route (path) for end-to-end data delivery. Unfortunately, existing studies on the design of PLS-based schemes mainly focus on either the single-hop (point-to-point) or two-hop relay systems, which are not applicable to the multi-hop decentralized IoT scenario. It is also worth noting that to ensure PLS performance, some mechanisms, such as [17], utilize extra devices to generate artificial jamming, where voluntary participation/cooperation is assumed. However, to generate jamming signals to deteriorate the reception at the eavesdropper, jammers need to consume their own power. Therefore, a jammer may not voluntarily participate in the cooperation unless it gains satisfying rewards to compensate for its power consumption. Such selfishness is more in line with the inherent characteristics of a device in practical IoT scenarios since devices are usually resource-limited. On the other hand, without adequate cooperation, the PLS performance of a mechanism may not achieve a qualified level.

Motivated by the above observations, in this paper, we for the first time propose a lightweight routing solution to secure data delivery in decentralized IoT. Taking into account the inherent selfishness of devices, we introduce an incentive mechanism into the routing design, aiming to facilitate cooperation between the source device and jammers. Specifically, the source provides jammers with rewards (payments) to stimulate them to generate jamming signals, such that the PLS performance of data delivery can be enhanced; while jammers individually compete for the rewards based on their contributions to the PLS enhancement to compensate for the power consumption. We develop a two-stage Stackelberg game-based framework to determine the optimal source rewards and jamming power. With the help of this framework, we formulate a shortest weighted path-finding problem to identify the optimal route for data delivery in the IoT, which can be solved by employing the Bellman-Ford or Dijkstra's algorithm.

The main contributions of this paper are summarized as follows:

- There is no existing scheme intended for secure data delivery in multi-hop decentralized IoT. To fill this void, this paper is the first to provide a lightweight routing solution, where an incentive mechanism is incorporated to stimulate artificial jamming to guarantee PLS performance.

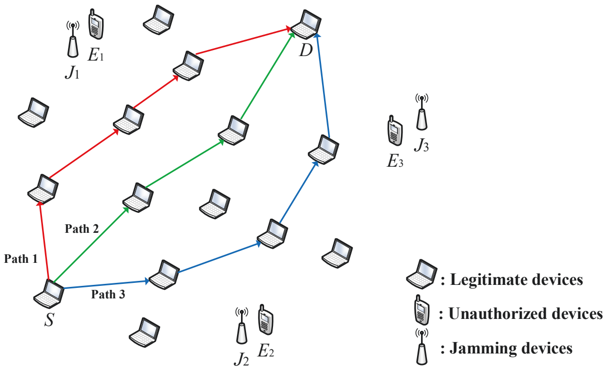


Fig. 1. Network model.

- We evaluate the PLS performance of a given route under a general configuration. Based on the performance evaluation, we employ a two-stage Stackelberg game to design the incentive mechanism: At the first stage, the source determines the optimal rewards for maximizing its utility; at the second stage, each jammer independently strategizes its jamming power to compete for the rewards based on its contribution to the PLS enhancement, which is formulated as a non-cooperative game. We demonstrate and compute the unique Stackelberg Equilibrium, which paves the way for the optimal route selection between the source and destination devices.
- Due to the elaborate design of the incentive mechanism, we can formulate a shortest weighted path-finding problem to identify the optimal route for data delivery in the IoT. We assign the corresponding weight to each link and apply Bellman-Ford or Dijkstra's algorithm to determine the optimal route, such that the incentive jamming-based secure routing design is completed. We demonstrate that the proposed routing scheme is individually rational, stable, distributed and computationally efficient.

B. *Paper Organization*

The remainder of this paper is organized as follows. Section II introduces the system models. Section III analyzes the PLS performance of a general route. We design the incentive mechanism in Section IV and propose the routing scheme in Section V. Simulation results are presented in Section VI. Section VII provides the related work, followed by the conclusion in Section VIII.

II. System Models

A. *Network Model*

As illustrated in Fig. 1, we consider a decentralized IoT that consists of arbitrarily distributed legitimate peer devices. The number of devices is N and each device uses a fixed power P to transmit a signal. Due to the transmission range limitation, data could be delivered from its source to its destination through multiple hops (links) in the IoT. L denotes the number of all available legitimate links in the IoT. Without loss of generality, we focus on a pair of source-destination devices, denoted as S and D, respectively. When S wants to transmit a message to D, there could be several candidate end-to-end paths (routes) through which the message can be delivered. We use $\Pi = \langle l_1, \cdots, l_K \rangle$ to represent a K-hop path composed of K links from l_1 to l_K, where a link $l_k \in \Pi$ connects two intermediate devices S_k and D_k on path Π, and $S_1 = S$, $S_k = D_{k-1}$, $D_K = D$. We use $\mathcal{P}$ to denote the set of all available paths between S and D.

There also exist M unauthorized devices (potential malicious eavesdroppers) which may intercept the transmitted message in a passive way. The set of eavesdroppers is denoted as $\mathcal{E} = \{E_i, i = 1, 2, \cdots, M\}$ and their locations are assumed to be known. This assumption is also widely adopted in other works of PLS-based routing design (such as [20], [21]) because it could characterize some practical scenarios. On the one hand, it can model the scenario where legitimate devices suspect the presence of malicious eavesdroppers at specific pre-determined locations (e.g., in military or battlefield applications). On the other hand, it is also applicable to the scenario where all devices are legitimate participants (and thus their locations are available) but some data is not intended for all devices. For example, for premium data, only the devices who have paid for it (legitimate receivers) can receive, while the reception of other devices ("eavesdroppers") should be denied. An eavesdropper E_i can intercept the transmission of all links on a path. The widely-used randomize-and-forward (RF) relay strategy [22] is adopted to avoid any eavesdropper decoding the message by combining different links' signals.

To enhance data delivery security, jamming devices (jammers) can be employed to deteriorate the data reception at eavesdroppers by transmitting jamming signals. However, since IoT devices are usually resource-limited, we assume jammers are selfish and thus will not voluntarily generate jamming signals unless they gain satisfying rewards to compensate for their power consumption. To establish a secure route for data delivery, source S recruits a set of jammers denoted as $\mathcal{J} = \{J_i, i = 1, 2, \cdots, M\}$, each jammer J_i is placed near the position of eavesdropper E_i correspondingly. The source grants jammers a total of rewards R to stimulate artificial jamming, while jammers compete for the rewards individually based on their contributions to the PLS enhancement. Taking both cost (i.e., power consumption) and return (i.e., rewards) into consideration, each jammer aims to maximize its own utility by making a strategy to determine its jamming power P_{J_i}. The source is also interested in maximizing its own utility by deciding an appropriate total of rewards R.

B. Wireless Channel Model

We consider that the wireless channel between any pair of transmitter X and receiver Y is characterized by the large-scale path loss along with the small-scale Rayleigh fading. The path loss exponent is denoted as α (typically between 2 and 6). The channel coefficient between X and Y is denoted as $h_{X,Y}$ and the channel gain $|h_{X,Y}|^2$ is exponentially distributed with mean $\mathbb{E}\{|h_{X,Y}|^2\} = 1$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. Such a wireless channel model is widely employed in the literature related to the physical layer [22], [23]. Note that for the considered IoT scenario, the artificial jamming signals are regarded as noise by eavesdroppers, and the jamming power at an eavesdropper could be much more dominant than the background noise power (because the source device aims to stimulate artificial jamming for PLS enhancement). Hence, we consider the widely-used interference-limited model and neglect the background noise [22], [23][1].

The frequently used notations are listed in Table I.

TABLE I
MAIN NOTATIONS.

Notation	Definition
N	number of peer legitimate devices
L	number of legitimate links
E_i, $\mathcal{E}$	an eavesdropper and the set of eavesdroppers
J_i, $\mathcal{J}$	a jammer and the set of jammers
M	number of eavesdroppers (jammers), i.e., $M = \lvert\mathcal{E}\rvert = \lvert\mathcal{J}\rvert$
Π, $\mathcal{P}$	a path and the set of paths
Π^{opt}	optimal path selected by the source
K	number of hops on a path
l_k	a link which connects two intermediate devices S_k and D_k on path Π
P	transmitting power of an legitimate device
$d_{X,Y}$	distance between X and Y
$h_{X,Y}$	channel coefficient between X and Y
α	path-loss exponent
γ_E	threshold of SIR for decoding the message at an eavesdropper
P_{so}	secrecy outage probability
P_{J_i}	jamming power (strategy) of J_i
$\mathbf{P_J}$	strategy profile of all jammers
$\mathbf{P}_{-J_i}$	strategy profile excluding P_{J_i}
U_{J_i}	utility function of jammer J_i
R	rewards paid by (strategy of) the source
U_S	utility function of the source

III. PLS Performance Modeling

In this section, we evaluate the PLS performance for a given path in the decentralized IoT under a general configuration, which lays the foundation for the incentive mechanism design in the next section.

We adopt secrecy outage probability (SOP) as the measurement to evaluate the PLS performance of a path in a decentralized IoT. For a transmission through an individual link l_k, the event of secrecy outage refers to the case when the SIR (signal-to-interference ratio) at one or more eavesdroppers is above a specified threshold γ_E, such that the message can be decoded by the eavesdropper(s). The SOP of this link $P_{so}(l_k)$ is defined as the probability the event of secrecy outage happens. Due to the RF relay strategy, we can evaluate the SOP of a path by treating each link on this path independently. Therefore, the SOP of a path Π, denoted as $P_{so}(\Pi)$, is defined as the probability that no link experiences secrecy outage when a message is delivered through this path.

