Incentive Mechanism for Cooperative Intrusion Response: A Dynamic Game Approach

Yunchuan Guo[1,2], Xiao Wang[1,3], Liang Fang[1], Yongjun Li[1,2], Fenghua Li[1,2], and Kui Geng[1(✉)]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
gengkui@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[3] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China

Abstract. Multi-hop D2D (Device-to-Device) communication is often exposed to many intrusions for its inherent properties, such as openness and weak security protection. To mitigate the intrusions in time, one of significant approaches is to establish a Cooperative Intrusion Response System (CIRS) to respond to intrusion activities during data transmission. In CIRS, user equipments that act as relays (RUEs) are assumed to actively help destination nodes to respond to intrusion activities. However, this assumption is often invalid in multi-hop D2D communication because the RUEs are selfish and unwilling to spend extra resources on undertaking response tasks. To address this problem, a game approach is proposed to encourage RUEs to cooperate. In detail, we formulate an incentive mechanism for CIRS in multi-hop D2D communication as a dynamic game and achieve an optimal solution to help RUEs decide whether to participate in detection or not. Theoretical analysis shows that only one Nash equilibrium exists for the proposed game. Simulations demonstrate that our mechanism can efficiently motivate potential RUEs to participate in intrusion detection and response, and it can also block intrusion propagation in time.

Keywords: Device-to-device · Cooperative intrusion response · Incentive mechanism · Game theory

1 Introduction

Multi-hop device-to-device (D2D) communication [15], which enables direct data transmission between source user equipments (SUEs) and destination user equipments (DUEs) with the assistance of other user equipments (UEs) acting as

Supported by the National Key Research and Development Program of China (No. 2016YFB0801001) and the National Natural Science Foundation of China (No. U1836203).

J. M. F. Rodrigues et al. (Eds.): ICCS 2019, LNCS 11536, pp. 590–603, 2019.
https://doi.org/10.1007/978-3-030-22734-0_43

relays (RUEs), provides a promising solution for mobile network operator to meet the growing users demands (such as higher throughput, lower transfer delay, and better power efficiency). Now multi-hop D2D communication has been widely used in various application, e.g., vehicle-to-vehicle networks [27], unmanned aerial vehicle (UAV) assisted wireless communications [11], and near field communications (NFC) [6].

However, multi-hop D2D communication may be exposed to many intrusions because of its openness, weak security protection on mobile UEs and the direct data transmission without the fixed network infrastructures. For example, in D2D-based vehicle-to-vehicle (V2V) communication [27], adversaries may disguise as normal vehicle equipment and send malicious packets via D2D communication to invade and compromise the destination vehicle equipment [12], thus threatening the lives of the people at destination vehicles. To mitigate the intrusions in a timely way, one significant thing that should be done is to establish a Cooperative Intrusion Response System (CIRS) for D2D communication to detect and respond to intrusion activities during data transmission. Through this approach, intrusion activities are detected and responded in time, communication overhead (e.g., the total volume of data traffic) are drastically reduced, thus communication security is improved.

Motivation: However, the CIRS cannot efficiently work in multi-hop D2D networks, because the RUEs are selfish and unwilling to spend extra resources on undertaking the intrusion detection and response tasks. Hence, a selfish RUE would not participate in responding intrusion events unless a satisfying incentive is given to compensate its extra cost. Without adequate participation of RUEs, the performance of a CIRS will be drastically decreased. To address this problem, an incentive mechanism, which motivates RUEs to promptly respond to intrusions, is required.

Considering the incentive resources being used to incentivize participation, existing incentive mechanism can be roughly divided into two categories: social-aware and financial-aware [7]. In the social-aware incentive mechanism [20], two social phenomena (i.e., social trust and social reciprocity) are used to find the social relationships among UEs and identify the best relays. However, privacy leakage is a serious challenge in social-aware incentive mechanism [22], because the process of identifying social relationships among UEs is usually accompanied by extra private information leakage. Compared with the social-aware incentive, the financial-aware incentive mechanism, which allocates financial resources to cooperators to incentivize participation, is a more desirable incentive paradigm in a practical application. However, existing CIRS and financial-aware incentive mechanisms are suffer from two problems, respectively: (1) **Low response accuracy.** In existing CIRS, response activities are operated based on aggregated monitored data from different sensors, thus most CIRS suffers from the loss of accuracy and the response accuracy is low. (2) **False-reporting attack.** When a packet is normal, malicious RUEs without carrying out detections might claim that they have detected the packet and have not found any abnormal data in this packet. Through this approach, they expects to win more rewards from DUEs.