[1] The interference-limited model will simplify the routing design greatly. In addition, the PLS performance derived under this model is a lower approximation of the actual one. It implies that the proposed routing scheme actually may implement data delivery more securely.

It is worth mentioning that in Wyner's encoding scheme [5], the transmitter chooses two rates, i.e., the rate of transmitted codewords r_t and the rate of confidential messages r_s. The rate difference $r_e = r_t - r_s$ reflects the cost for securing the messages against the eavesdroppers. When the wiretap channel capacity is higher than r_e, the secrecy outage happens. According to Shannon's Theorem, the channel capacity is determined by the corresponding SIR at the receiver. Thus, the definition of SOP based on the SIR threshold can be easily mapped to that based on the Wyner's encoding scheme, where the conversion between the SIR threshold and code rate is $\gamma_E = 2^{r_e} - 1$. The SIR-based formulation of SOP is also widely used in other studies, e.g., [22].

Regarding the evaluation of $P_{so}(\Pi)$, we have the following lemma.

Lemma 1: For a concerned IoT under a general configuration, i.e., the jamming power P_{J_i} of jammer J_i is arbitrarily set, the upper bound of SOP of a path $P_{so}(\Pi)$ is given by

$$P_{so}(\Pi) = 1 - \exp\left(-P \cdot \sum_{l_k \in \Pi} \omega_k\right), \tag{1}$$

where $\omega_k = \dfrac{1}{\gamma_E} \displaystyle\sum_{i=1}^{M} \dfrac{d^{\alpha}_{J_i,E_i}}{P_{J_i} d^{\alpha}_{S_k,E_i}}$ and d_{S_k,E_i} (resp. d_{J_i,E_i}) denotes the distance between S_k (resp. J_i) and E_i.

Proof: We first derive the expression of $P_{so}(l_k)$, i.e., the SOP of a link l_k on path Π. For the transmission from S_k to D_k, we let x_{S_k} and x_{J_i} denote the normalized (unit power) symbol stream to be transmitted by S_k and the i^{th} jammer J_i, respectively. P and P_{J_i} are the transmitting power and jamming power correspondingly. For an eavesdropper $E_i \in \mathcal{E}$, let y_{E_i} denote its received signal. Then we have

$$y_{E_i} = \frac{\sqrt{P} h_{S_k,E_i}}{d^{\alpha/2}_{S_k,E_i}} x_{S_k} + \sum_{J_j \in \mathcal{J}} \frac{\sqrt{P_{J_j}} h_{J_j,E_i}}{d^{\alpha/2}_{J_j,E_i}} x_{J_j}. \tag{2}$$

According to expression (2) and the definition of SOP, $P_{so}(l_k)$ can be formulated as

$$P_{so}(l_k) = \mathbb{P}\left\{\max_{E_i \in \mathcal{E}} \frac{P|h_{S_k,E_i}|^2/d^{\alpha}_{S_k,E_i}}{\sum\limits_{J_j \in \mathcal{J}} P_{J_j}|h_{J_j,E_i}|^2/d^{\alpha}_{J_j,E_i}} > \gamma_E\right\} \tag{3}$$

$$\leq \mathbb{P}\left\{\max_{E_i \in \mathcal{E}} \frac{P|h_{S_k,E_i}|^2/d^{\alpha}_{S_k,E_i}}{P_{J_i}|h_{J_i,E_i}|^2/d^{\alpha}_{J_i,E_i}} > \gamma_E\right\}. \tag{4}$$

We can see that expression (4) is an upper bound of $P_{so}(l_k)$, which means the exact PLS performance can be better than that in the case of using the upper bound as an approximation. Such an approximation can be close to the exact SOP in the considered network scenario because the interference at an eavesdropper caused by its corresponding jammer is much more dominant than that caused by other jammers. Moreover, by using this approximation, we can easily measure the contribution of a jammer to the PLS enhancement when designing the incentive mechanism, as well as reduce greatly the computational complexity of the entire routing framework, as shown in the subsequent sections.

We further convert (4) into (5), shown at the bottom of this page.

Note that for each eavesdropper E_i, the corresponding jammer J_i is placed near the position of E_i. Thus, we have $d^{\alpha}_{J_i,E_i} \ll d^{\alpha}_{S_k,E_i}$ and then $\frac{P d^{\alpha}_{J_i,E_i}}{\gamma_E P_{J_i} d^{\alpha}_{S_k,E_i}} \ll 1$. Following the approximation that $1 + x \approx e^x$ when $0 < x \ll 1$, (5) can be further transformed as

$$\begin{aligned} P_{so}(l_k) &= 1 - \prod_{i=1}^{M} \left(\frac{1}{1 + \frac{P d^{\alpha}_{J_i,E_i}}{\gamma_E P_{J_i} d^{\alpha}_{S_k,E_i}}}\right) \\ &\approx 1 - \prod_{i=1}^{M} \exp\left(-P \frac{d^{\alpha}_{J_i,E_i}}{\gamma_E P_{J_i} d^{\alpha}_{S_k,E_i}}\right) && (6) \\ &= 1 - \exp\left(-\frac{P}{\gamma_E} \sum_{i=1}^{M} \left(\frac{d^{\alpha}_{J_i,E_i}}{P_{J_i} d^{\alpha}_{S_k,E_i}}\right)\right) \\ &= 1 - \exp\left(-P \omega_k\right). && (7) \end{aligned}$$

Therefore, the SOP of path Π can be calculated as

$$\begin{aligned} P_{so}(\Pi) &= 1 - \prod_{l_k \in \Pi} \{1 - P_{so}(l_k)\} && (8) \\ &= 1 - \exp\left(-P \cdot \sum_{l_k \in \Pi} \omega_k\right). \end{aligned}$$

■

Remark 1: It is worth noting that jamming signals also influence the quality of service (QoS) of legitimate transmissions, but we can expect two promising ways to mitigate or eliminate their impacts. 1) Since legitimate devices and jammers are cooperators, it is possible for the receiver to know the characteristics of jamming signals, and thus it can

$$\begin{aligned} P_{so}(l_k) &= \mathbb{P}\left\{\max_{E_i \in \mathcal{E}} \frac{P|h_{S_k,E_i}|^2/d^{\alpha}_{S_k,E_i}}{P_{J_i}|h_{J_i,E_i}|^2/d^{\alpha}_{J_i,E_i}} > \gamma_E\right\} = 1 - \prod_{i=1}^{M} \mathbb{P}\left\{\frac{P|h_{S_k,E_i}|^2/d^{\alpha}_{S_k,E_i}}{P_{J_i}|h_{J_i,E_i}|^2/d^{\alpha}_{J_i,E_i}} < \gamma_E\right\} \\ &= 1 - \prod_{i=1}^{M} \left\{1 - \mathbb{E}_{|h_{J_i,E_i}|^2}\left\{\exp\left(\frac{-\gamma_E P_{J_i}|h_{J_i,E_i}|^2 d^{\alpha}_{S_k,E_i}}{P d^{\alpha}_{J_i,E_i}}\right)\right\}\right\} = 1 - \prod_{i=1}^{M} \left(1 - \frac{1}{1 + \frac{\gamma_E P_{J_i} d^{\alpha}_{S_k,E_i}}{P d^{\alpha}_{J_i,E_i}}}\right) \\ &= 1 - \prod_{i=1}^{M} \left(\frac{1}{1 + \frac{P d^{\alpha}_{J_i,E_i}}{\gamma_E P_{J_i} d^{\alpha}_{S_k,E_i}}}\right). && (5) \end{aligned}$$

utilize the technique of interference cancellation to subtract jamming signals from the combined received signal. 2) Several classical spatial domain signal processing methods can be employed for wireless interference management. For example, when directional antennas or multiple antennas are available at a jammer, it can employ beamforming techniques to steer its jamming signal just in the direction of the corresponding eavesdropper; when multiple antennas are available at the legitimate receiver, jamming signals can be nullified by aligning the receive filter's main lobe in the direction of the transmitter. Regarding the research on the techniques and strategies for QoS performance improvement, please kindly refer to the corresponding literature, e.g., [24]–[28].

IV. Incentive Mechanism Design

From the theoretical performance modeling in the previous section, we know that a larger jamming power P_{J_i} will lead to a lower SOP. However, due to the inherent selfishness of the jammers, they are not willing to generate jamming signals to help establish a secure route, unless they gain satisfying rewards to compensate for their power consumption. To this end, in this section, we design an incentive mechanism based on the game-theoretic approach to stimulate artificial jamming for PLS performance enhancement.

We first give a general introduction to the Stackelberg game. The Stackelberg game, which is also termed as the leader-follower game, is initially proposed by Stackelberg in 1952 based on some economic monopolization phenomena [29]. The Stackelberg game features strategic interactions among rational agents in markets on which some hierarchical competition takes place. In such a hierarchical game, the declaring player can be in a position to enforce its own strategies upon the other players. Thus, the player who holds the strong position and that can impose its own strategy upon the others is called the leader while the players who react to the leader's declared strategy are called followers. The problem is to find an optimal strategy for the leader, assuming that the followers react in such a rational way that they optimize their objective functions given the leader's actions [30], [31].

We then provide an overall description of our incentive mechanism. As illustrated in Fig. 2, we model the incentive mechanism as a Stackelberg game, which we term as the PLS-enhancing game. The PLS-enhancing game is composed of two stages: at Stage I, the source device (i.e., the leader) determines the rewards R that is granted to the jammers to maximize its utility; at Stage II, each jammer (i.e., the follower) strategizes its jamming power to maximize its own utility. Thus, both the source and jammers are players in the PLS-enhancing game. The strategy of the source is its rewards R, and the strategy of jammer J_i is its jamming power P_{J_i}. We use $\mathbf{P}_J = (P_{J_1}, P_{J_2}, \cdots, P_{J_M})$ to denote the strategy profile containing all jammers' strategies, and $\mathbf{P}_{-J_i}$ to denote the strategy profile excluding P_{J_i}, i.e., $\mathbf{P}_J = (P_{J_i}, \mathbf{P}_{-J_i})$. Note that due to the selfishness of jammers, at Stage II all jammers compete with each other individually for gaining parts of the total rewards from the source. Thus, the competition among jammers can be modeled as a non-cooperative game. We term this game as the Jamming Power Determination (JPD) game.

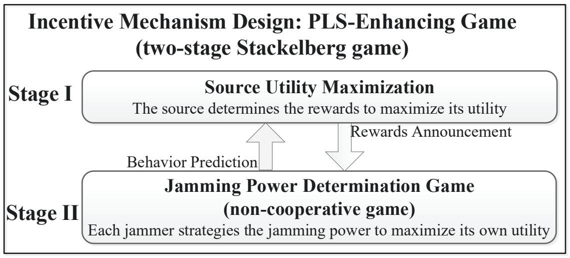

Incentive Mechanism Design: PLS-Enhancing Game
(two-stage Stackelberg game)
Stage I
Source Utility Maximization
The source determines the rewards to maximize its utility
Behavior Prediction
Rewards Announcement
Stage II
Jamming Power Determination Game
(non-cooperative game)
Each jammer strategies the jamming power to maximize its own utility

Fig. 2. Incentive mechanism design.

Remark 2: It is worth emphasizing that with our incentive mechanism, on the one hand, the source and jammers are cooperators in the sense that the source grants jammers rewards to stimulate artificial jamming for PLS enhancement. On the other hand, jammers are in competition with each other since they compete for the rewards individually. Therefore, the competition behaviors among jammers are modeled as a typical non-cooperative game in the Game Theory. The interplay between the source and jammers, together with the non-cooperative game among jammers, constitute a typical two-stage Stackelberg game.

In Section IV-A, we will design the utility functions for the source and jammers which are reasonable and have provably good properties, completing the PLS-enhancing game formulation, and then we are interested in investigating the following problems:

P1: For given rewards R, is there a stable strategy profile in the JPD game, such that no jammer can gain more utility by unilaterally changing its current strategy?

P2: If the result in P1 is yes, is the stable strategy profile unique? If unique, it can be guaranteed that jammers will certainly choose the strategies in this stable strategy profile.

P3: How can the source determine the value of rewards R to maximize its own utility?

It is worth noting that the stable strategy profile in P1 corresponds to the concept of Nash Equilibrium (NE) in Game Theory [31], which can be defined as follow.

Definition 1 (Nash Equilibrium): A strategy profile $\mathbf{P}_J^{ne} = (P_{J_1}^{ne}, P_{J_2}^{ne}, \cdots, P_{J_M}^{ne})$ is a Nash Equilibrium of the JPD game, if for any jammer J_i and any strategy $P_{J_i} \geq 0$ we have

$$U_{J_i}(P_{J_i}^{ne}, \mathbf{P}_{-J_i}^{ne}) \geq U_{J_i}(P_{J_i}, \mathbf{P}_{-J_i}^{ne}), \tag{9}$$

where U_{J_i} denotes the utility function of J_i.

The existence and uniqueness of NE are of great importance, since they enable the source to predict the behaviors of all jammers and thus decide the optimal value of R in a backward inductive way. That is to say, the result of P3 depends heavily on P1 and P2. The unique NE of the JPD game together with the optimal solution derived in P3 form the solution to the PLS-enhancing game.

A. Utility Function Design

We first design the utility function for jammers. It is reasonable to design that the jammers compete for the total rewards from the source based on their contributions to the transmission security performance of a path. In other words, the rewards that a jammer can receive should be proportional to the contribution it makes to the artificial jamming. Note that a jammer is leveraged to generate the jamming signal at its corresponding eavesdropper as revealed in expression (2). Thus, we characterize the contribution of jammer J_i approximately as $P_{J_i} \cdot r_i$, where r_i is the contribution factor given by

$$r_i = d_{J_i,E_i}^{-\alpha}. \tag{10}$$

The cost of J_i for artificial jamming is computed as $c \cdot P_{J_i}$, where $c > 0$ is the unit cost of jamming power. Then, the utility function U_{J_i} of jammer J_i is formulated as

$$U_{J_i} = \frac{P_{J_i} r_i}{\sum_{J_j \in \mathcal{J}} P_{J_j} r_j} R - c P_{J_i}, \tag{11}$$

i.e., rewards minus cost. Since a rational jammer is not willing to participate in the artificial jamming for a negative utility, J_i will set $P_{J_i} = 0$ when $R \leq \frac{c}{r_i} \sum_{J_j \in \mathcal{J} \setminus \{J_i\}} P_{J_j} r_j$. In Section IV-B, we will demonstrate that the designed jammer utility function also has the favorable property of ensuring the existence and uniqueness of NE in the JPD game.

We next design the utility function U_S for the source. A desirable formulation of U_S needs to satisfy the following properties:

1) Since the source stimulates the artificial jamming for PLS enhancement, U_S should be a monotonically decreasing function of $P_{so}(\Pi)$.
2) To ensure the uniqueness of the solution to the PLS-enhancing game, the formulation of U_S should result in a unique optimal value of R for maximizing U_S.
3) Since the final goal is to design a secure routing scheme, the formulation of U_S should result in a good computational efficiency in finding the optimal path, i.e., we can employ some efficient path-finding algorithms rather than the exhaustive search method.

With the above observations and being aware of the structure of $P_{so}(\Pi)$ in expression (1), we formulate the source utility function as

$$U_S = \frac{\lambda}{1 - \ln(1 - P_{so}(\Pi))} - R, \tag{12}$$

where $\lambda > 1$ is a system parameter. In the following text, we will abbreviate $P_{so}(\Pi)$ as P_{so} if there is no ambiguity.

Computing the first-order derivative of U_S with respect to P_{so}, we have

$$\frac{\partial U_S}{\partial P_{so}} = -\frac{\lambda}{[1 - \ln(1 - P_{so})]^2 (1 - P_{so})} < 0. \tag{13}$$

Thus, U_S is a monotonically decreasing function of P_{so}, satisfying the property 1). Moreover, we plot the curve of $f(x) = \frac{1}{1-\ln(1-x)}$ in Fig. 3. We can find that for a large range of P_{so}, U_S decreases almost linearly as P_{so} increases, while when P_{so} is very high, for example, more than 0.9, U_S diminishes sharply. Such a behavior accords with the intuitive desirable requirement of the source utility. It will be demonstrated later that the designed source utility in (12) also satisfies the properties 2) and 3).

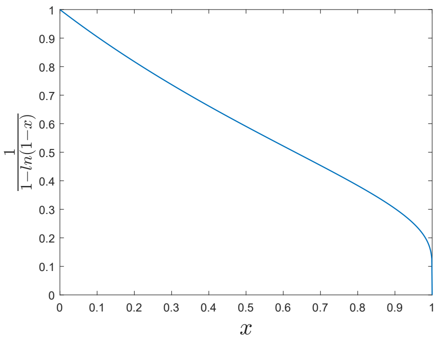


Fig. 3. Curve of $f(x) = \frac{1}{1-\ln(1-x)}$.

B. Jamming Power Determination

In the JPD game, every jammer individually competes with each other for gaining a part of given total rewards R. Therefore, the JPD game is modeled as a non-cooperative game. As a notational convention, we use $G = (\mathcal{J}, \{\mathbf{P}_J\}, \{U_{J_i}\})$ to denote the JPD game, where $\mathcal{J}$, $\{\mathbf{P}_J\}$ and $\{U_{J_i}\}$ are the sets of players (i.e., jammers), strategy profiles and utility functions, respectively. To achieve its maximal utility, each player will play its best response strategy in the JPD game, which is defined as follow.

Definition 2 (Best Response Strategy): Given $\mathbf{P}_{-J_i}$, a strategy is the best response strategy of jammer J_i, denoted as $b_i(\mathbf{P}_{-J_i})$, if it satisfies $U_{J_i}(b_i(\mathbf{P}_{-J_i}), \mathbf{P}_{-J_i}) \geq U_{J_i}(P_{J_i}, \mathbf{P}_{-J_i})$ for all $P_{J_i} \geq 0$.

According to the definition of NE, we know that every jammer plays its best response strategy in an NE. Therefore, the strategy profile which all jammers play in the JPD game will converge to an NE, if it exists. Regarding the existence of an NE in a non-cooperative game, we have the following proposition [32, Theorem 1].