Contribution: To address the above problems, in this paper, a dynamic game approach is utilized to establish a decentralized incentive mechanism for CIRS, which promote the response accuracy and mitigates the potential false-reporting attack. Our main contributions are as follows.

(1) In this paper, we formulate an incentive mechanism for CIRS in multi-hop D2D communication as a dynamic game and achieve the only one Nash equilibrium for RUEs to decide whether to participate in detection or not.
(2) We evaluate the benefit and cost of DUE and RUEs to analyze the proposed game. A reputation-based spot-check mechanism is also proposed to mitigate the potential false-reporting attack.
(3) Simulations demonstrate that our mechanism can efficiently motivate potential RUEs to participate in intrusion detection and response, and can also block intrusion propagation in time.

The remainder of this paper is organized as follows. In Sect. 2, we discuss the related work. We introduce the system model and discuss the spot-check mechanism in Sect. 3. Payoffs of RUEs and DUE are evaluated in Sect. 4. In Sect. 5, we formulate the incentive mechanism as a dynamic game and analyze its Nash equilibrium in Sect. 5. Simulations are provided in Sect. 6 to demonstrate the validity of proposed results. Section 7 draws the conclusion.

2 Related Work

2.1 D2D Communication

D2D communication [10,19] has received considerable attention in recent years and can be divided into two categories: standalone D2D and network-assisted D2D. UEs in standalone D2D organize communications by themselves and transfer messages directly without fixed network infrastructures (e.g., base stations) [3]. However, it is a big challenge for standalone D2D UEs to establish, maintain and control the communication only by themselves, which requires high complexity of the UEs. As a solution to this challenge, network-assisted D2D communication, which utilizes fixed network infrastructures for communication organization and resources allocation, has been widely studied. Zhou *et al.* [26] proposed a bargaining game to promote security and efficiency in network-assisted D2D with the presence of malicious eavesdroppers. Though network-assisted D2D works better than standalone D2D in practical applications, those two D2D paradigms could be failed due to long distance for their one-hop structure.

To solve the above problems, multi-hop D2D communication problems have been widely studied and applicated in various fields [6,11,27]. Zhou *et al.* [27] addressed the dependable D2D content distribution problem using a coalition formation game approach to optimize peer discovery, route selection, and spectrum allocation jointly. The spectrum trading contract was designed in [11] for D2D-based UAV-assisted cellular networks to better serve local mobile users.

Liu *et al.* [13] designed multi-hop D2D communication protocol and algorithm to address resource allocation problem for the general multi-hop D2D communication underlying cellular networks. Liu *et al.* [14] proposed three wireless power transfer policies in the power transfer model to analyzed the physical layer security in energy constrained D2D communication. Xu *et al.* [12] investigated the interplay between incentives and interdependent security risks in D2D offloading, and designed security-aware incentive mechanisms.

Multi-hop D2D communication provides an efficient D2D communication scheme with a variety of advantages such as improved spectral efficiency, and increased network capacity. Unfortunately, due to the weak security protection on ordinary mobile UEs, D2D communication may be exposed to many intrusions. In the past few decades, researchers are mainly focused on the security issues in single-hop D2D communication. So far, however, there has been little discussion about the security problems in multi-hop D2D communication.