Proposition 1: An NE exists in the JPD game $G = (\mathcal{J}, \{\mathbf{P}_J\}, \{U_{J_i}\})$, if: i) $\{\mathbf{P}_J\}$ is a nonempty, compact and convex subset of the M-dimensional Euclidean space $\mathbf{R}^M$; ii) U_{J_i} is concave on P_{J_i}, for every $J_i \in \mathcal{J}$.

Since the strategy of player J_i is $P_{J_i} \geq 0$, the strategy space of the JPD game $\{\mathbf{P}_J\}$ is a nonempty, compact and convex subset of the M-dimensional Euclidean space $\mathbf{R}^M$. Taking the first- and second-order derivatives of U_{J_i} with respect to P_{J_i} yields

$$\frac{\partial U_{J_i}}{\partial P_{J_i}} = \frac{R r_i}{\sum_{J_j \in \mathcal{J}} P_{J_j} r_j} - \frac{R P_{J_i} r_i^2}{\left(\sum_{J_j \in \mathcal{J}} P_{J_j} r_j\right)^2} - c, \tag{14}$$

$$\frac{\partial^2 U_{J_i}}{\partial P_{J_i}^2} = -2 \frac{R r_i^2 \sum_{J_j \in \mathcal{J} \setminus \{J_i\}} P_{J_j} r_j}{\left(\sum_{J_j \in \mathcal{J}} P_{J_j} r_j\right)^3} < 0. \tag{15}$$

We see that U_{J_i} is continuous and differentiable on P_{J_i}, and the second-order derivative of $U_{P_{J_i}}$ with respect to P_{J_i} is negative. Therefore, U_{J_i} is a concave function of P_{J_i}. With the above statements, we prove the following theorem.

Theorem 1: There exists at least an NE in the JPD game $G = (\mathcal{J}, \{\mathbf{P}_J\}, \{U_{J_i}\})$.

Next, we check the uniqueness of NE in the JPD game. Let $\mathbf{b}(\mathbf{P}_J) = (b_1(\mathbf{P}_{-J_1}), b_2(\mathbf{P}_{-J_2}), \cdots, b_M(\mathbf{P}_{-J_M}))$, which we term as the best response correspondence of the game. By definition, we know that an NE is actually a fixed point of the best response correspondence $\mathbf{b}(\mathbf{P}_J)$, i.e., $\mathbf{P}_J^{ne} = \mathbf{b}(\mathbf{P}_J^{ne})$. Therefore, the uniqueness of NE is equivalent to that the function $\mathbf{b}(\mathbf{P}_J)$ has a unique fixed point, and we have the following proposition [33, Theorem 1].

Proposition 2: If the function $\mathbf{b}(\mathbf{P}_J)$ is *standard*, then its fixed point is unique.

Regarding the standard function, we have the following definition.

Definition 3: Function $\mathbf{b}(\mathbf{P}_J)$ is standard if for all $\mathbf{P}_J \geq 0$, the following properties are satisfied.

- positivity: $\mathbf{b}(\mathbf{P}_J) > 0$.
- monotonicity.
- scalability: for all $\beta > 1$, $\beta\mathbf{b}(\mathbf{P}_J) > \mathbf{b}(\beta\mathbf{P}_J)$.

Note that U_{J_i} is a concave function of P_{J_i}, and thus the best response strategy $b_i(\mathbf{P}_{-J_i})$ can be obtained by setting the first-order derivative of U_{J_i} with respect to P_{J_i} to be 0, which yields

$$\frac{Rr_i}{\sum_{J_j \in \mathcal{J}} P_{J_j} r_j} - \frac{RP_{J_i} r_i^2}{\left(\sum_{J_j \in \mathcal{J}} P_{J_j} r_j\right)^2} - c = 0. \tag{16}$$

Solving P_{J_i} in (16), we have

$$P_{J_i} = \sqrt{\frac{R \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j} r_j}{c r_i}} - \frac{1}{r_i} \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j} r_j. \tag{17}$$

If the right hand side of (17) is positive, it is also the best response strategy of jammer J_i due to the concavity of U_i. If the right hand side of (17) is less than or equal to 0, then jammer J_i will not participate in the artificial jamming by setting $P_{J_i} = 0$. Hence, we can determine the best response strategy of J_i, as shown in formula (18) at the bottom of this page.

We see from (18) that for every jammer J_i which participates in the artificial jamming, its best response function $b_i(\mathbf{P}_{-J_i})$ is always positive and monotonic. As for scalability, we have

$$\beta b_i(\mathbf{P}_{-J_i}) - b_i(\beta\mathbf{P}_{-J_i}) = (\beta - \sqrt{\beta})\sqrt{\frac{R \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j} r_j}{c r_i}}. \tag{19}$$

For $\forall\beta > 1$ there is $\beta - \sqrt{\beta} > 0$. Thus, (19) is positive and $\beta\mathbf{b}(\mathbf{P}_J) > \mathbf{b}(\beta\mathbf{P}_J)$ holds.

In summary, the best response correspondence $\mathbf{b}(\mathbf{P}_J)$ is a standard function. As a result, we prove the following theorem.

Theorem 2: The JPD game has a unique NE.

According to Theorem 2, every player will play the strategy of the unique NE in the JPD game. We provide the following theorem for the computation of the NE.

Theorem 3: The unique NE for the JPD game is given by

$$P_{J_i}^{ne} = R \cdot \kappa_i, \tag{20}$$

where

$$\kappa_i = \left[\frac{1}{c}(M-1)\left(\sum_{j=1}^{M} \frac{r_i}{r_j} - M + 1\right)\left(\sum_{j=1}^{M} \frac{r_i}{r_j}\right)^{-2}\right]^+, \tag{21}$$

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

Proof: Note that every jammer plays its best response strategy in the NE, but a jammer cannot compute its best response strategy individually by using formula (18) since it contains the strategies of all other players. Let $S_i = \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j}^{ne} r_j$. By some basic algebraic transformations on expression (16) we know that for the NE $\mathbf{P}_J^{ne}$, there is

$$\begin{aligned} r_i S_i &= \frac{c}{R}(S_i + P_{J_i}^{ne} r_i)^2 = \frac{c}{R}\left(\sum_{J_k \in \mathcal{J}} P_{J_k}^{ne} r_k\right)^2 \\ &= \frac{c}{R}(S_j + P_{J_j}^{ne} r_j)^2 = r_j S_j,\ \forall J_i, J_j \in \mathcal{J}. \end{aligned}$$

Then we have $S_j = \frac{r_i}{r_j} S_i$ for $\forall J_j \in \mathcal{J}$ and obtain the following system of equations:

$$\begin{cases} S_1 = \frac{r_i}{r_1} S_i \\ S_2 = \frac{r_i}{r_2} S_i \\ \vdots \\ S_M = \frac{r_i}{r_M} S_i \end{cases}, \tag{22}$$

For (22), by calculating the sum of the left side and the sum of the right side separately, it yields

$$S_1 + S_2 + \cdots + S_M = \frac{r_i}{r_1} S_i + \frac{r_i}{r_2} S_i + \cdots + \frac{r_i}{r_M} S_i = \sum_{j=1}^{M} \frac{r_i}{r_j} S_i.$$

Since $S_j = \sum_{J_k \in \mathcal{J}\setminus\{J_j\}} P_{J_k}^{ne} r_k = S_i + P_{J_i}^{ne} r_i - P_{J_j}^{ne} r_j$, there is

$$\begin{aligned} \sum_{i=1}^{M} S_i &= M(S_i + P_{J_i}^{ne} r_i) - \sum_{j=1}^{M} P_{J_j}^{ne} r_j \\ &= M(S_i + P_{J_i}^{ne} r_i) - (S_i + P_{J_i}^{ne} r_i) \\ &= (M-1)(S_i + P_{J_i}^{ne} r_i) = \sum_{j=1}^{M} \frac{r_i}{r_j} S_i, \end{aligned} \tag{23}$$

and thus

$$S_i = \frac{(M-1) r_i P_{J_i}^{ne}}{\sum\limits_{j=1}^{M} \frac{r_i}{r_j} - M + 1}. \tag{24}$$

$$b_i(\mathbf{P}_{-J_i}) = \begin{cases} 0, & R \leq \frac{c}{r_i} \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j} r_j; \\ \sqrt{\frac{R \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j} r_j}{c r_i}} - \frac{1}{r_i} \sum_{J_j \in \mathcal{J}\setminus\{J_i\}} P_{J_j} r_j, & \text{otherwise} \end{cases} \tag{18}$$

Substituting (24) into (17) and performing some algebraic operations, we have

$$P_{J_i}^{ne} = \frac{R(M-1)\left(\sum\limits_{j=1}^{M}\frac{r_i}{r_j} - M + 1\right)}{c\cdot\left(\sum\limits_{j=1}^{M}\frac{r_i}{r_j}\right)^2} = R\cdot\kappa_i.$$

■

Theorem 3 also implies that the JPD game has a unique NE, which is the one computed by formula (20).

C. Source Utility Maximization

Based on the above analysis, the source, which serves as the employer in the PLS-enhancing game, is aware that for any given rewards R, there exists a unique NE at which every jammer adopts its jamming power. As a result, the source can maximize its own utility by choosing an optimal value of R.