2.2 Incentive Mechanism

Existing work investigates the incentive mechanism in wireless networks can be roughly divided into two categories: social-aware and financial-aware. Social-aware incentive mechanism for wireless networks is studied in [1,5,18]. Chen *et al.* [20] proposed a social-trust and social-reciprocity-based framework to promote cooperation among devices for multi-hop D2D communication. A cooperative video multicast system was developed in [4] to provide incentive for clients to share video packets with each other based on social ties in D2D communication. Gao *et al.* [8] formulates the dynamic social-aware peer selection problem as a dynamic optimization problem and proposes the drift-plus-penalty ratio algorithm to solve it. However, privacy leakage is a serious and inevitable problem in social-aware incentive mechanism.

Considering the privacy leakage issue, financial-aware incentive mechanism [12] is a more desirable incentive mechanism paradigm in practical application. Yang *et al.* [21] designed and analyzed platform-centric and user-centric financial-aware incentive mechanisms for mobile phone sensing. Guo *et al.* [9] formulated the incentive mechanism for CIDS as an evolutionary game to maximize nodes utility and motivate nodes to cooperate. However, financial-aware incentive mechanism may suffer serval attacks, and among them false-reporting attack is common and inevitable [25]. Zhang *et al.* [23,24] studied the free-riding and false-reporting problem in crowdsourcing and designed an incentive mechanism to motivating providers to complete their assigned tasks.

3 Basic Idea and System Model

3.1 Communication-Response Model

Figure 1 gives the communication process of multi-hop D2D and the mechanism of CIRS. Its detail processes are as follows. First, DUE requests a file with size

D from SUE. After SUE receives the request from DUE, it computes the routing path uses via routing algorithms (e.g., interference aware touting algorithms [16]) and obtains a set RP of RUEs where $RP = \{\text{RUE}_0, \text{RUE}_1, ..., RUE_{N-1}\}$ and N is the number of RUEs. Then, SUE sends a packet containing the file to its nearby RUE. When a neighboring RUE receives the packet and detects its potential threat (e.g., virus, Trojan) with detection rate α via intrusion detection technology (e.g. pattern matching). If without any threat included in this packet, RUE will relay the packet to its next nearby RUE in the routing path. Otherwise, it will pre-undertake corresponding countermeasures (e.g., interrupting the current communication and isolating the packet) and upload the threaten evidence to a trusted third party (TTP). In our work, we assume that the probability of malicious packets is ρ and no collusion between UEs exists.

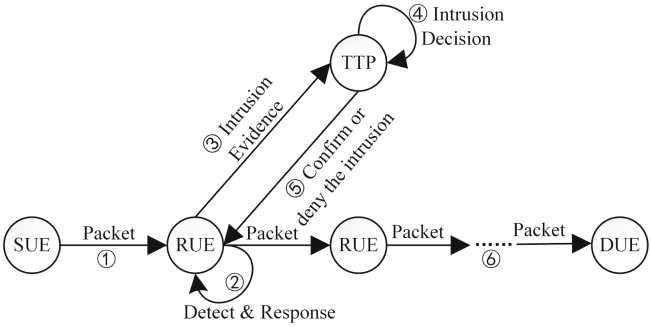

Fig. 1. Communication-response model.

3.2 Incentive Mechanism

As described in Sect. 1, RUEs are uninterested in participating in intrusion detection and response without sufficient incentive. To address this problem, a dynamic game-theoretic approach is proposed to stimulate a selfish RUE to detect and respond to an intrusion event. In our approach, RUE first evaluates the benefit and cost for detecting and responding to the potential intrusion, and then takes action based on its decision. After the multi-hop D2D communication is completed, DUE will decide to pay a reward only to the RUE who has worked correctly. Furthermore, due to the reward for RUE is paid after the communication is completed, some RUEs (called false-reporters) may lie to DUE that they have detected the packet in order to get rewards without detecting the packet if no intrusion is found by the RUEs before them. To address this problem, we design a reputation-based spot-check mechanism.

3.3 Spot-Check Mechanism

To mitigate false-reporting attack, we design a reputation-based spot-check mechanism. We assume that all UEs have a reputation score *rep*. If a RUE's

reputation is less than a preset threshold rep_{th}, it will receive less reward gained from intrusion detection than normal RUEs. The process of spot-check mechanism is described as follows.

First, DUE notifies the SUE to start the spot-check activity. After receiving the packet, SUE intentionally sends a malicious packet mp with no to its nearby RUE with the destination of DUE. If the RUE claims that it has detected and then relays mp to the next RUE, we can regard this RUE as a false-reporter and reduce the RUE's reputation. Finally, DUE rewards the RUEs which correctly responds to mp. The spot-check mechanism runs and repeats irregularly when the multi-hop D2D routing path is idle, and the running status is only known to SUE, DUE. In the following section, We assume that all UEs are normal and have a reputation score above the threshold rep_{th}.

4 Benefit and Cost

4.1 RUE (User Equipment as Relay)

To establish the multi-hop D2D communication, RUE selection algorithm, which can find the optimal RUE and generate routing path for each UE, is significant. As the issue of RUE selection algorithm has been fully discussed in [13], in this paper, we will not investigate this problem and will assume the optimal routing path for multi-hop D2D communication has been selected. Here we consider the $\text{RUE}_\text{i} \in \text{RP}$ as the $(i+1)$th RUE that receives packets from SUE, where $i = 0, 1, 2, ..., N-1$. Hence, we evaluate the detection cost and response cost of RUE_i as follows.

Detection Cost: Each kind of intrusions has a unique attack pattern that can be recognized by attack pattern matching algorithms (e.g. Aho-Corasick algorithm [2]). In this paper, RUE_i matches the packet to existing attack patterns to detect the potential intrusion activity. The number of attack patterns for match is m_i and the computational complexity of the pattern matching algorithm that RUE_i selected is $cpma(m_i, D)$, where D is the size of the packet. Hence, the detection cost of RUE_i can be defined as follows.

$$C_{detection_i} = \lambda_{dc} \cdot cpma(m_i, D), \tag{1}$$

where the λ_{dc} is the cost unit for computational complexity of the pattern matching algorithm selected by RUE_i.

Response Cost: If the packet is detected to be malicious, RUE_i will consume its resources to undertake countermeasures. Here we consider two types of resources: the memory space and the energy of RUE_i. If intrusion response requires too many resources or RUE's idle resources are limited, the response cost will be expensive for RUEs. Here we donate the memory and energy utilization for undertaking countermeasures as M_{u_i} and E_{u_i}, respectively. Furthermore, the idle memory and energy are described as M_{f_i} and E_{f_i}, respectively. Hence, the response cost of RUE_i can be defined as follows.

$$C_{response_i} = \lambda_{rc} \cdot (\frac{M_{u_i}}{M_{f_i}} + \frac{E_{u_i}}{E_{f_i}}), \tag{2}$$

where the λ_{rc} is the cost unit for resource utilization in undertaking countermeasures.

4.2 DUE (User Equipment as Destination)

After the multi-hop D2D communication is completed, DUE will be in one of three states: (1) **State 1.** DUE has received the normal packet; (2) **State 2.** DUE is invaded by the malicious packet; (3) **State 3.** No packet reaches DUE because the packet from SUE is detected to be malicious by $\text{RUE}_\text{i} \in \text{RP}$. Under above states, DUE gains three different benefits as follows.

State 1: In this state, DUE receives normal packet and no intrusion activity happens. The total benefit of DUE is gained from the packet received, and can be divided into two parts. One part is the fixed benefit F that gains from receiving the packet successfully. The other gains from DUE's interest in the content of the packet, where the interest factor per unit of packet size is θ. If DUE is interested in the received packet, the larger the packet size D is, the higher benefit DUE can gain from it. Hence, the benefit of DUE can be defined as follows.

$$B_{s_1} = \lambda_{s_1} \cdot (F + \theta D), \tag{3}$$

where λ_{s_1} is the cost unit for DUE's interest.