Regarding the solution to the PLS-enhancing game, we have the following theorem.

Theorem 4: There exists a unique Stackelberg Equilibrium $(R^*, \mathbf{P}_J^{ne})$ in the PLS-enhancing game. R^* is the optimal rewards that maximize the source utility in (12) over $R \in [0, \infty)$, determined as

$$R^* = \sqrt{\lambda\Delta(\Pi)} - \Delta(\Pi), \tag{25}$$

where

$$\Delta(\Pi) = \frac{P}{\gamma_E}\sum_{l_k\in\Pi}\sum_{i=1}^{M}\frac{d_{J_i,E_i}^{\alpha}}{\kappa_i\cdot d_{S_k,E_i}^{\alpha}}, \tag{26}$$

and it is abbreviated as Δ if there is no ambiguity. $\mathbf{P}_J^{ne}$ is computed by formula (20) with the source rewards set to be R^*. The maximal utility U_S^* which can be achieved by the source is given by

$$U_s^* = \left(\sqrt{\lambda} - \sqrt{\Delta}\right)^2. \tag{27}$$

Proof: Substituting (1) into (12), U_S can be expressed as

$$U_S(R) = \frac{\lambda}{1 + \sum_{l_k\in\Pi} P\omega_k} - R. \tag{28}$$

Further substituting (20) into (28) we have

$$\begin{aligned} U_S(R) &= \frac{\lambda}{1 + \frac{P}{R\cdot\gamma_E}\sum\limits_{l_k\in\Pi}\sum\limits_{i=1}^{M}\frac{d_{J_i,E_i}^{\alpha}}{\kappa_i\cdot d_{S_k,E_i}^{\alpha}}} - R \\ &= \frac{\lambda}{1+\frac{\Delta}{R}} - R. \end{aligned} \tag{29}$$

Taking the first- and second-order derivatives of $U_S(R)$ with respect to R yields

$$\frac{\partial U_S}{\partial R} = \frac{\lambda\Delta}{(R+\Delta)^2} - 1, \tag{30}$$

$$\frac{\partial^2 U_S}{\partial R^2} = \frac{-2\lambda\Delta}{(R+\Delta)^3} < 0. \tag{31}$$

We can see that U_S is continuous and differentiable on R, and the second-order derivative is always negative. Hence, there exists a unique optimal value of R, termed as R^*, such that U_S can achieve its maximum. Since R^* satisfies that $\frac{\partial U_S}{\partial R}|_{R=R^*} = 0$, by setting (30) to be 0, R^* can be determined as

$$R^* = \sqrt{\lambda\Delta} - \Delta.$$

Substituting R^* into (29), U_S^* can be determined as

$$U_s^* = (\sqrt{\lambda} - \sqrt{\Delta})^2.$$

■

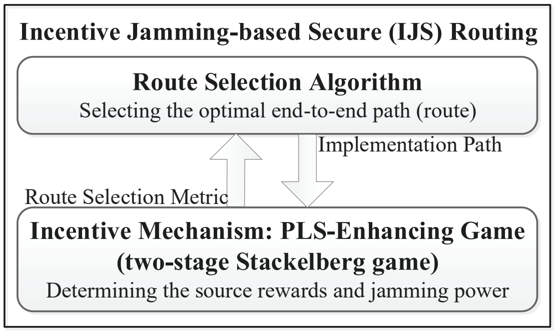

Incentive Jamming-based Secure (IJS) Routing
Route Selection Algorithm
Selecting the optimal end-to-end path (route)
Implementation Path
Route Selection Metric
Incentive Mechanism: PLS-Enhancing Game
(two-stage Stackelberg game)
Determining the source rewards and jamming power

Fig. 4. Framework of incentive jamming-based secure routing scheme.

Remark 3: Now we complete the design of the incentive mechanism. It can be seen that the proposed incentive mechanism is reasonable and shows some desirable properties. It is stable since the optimal strategy profile of the source and jammers is unique. It is implemented easily since the optimal strategies of the source and jammers are all in closed form. The expression of the optimal source utility also has a simple closed form, which will greatly facilitate the routing protocol design, i.e., enabling the route selection to be tractable by employing some efficient path-finding algorithms rather than the exhaustive search method.

V. Routing Design

In the previous section, we have designed the incentive mechanism for a given path, based on which we further investigate in this section the design of the **i**ncentive **j**amming-based **s**ecure routing, abbreviated as IJS.

A. IJS Routing Algorithm

As illustrated in Fig. 4, the framework of the IJS routing is composed of two layers. The bottom layer is the incentive mechanism, which formulates the behaviors of the source and jammers for a given path. The top layer is the route selection (path-finding) scheme, where the source selects the optimal end-to-end path that can maximize its utility when employing the incentive mechanism. Therefore, the entire IJS routing determines the optimal path through which the message is delivered, the optimal rewards that the source pays to stimulate artificial jamming, and the jamming power of the recruited jammers.

Note that for a pair of source S and destination D in a multi-hop decentralized IoT, there could exist multiple paths connecting them (see Fig. 1). The source employs the route selection scheme to find the optimal path to maximize its utility. Thus, the route selection problem can be formulated as

$$\max_{\Pi\in\mathcal{P};R;\mathbf{P}_J} \quad U_S(\Pi) \tag{32a}$$

$$\text{s.t.} \quad \text{PLS-enhancing game is played.} \tag{32b}$$

We use Π^{opt} to denote the selected optimal path, i.e.,

$$\Pi^{opt} = \arg\max_{\Pi\in\mathcal{L};R;\mathbf{P}_J} U_S(\Pi). \tag{33}$$

Based on the incentive mechanism and Theorem 4, the route selection problem is equivalent to

$$\max_{\Pi\in\mathcal{P}} \left(\sqrt{\lambda} - \sqrt{\Delta(\Pi)}\right)^2. \tag{34}$$

Thus, Π^{opt} can be determined as

$$\Pi^{opt} = \arg\min_{\Pi\in\mathcal{P}} \Delta(\Pi). \tag{35}$$

Substituting expression (26) into (35), we have

$$\begin{aligned}\Pi^{opt} &= \arg\min_{\Pi\in\mathcal{P}} \sum_{l_k\in\Pi} \sum_{i=1}^{M} \frac{d_{J_i,E_i}^{\alpha}}{\kappa_i \cdot d_{S_k,E_i}^{\alpha}} \\ &\triangleq \arg\min_{\Pi\in\mathcal{P}} \sum_{l_k\in\Pi} \Xi_k,\end{aligned} \tag{36}$$

where Ξ_k is given by

$$\Xi_k = \sum_{i=1}^{M} \frac{d_{J_i,E_i}^{\alpha}}{\kappa_i \cdot d_{S_k,E_i}^{\alpha}}. \tag{37}$$

From expression (36), we can see that the problem of optimal route selection is equivalent to finding the "shortest weighted path" which connects the source and its destination. With this important observation, we can assign each candidate link l_k a corresponding weight Ξ_k, and then find the path Π^{opt} which has a minimum sum link weight. This problem can be directly solved by the classical Bellman-Ford algorithm or the Dijkstra's algorithm [34], which returns the shortest path from a source vertex to all other vertices in a weighted graph.

After finding the shortest weighted path Π^{opt}, the IJS routing algorithm should execute remaining key operations, i.e., determining the corresponding rewards R of the source and jamming power of all jammers for path Π^{opt} based on formulas (25) and (20), respectively. The details of IJS routing algorithm are summarized in Algorithm 1.

Algorithm 1 Incentive Jamming-based Secure Routing Algorithm.

```
Input: Network topology and basic system parameters {$\alpha, \gamma_E, P, \lambda, c$};
Output: The optimal path $\Pi^{opt}$, the optimal rewards of the source $R^*$, and the optimal jamming power of every jammer $\mathbf{P}_J^{ne}$;
For every candidate link, compute the corresponding link weight according to formula (37);
Find the shortest path in terms of the sum link weight between the source and its destination. The classical Bellman-Ford or Dijkstra's algorithm can be used for this procedure;
Assign the shortest weighted path to $\Pi^{opt}$;
The source applies formula (25) to determine the optimal rewards $R^*$;
The source announces the rewards $R^*$ to all jammers;
Every jammer applies formula (20) to calculate the optimal jamming power $P_{J_i}^{ne}$;
return {$\Pi^{opt}, R^*, \mathbf{P}_J^{ne}$};
```

We next analyze the favorable properties the IJS routing algorithm possesses. According to the PLS-enhancing game, we know that every jammer which participates in the artificial jamming will have a non-negative utility, the source also pays an optimal value of rewards to maximize its utility. Thus, the IJS routing algorithm is *individually rational*. Since the link weight Ξ_k is non-negative, the Bellman-Ford or Dijkstra's algorithm ensures a definite shortest weighted path to be found. For this given path, the PLS-enhancing game ensures a unique Stackelberg Equilibrium that determines the rewards of the source and the jamming power of each jammer. Therefore, the IJS routing algorithm ensures the routing convergences to a unique solution and thus is *stable*. By exchanging information between neighboring devices, the Bellman-Ford or Dijkstra's algorithm enables a source device to compute the routing to its destination individually without a centralized control. Thus, the IJS routing algorithm is *distributed*.

We use the asymptotic notation O [35] to measure the computational complexity of the IJS routing algorithm, which mainly consists of three parts, i.e., computing the link weight, finding the shortest path, and computing the rewards and jamming power. According to formula (37), the complexity for computing the link weight is $O(LM)$. Note that there is $L \leq N(N-1)/2$, and thus the complexity for computing the link weight is $O(MN^2)$. The computational complexities of Bellman-Ford and Dijkstra's algorithm are $O(N^3)$ and $O(N^2)$, respectively, much lower than that of the exhaustive search method whose complexity is $O((N-2)!)$. According to formulas (25) and (20), the complexity for computing the rewards and jamming power is $O(M^2)$. Since usually $M < N$ holds for a general network configuration, we can summarize that the computational complexity of the IJS routing algorithm is $O(N^3)$. Therefore, the IJS routing algorithm can be computed in polynomial time and thus is *computationally efficient*.

The above statements prove the following theorem.

Theorem 5: IJS routing algorithm is individually rational, stable, distributed and computationally efficient.

B. IJS Routing Implementation

It is worth noting that performing the required tasks of the IJS routing is almost the same as that of a classical ad hoc routing, except that the source device needs to interact with jammers. According to the features and requirements of an IoT, the practical implementation of IJS routing can be either in a proactive way (table-driven) like OLSR [36] or a reactive way (on-demand) like AODV [37]. For example, for a static IoT that requires low latency, the IJS routing should be

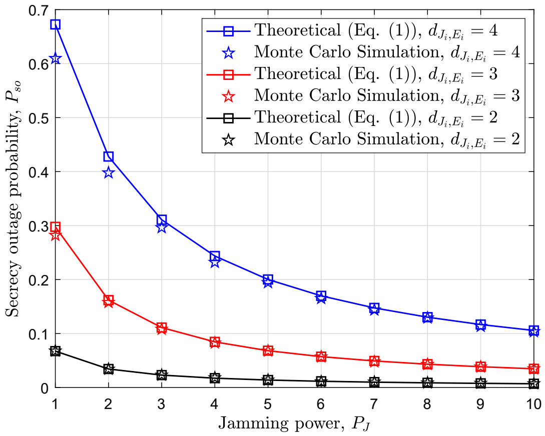


Fig. 5. Validation of theoretical PLS performance analysis.

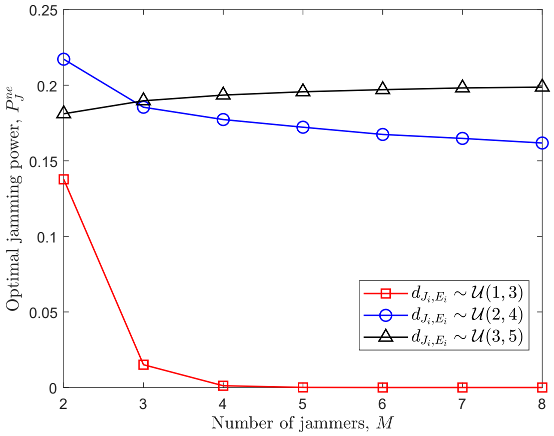


Fig. 6. Optimal jamming power versus number of jammers.

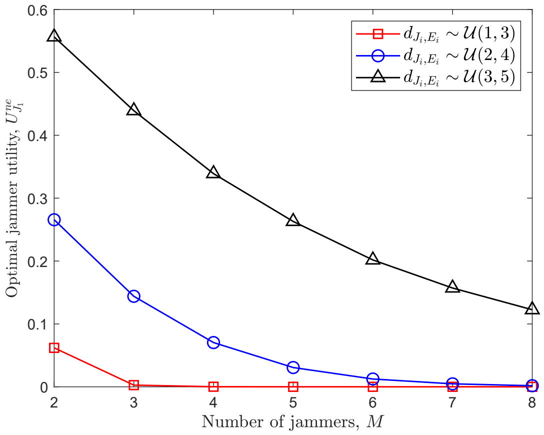


Fig. 7. Optimal jammer utility versus number of jammers.

implemented in a proactive way; for a highly-dynamic IoT that can tolerate large latency, a reactive manner is more efficient. Implementing the tasks of IJS routing needs the knowledge of network topology, which can be available by exchanging location information between neighboring devices or adopting a global positioning system. With the help of the network topology information, the source device can individually compute the route for data delivery, the optimal total rewards, as well as the rewards granted to each jammer. Then, the source can inform every jammer of the total rewards and pay them corresponding rewards through dedicated links, while each jammer individually decides its jamming power. Finally, data is delivered over the computed route, and meanwhile, jammers generate jamming signals to deteriorate the data reception at eavesdroppers. For the details of practical routing implementation, please kindly refer to [34], [38].

VI. Simulation Results

In this section, we first conduct Monte Carlo [39] simulations to validate the theoretical analysis for PLS performance, and then present numerical results of the IJS routing performance [40].

A. Validation of PLS Performance Evaluation

We consider a given path consisting of 3 hops in a straight line. The distance of each hop is 5, i.e., $d_{S_k,D_k}=5$ for $k \in \{1,2,3\}$. There exist two eavesdroppers. The line connecting them is normal to and intersects the center of the path. The distance between each eavesdropper to the center of the path is 10, and the distance between each jammer to its corresponding eavesdropper is $\{2,3,4\}$. We set $P=10$, $\alpha=4$, $\gamma_E=1$ and $P_{J1}=P_{J2}$. The number of trials in each task of Monte Carlo simulation is set to 10^7, and the simulated SOP is computed as

$$\text{Simulated SOP} = 100\% \times \frac{N_{so}}{10^7}, \tag{38}$$

where N_{so} denotes the number of times that the event of secrecy outage occurs in each simulation.

We summarize in Fig. 5 the theoretical and simulation results of SOP performance. The theoretical curves are plotted according to Eq. (1) while the simulated results are obtained based on Eq. (38). We can see from Fig. 5 that the simulation results match well with the theoretical ones for all the cases, which verifies the correctness of our PLS performance evaluation for multi-hop decentralized IoT. Fig. 5 shows that as the jamming power increases, the SOP monotonically decreases, indicating that artificial jamming can be employed to improve the PLS performance. Another observation from Fig. 5 is that a shorter distance between the jammer and eavesdropper can lead to a better PLS performance.

B. Routing Performance

Fig. 6 shows how the optimal jamming power varies with the number of jammers in the JPD game, where we set $R=1$, $c=1$ and $\alpha=4$. We focus on player (jammer) J_1 with $d_{J_1,E_1}=3$, and set that d_{J_i,E_i} $(i \neq 1)$ follows an identical and independent uniform distribution. For each setting of d_{J_i,E_i}, we conduct 10^6 trials and summarize the average optimal jamming power $P_{J_1}^{ne}$. We can see from Fig. 6 that when $d_{J_i,E_i} \sim \mathcal{U}(2,4)$, i.e., $\mathbb{E}\{d_{J_i,E_i}\}=3=d_{J_1,E_1}$, $P_{J_1}^{ne}$

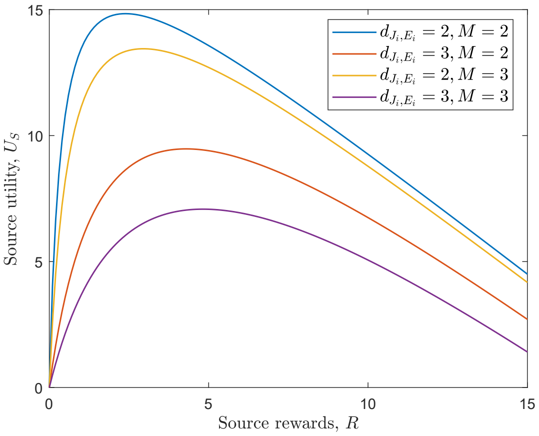


Fig. 8. Source utility versus source rewards.

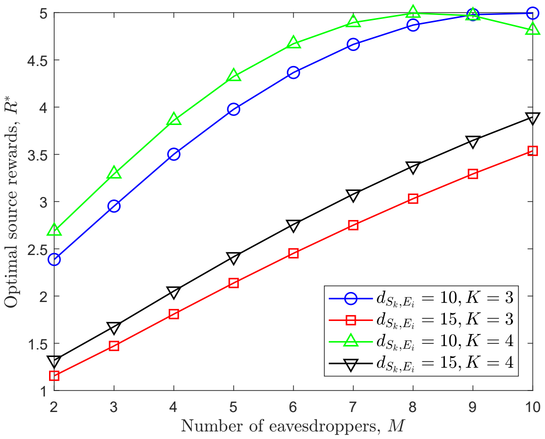


Fig. 9. Optimal source rewards versus number of eavesdroppers.