However, B_{s_1} donates the sum of N benefits gained from RUEs in RP. As a result of this, the benefit of DUE that gains from RUE_i can be given as follows.

$$B_{s_1 i} = \lambda_{s_1} \cdot \frac{F + \theta D}{N}, \tag{4}$$

State 2: In this state, DUE receives malicious packet and is invaded. The benefit of DUE is negative and depends on the risk of the exploited vulnerability. Here we consider the factors proposed in [17] to evaluate the exploited vulnerability, and the risk can be calculated by weighting all those factors. The risk from exploiting vulnerability v_j can be defined as r_j with $0 < r_j < 1$. Hence, the benefit of DUE under the state 2 can be defined as follows.

$$B_{s_2} = -\lambda_{s_2} \cdot r_j, \tag{5}$$

where λ_{s_2} is the cost unit for the risk of exploiting a vulnerability.

Under this state, DUE is invaded and all the RUEs that have detected the packet should be responsible for the intrusion. Moreover, the RUEs who receives and detects the packet early should have greater responsibilities than RUEs after them. As a result of this, the negative benefit of DUE gained from RUE_i can be given as follows.

$$B_{s_2 i} = -\lambda_{s_2} \cdot \frac{2 \cdot r_j \cdot (N - i)}{N(N + 1)}, \tag{6}$$

State 3: No packet reaches DUE because the packet is detected to be malicious and an intrusion is responded by $\text{RUE}_\text{i} \in \text{RP}$. If the intrusion packet is detected by RUE_i with a small serial number i, which means the intrusion is blocked in time, the benefit of DUE will be high. Hence, the benefit gained from RUE_i can be given as follows.

$$B_{s_3 i} = \lambda_{s_2} \cdot \frac{(N-i) \cdot r_j}{N}. \tag{7}$$

5 Dynamic Game and Its Analysis

We define the game as a triplet $G = \{\{\text{DUE}\} \cup RP, S, U\}$, where RP is the set which consists of the RUEs in routing path, S donates the strategy space, and U is the set of players' utilities. Here we assume that the probability that the packet is malicious is ρ. The game tree can be seen in Fig. 2, where the leaf nodes present the players' utilities with the tuple $U = (U_{DUE}, U_{RUE})$. We define the strategy combination as a tuple $S = (S_{RUE}, S_{DUE})$, where $S_{RUE} = (detect, no\_detect)$ and $S_{DUE} = (pay, no\_pay)$. We analyze the game in two levels.

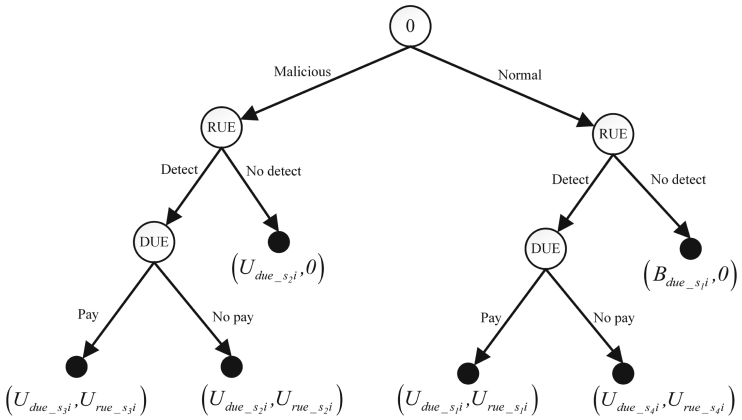

Fig. 2. The dynamic game tree.

5.1 DUE Level

The benefits of DUE gained from RUE_i in this game are described in (4), (6), and (7). After the communication is completed, there are four possible states of DUE and RUE. Therefore, the rewards for RUEs are defined as P_{s_1}, P_{s_2}, P_{s_3}, P_{s_4}. As the benefits of DUE are described in Sect. 4.2, for each RUE_i, DUE's four different utilities are as follows.

When the multi-hop D2D communication is completed, if DUE has received the normal packet and RUE_i detects correctly, the DUE's utility gained from RUE_i can be defined as follows.

$$U_{due\_s_1 i} = B_{s_1 i} - P_{s_1 i} = \lambda_{s_1} \cdot \frac{F + \theta D}{N} - \frac{P_{s_1}}{N}, \tag{8}$$

where $P_{s_1 i}$ is the reward for RUE_i.