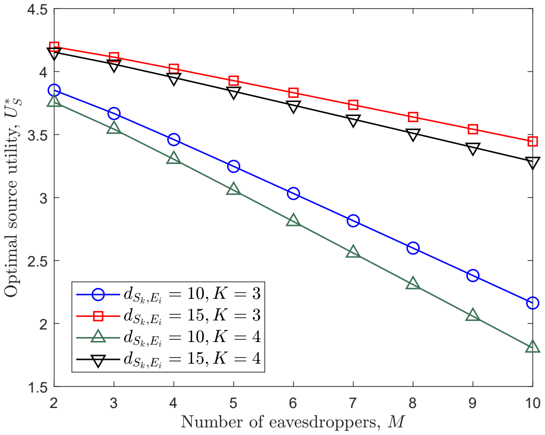


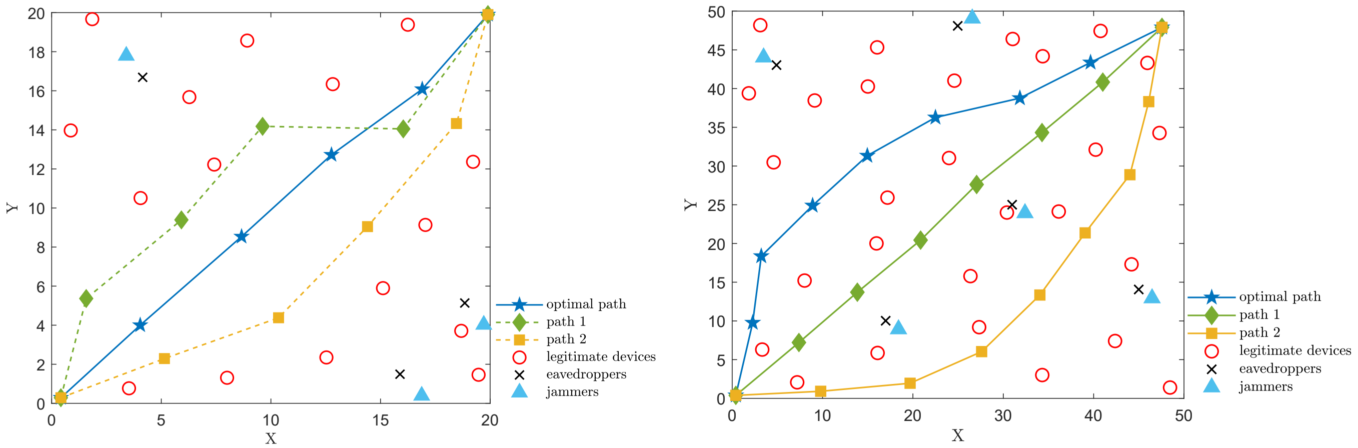
Fig. 10. Optimal source utility versus number of eavesdroppers.

decreases gradually with M. It is because that each player owns a similar competency (i.e., contribution factor), as the number of players increases the portion of rewards that J_1 can compete for decreases, and thus it reduces the power (i.e., the cost) to achieve its maximal utility. When $d_{J_i,E_i} \sim \mathcal{U}(1,3)$, i.e., $\mathbb{E}\{d_{J_i,E_i}\} = 2 < d_{J_1,E_1}$, $P_{J_1}^{ne}$ decreases more fleetly with M. It is because not only the number of competitors increases but also their competency is superior to that of J_1. When $d_{J_i,E_i} \sim \mathcal{U}(3,5)$, i.e., $\mathbb{E}\{d_{J_i,E_i}\} = 4 > d_{J_1,E_1}$, the contribution factor of J_1 is higher than that of other players, even as the number of players increases, J_1 will slightly increase the jamming power to compete for more rewards so as to achieve the maximal utility.

With the same setting as Fig. 6, we focus on jammer J_1 and plot Fig. 7 to show how its optimal utility varies with the number of jammers in the JPD game. Fig. 7 shows that as the number of jammers M increases, the optimal utility $U_{J_1}^{ne}$ monotonically decreases for all the cases. It is because the source rewards R (i.e., total rewards) is fixed, an increase in the competitors will lead to a reduction in the rewards granted to each competitor. We can also see from Fig. 7 that the larger d_{J_i,E_i} $(i \neq 1)$ is, the more utility J_1 can achieve. It is because in the JPD game the rewards granted to a jammer is positively correlated with its contribution factor, while the contribution factor is negatively correlated with the distance between the jammer and the eavesdropper. Another interesting observation is that $U_{J_1}^{ne}$ gradually approaches 0 as M increases. It indicates that when the number of eavesdroppers varies, the source device needs to adjust its rewards to ensure a considerable jammer utility, such that the artificial jamming can be stimulated for PLS performance enhancement.

We then plot Fig. 8 to show how the source utility varies with the source rewards in the PLS-enhancing game, where we set $P = 10$, $\gamma_E = 1$, $\alpha = 4$, $\lambda = 20$, $c = 1$ and $d_{S_k,E_i} = 10$. We can see that for all cases considered here, as the source rewards R increases, the source utility first increases and then decreases. There always exists a unique optimal value of the rewards that maximizes the source utility, which demonstrates that our design of source utility can guarantee the uniqueness of the solution to the PLS-enhancing game. Fig. 8 also shows that a shorter distance between the jammer and the eavesdropper and/or a smaller number of eavesdroppers can lead to a higher source utility. This is due to the reason that the PLS performance is negatively correlated to these two factors.

We further summarize in Fig. 9 and Fig. 10 the behaviors of the optimal source rewards and optimal source utility with the variation of the number of eavesdroppers, respectively. We set $d_{J_i,E_i} = 2$ and other parameters the same as those in Fig. 8. We can observe from Fig. 9 that for most of the cases considered here, the optimal source rewards R^* increases as the number of eavesdroppers, except that for $d_{S_k,E_i} = 10$ and $K = 4$, R^* first increases and then decreases. It implies that the source needs to pay more rewards for artificial jamming to confront more serious eavesdropping situation, unless the situation is too serious so that paying more rewards is not worthy. Fig. 10 shows that the optimal source utility monotonically decreases with the increasing of the number of eavesdroppers for all the cases. We can also see that a longer d_{S_k,E_i} and/or a smaller K can result in a higher U_S^*. All the behaviors are in accordance with the intuition that it is impossible for the source to gain more utility when the



(a) Case 1.

(b) Case 2.

Fig. 11. Snapshots of the optimal path computed by the IJS routing algorithm.

TABLE II
COMPARISON OF DIFFERENT PATHS.

(a) Case 1.

Path	$\sum_{l_k \in \Pi} \Xi_k$	R^*	U_S^*	$\mathbf{P}_J^{ne}$	P_{so}
Optimal path	0.0165	1.6525	16.5299	$(0.2606, 0.3687, 0.4114)$	9.51%
Path 1	0.0232	1.9227	15.9224	$(0.3032, 0.4290, 0.4787)$	11.38%
Path 2	0.0548	2.7627	13.9267	$(0.4356, 0.6163, 0.6878)$	17.99%

(b) Case 2.

Path	$\sum_{l_k \in \Pi} \Xi_k$	R^*	U_S^*	$\mathbf{P}_J^{ne}$	P_{so}
Optimal path	0.0298	2.1446	15.4123	$(0.3885, 0.3981, 0.2142, 0.4627, 0.1733)$	12.99%
Path 1	0.2406	4.5308	8.5326	$(0.8208, 0.8410, 0.4525, 0.9775, 0.3660)$	42.07%
Path 2	0.0613	2.8889	13.6089	$(0.5233, 0.5362, 0.2885, 0.6233, 0.2334)$	19.13%

eavesdropping situation deteriorates.

We lastly plot Fig. 11 to illustrate the optimal path computed by the IJS routing algorithm. We consider two network cases. In case 1, we focus on a 20×20 square network area. We randomly and uniformly place 30 legitimate devices and 3 eavesdroppers in the area and also place a jammer close to each eavesdropper. The maximum transmission range of a single hop is set as 7. In case 2, we focus on a 50×50 square network area. We randomly and uniformly place 50 legitimate devices and 5 eavesdroppers in the area and also place a jammer close to each eavesdropper. The maximum transmission range of a single hop is set as 10. In addition, we set $P = 10$, $\gamma_E = 1$, $\alpha = 4$, $\lambda = 20$, $c = 1$. Fig. 11(a) and Fig. 11(b) present a snapshot of the network topology for the two cases, respectively, where we plot the optimal path computed by the IJS routing algorithm, as well as two other candidate paths (path 1 and path 2) for comparison.

Table II summarizes the critical metrics of different paths. We can see clearly that comparing with path 1 and path 2, the optimal path has the minimum sum link weight and enables the source device to achieve the maximal utility and the lowest secrecy outage probability. Comparing the optimal path with path 1 in case 2, an interesting observation is that the optimal path has more hops, but it receives a much higher source utility and a much lower SOP. It is because that the IJS routing algorithm employs expression (37) as the link weight and thus it can take a detour to avoid the positions of eavesdroppers for guaranteeing the PLS performance.

VII. RELATED WORK

As far as we know, some initial works have been conducted to explore the secure routing in multi-hop wireless networks [20], [21], [23], [41]–[46]. Specifically, Ren *et al.* [41] proposed an encryption scheme to achieve multicast security in wireless sensor networks. Wan *et al.* [42] developed an unobservable secure routing scheme to offer complete unlinkability and content unobservability for all types of packets in mobile ad hoc networks, where the group signature and ID-based encryption were jointly applied for route discovery. Saad *et al.* [20] proposed a secure pathfinding mechanism based on the tree-formation game. With the consideration of energy consumption, Ghaderi *et al.* [21] explored the routing protocol design which can guarantee the transmission security with the minimum energy cost for multi-hop wireless networks. Later, Yao *et al.* [23] studied the PLS-based routing in a multi-hop wireless network with the decode-and-forward relaying scheme. In our previous studies [43]–[45], we investigated that how to design the routing protocol which can guarantee the transmission security while ensuring the communication quality of service, and explored the tradeoff issue between the two aspects. More recently, Xu *et al.* [46] designed a secure routing mechanism for multi-hop cognitive radio networks with the aid of artificial noise.

It is worth noting that this work is distinguishable from the existing ones in the sense that the inherent selfishness of resource-limited IoT devices is considered, and an incentive mechanism intended to stimulate artificial jamming is incorporated into the routing design correspondingly. Such differences clarify the novelty of this work. It is also worth mentioning that except for cryptography and PLS, there exist other techniques, like blockchain [47], that are promising to guarantee IoT security. For a comprehensive survey on current research of IoT security, please kindly refer to [48] and the references therein.

VIII. Conclusion

In this paper, we have designed an incentive jamming-based secure routing scheme for secure data delivery in multi-hop decentralized IoT. First, we evaluated the PLS performance for a general path. With the help of performance evaluation, we next employed a two-stage Stackelberg game to design the incentive mechanism which stimulates artificial jamming for PLS performance enhancement. Based on the incentive mechanism, we further designed the routing algorithm that can find the optimal path by utilizing the Bellman-Ford or Dijkstra's algorithm. We have demonstrated that the proposed routing algorithm is individually rational, stable, distributed and computationally efficient, and also conducted simulations to evaluate the routing performance.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, New Jersey: Pearson, 2017.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[7] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, 2011.

[8] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

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

[10] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015.

[11] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018.

[12] 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.

[13] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, 2013.

[14] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66 – 72, 2015.

[15] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, 2013.

[16] X. He and A. Yener, "Providing secrecy with structured codes: Two-user gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, 2014.

[17] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, 2017.

[18] J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Link selection for security-qos tradeoffs in buffer-aided relaying networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1347–1362, 2019.

[19] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 2019.

[20] W. Saad, X. Zhou, B. Maham, T. Başar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, 2012.

[21] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, 2015.

[22] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, 2011.

[23] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, 2016.

[24] S. Gollakota, S. D. Perli, and D. Katabi, "Interference alignment and cancellation," in *Proc. ACM SIGCOMM*, 2009, pp. 159–170.

[25] R. Zhang and S. Cui, "Cooperative interference management with miso beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 5450–5458, 2010.

[26] C. Psomas, M. Mohammadi, I. Krikidis, and H. A. Suraweera, "Impact of directionality on interference mitigation in full-duplex cellular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 487–502, 2016.

[27] Z. Li, Y. Liu, K. G. Shin, J. Liu, and Z. Yan, "Interference steering to manage interference in iot," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10 458–10 471, 2019.

[28] F. Z. Bousbaa, N. Lagraa, C. A. Kerrache, F. Zhou, M. B. Yagoubi, and R. Hussain, "A distributed time-limited multicast algorithm for vanets

using incremental power strategy," *Computer Networks*, vol. 145, pp. 141–155, 2018.

[29] H. Von Stackelberg, *The Theory of the Market Economy*. London, U.K.: Oxford Univ. Press, 1952.

[30] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[31] R. B. Myerson, *Game Theory*. Cambridge, MA, USA: Harvard Univ. Press, 2013.

[32] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.

[33] R. D. Yates, "A framework for uplink power control in cellular radio systems," *IEEE J. Sel. Areas Commun.*, vol. 13, no. 7, pp. 1341–1347, 1995.

[34] D. Medhi and K. Ramasamy, *Network Routing: Algorithms, Protocols, and Architectures*. San Mateo, CA, USA: Morgan Kaufmann, 2017.

[35] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and S. Clifford, *Introduction to Algorithms*. Cambridge, MA, USA: MIT Press, 2009.

[36] T. Clausen and P. Jacquet, "Optimized link state routing protocol (olsr)," *RFC 3626, IETF Network Working Group*, 2003.

[37] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," *RFC 3561, IETF Network Working Group*, 2003.

[38] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D. Turgut, "Routing protocols in ad hoc networks: A survey," *Computer Networks*, vol. 55, no. 13, pp. 3032–3080, 2011.

[39] K. Binder and D. Heermann, *Monte Carlo Simulation in Statistical Physics: An Introduction*. New York, NY, USA: Springer, 2010.

[40] J. Liu, "Matlab simulation for incentive jamming-based secure routing in decentralized iot," 2020. [Online]. Available: https://github.com/JLIU-NII/Research-on-Physical-Layer-Security/tree/Matlab-Simulation-for-Incentive-Jamming-based-Secure-Routing-in-Decentralized-IoT.

[41] K. Ren, W. Lou, B. Zhu, and S. Jajodia, "Secure and efficient multicast in wireless sensor networks allowing ad hoc group formation," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 2018–2029, 2008.

[42] Z. Wan, K. Ren, and M. Gu, "Usor: An unobservable secure on-demand routing protocol for mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1922–1932, 2012.

[43] Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/qos-aware route selection in multi-hop wireless ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2016, pp. 1–6.

[44] Y. Xu, J. Liu, O. Takahashi, N. Shiratori, and X. Jiang, "Soqr: Secure optimal qos routing in wireless ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2017, pp. 1–6.

[45] Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, vol. 123, pp. 77–87, 2017.

[46] Q. Xu, P. Ren, H. He, and D. Xu, "Security-aware routing for artificial-noise-aided multi-hop secondary communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.

[47] F. Ahmad, Z. Ahmad, C. A. Kerrache, F. Kurugollu, A. Adnane, and E. Barka, "Blockchain in internet-of-things: architecture, applications and research directions," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, 2019, pp. 1–6.

[48] M. b. M. Noor and W. H. Hassan, "Current research on internet of things (iot) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

Yang Xu (Member, IEEE) received the B.E. degree from the School of Telecommunications Engineering and the Ph.D. degree from the Department of Communication and Information Systems, Xidian University, Xi'an, China, in 2006 and 2014, respectively, where she is currently an associate professor with the School of Economics and Management. Dr. Xu has published over 30 academic papers at premium international journals and conferences, like the IEEE Transactions on Wireless Communications (TWC), the IEEE Transactions on Vehicular Technology (TVT), the IEEE INFOCOM, Computer Networks. Dr. Xu's research interests include wireless network security, physical layer security, block-chain, routing protocol design and network performance evaluation.

Jia Liu (Member, IEEE) received the B.E. degree from the School of Telecommunications Engineering, Xidian University, Xi'an, China, in 2010, and received the Ph.D. degree from the School of Systems Information Science, Future University Hakodate, Japan, in 2016. Dr. Liu is currently an assistant professor with the Center for Cybersecurity Research and Development, National Institute of Informatics, Japan. Dr. Liu's research interests include wireless network security, physical layer security, 5G communications, mobile ad hoc networks, network performance evaluation, etc. Dr. Liu has published over 40 academic papers at premium international journals and conferences, like the IEEE Transactions on Wireless Communications (TWC), the IEEE Transactions on Information Forensics and Security (TIFS), the IEEE INFOCOM. Dr. Liu received the 2016 IEEE Sapporo Section Encouragement Award.

Yulong Shen (Member, IEEE) received the B.S. and M.S. degrees in computer science and Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services Networks. His research interests include wireless network security and cloud computing security. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN.

Jun Liu (Member, IEEE) received her Ph.D. degrees from Northeastern University, Shenyang, China, in 2011 and worked as a lecturer with college of information science and engineering from 2011-2016 in Northeastern University. She worked as a postdoctoral research fellow from 2016-2018 in CECA Dept. at Peking University. She is currently an assistant professor with the Institute of Network Sciences and Cyberspace at Tsinghua University (Beijing, China), and a researcher with the Beijing National Research Center for Information Science and Technology (Beijing, China). Her research interests focus on network routing security.

Xiaohong Jiang (Senior Member, IEEE) received his B.S., M.S. and Ph.D degrees in 1989, 1992, and 1999 respectively, all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from Feb. 2005 to Mar. 2010. Dr. Jiang's research interests mainly include wireless networks, network security, optical networks, router/switch design, etc. He has published over 300 technical papers at premium international journals and conferences, which include over 80 papers published in top IEEE journals and top IEEE conferences, like the IEEE/ACM Transactions on Networking (TON), the IEEE Journal of Selected Areas on Communications (JSAC), the IEEE INFOCOM.

Tarik Taleb (Senior Member, IEEE) received the B.E. degree (Hons.) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from GSIS, Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Professor with the School of Electrical Engineering, Aalto University, Espoo, Finland. He is a member of the IEEE Communications Society Standardization Program Development Board. In an attempt to bridge the gap between academia and industry, he founded the IEEE-Workshop on Telecommunications Standards: From Research to Standards, a successful event that was recognized with the Best Workshop Award by the IEEE Communication Society (ComSoC). Based on the success of this workshop, he has also founded and has been the Steering Committee Chair of the IEEE Conference on Standards for Communications and Networking. He is the General Chair of the 2019 IEEE Wireless Communications and Networking Conference, Marrakech, Morocco. He is/was on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE WIRELESS COMMUNICATIONS MAGAZINE, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, and a number of Wiley journals. He is a Distinguished Lecturer of the IEEE Communications Society (ComSoc).