When the multi-hop D2D communication is completed, DUE is invaded by the malicious packet, the DUE's utility gained from RUE_i can be defined as follows.

$$U_{due\_s_2 i} = B_{s_2 i} - P_{s_2 i} = -\lambda_{s_2} \cdot \frac{2 \cdot r_j \cdot (N - i)}{N(N + 1)}, \tag{9}$$

where $P_{s_2 i} = 0$ because DUE is invaded but no intrusion is detected by RUE_i.

When the multi-hop D2D communication is completed, no packet reaches DUE because the packet is detected to be malicious by $\text{RUE}_\text{i} \in \text{RP}$, the DUE's utility gained from RUE_i can be defined as follows.

$$U_{due\_s_3 i} = B_{s_3 i} - P_{s_3 i} = \frac{(N - i)}{N} \cdot (\lambda_{s_2} \cdot r_j - P_{s_3}) \tag{10}$$

where $P_{s_3 i}$ is the reward for RUE_i and it is high for the RUE_i with a small serial number i because they have blocked the propagation of malicious packet in a timely way.

When the multi-hop D2D communication is completed, if DUE has received the normal packet and RUE_i has detected incorrectly and responded to it, the DUE's utility gained from RUE_i can be defined as follows.

$$U_{due\_s_4 i} = B_{s_1 i} - 0 = \lambda_{s_1} \cdot \frac{F + \theta D}{N}. \tag{11}$$

5.2 RUE Level

The costs of RUE_i in this game are described in (1) and (2), and the rewards that DUE can pay are given in (8)–(11). Therefore, the utilities of RUE_i can be expressed as follows.

When the multi-hop D2D communication is completed and no intrusion happens, if RUE_i has detected the packet correctly, the utility of RUE_i can be defined as follows.

$$U_{rue\_s_1 i} = P_{s_1 i} - C_{detection_i} = \frac{P_{s_1}}{N} - \lambda_{dc} \cdot cpma(m_i, D). \tag{12}$$

When the multi-hop D2D communication is completed and intrusion happens, if RUE_i hasn't found the intrusion after detecting the packet, the utility of RUE_i can be defined as follows.

$$U_{rue\_s_2 i} = P_{s_2 i} - C_{detection_i} = -\lambda_{dc} \cdot cpma(m_i, D). \tag{13}$$

When the multi-hop D2D communication is completed and intrusion is detected and responded by RUE_i, the utility of RUE_i can be defined as follows.

$$\begin{aligned} U_{rue\_s_3 i} &= P_{s_3 i} - C_{detection_i} - C_{response_i} \\ &= \frac{(N - i) \cdot P_{s_3}}{N} - \lambda_{dc} \cdot cpma(m_i, D) - \lambda_{rc} \cdot \left(\frac{M_{u_i}}{M_{f_i}} + \frac{E_{u_i}}{E_{f_i}}\right), \end{aligned} \tag{14}$$

When the multi-hop D2D communication is completed and no intrusion happens, if $\mathrm{RUE_i}$ has detected the packet incorrectly and responded to it, the utility of $\mathrm{RUE_i}$ can be defined as follows.

$$\begin{aligned} U_{rue\_s_4 i} &= 0 - C_{detection_i} - C_{response_i} \\ &= -\lambda_{dc} \cdot cpma(m_i, D) - \lambda_{rc} \cdot (\frac{M_{u_i}}{M_{f_i}} + \frac{E_{u_i}}{E_{f_i}}), \end{aligned} \tag{15}$$

5.3 Equilibrium Analysis

Theorem 1. *The strategy $s = (detect, pay)$ is the only Nash equilibrium of the dynamic game, if DUE's rewards for RUEs satisfy the conditions as follows.*

$$\begin{cases} \lambda_{rc} \dfrac{1-\alpha}{\alpha} (\dfrac{M_{u_i}}{M_{f_i}} + \dfrac{E_{u_i}}{E_{f_i}}) \cdot N < P_{s_1} < \lambda_{s_1} \cdot (F + \theta D), \\ P_{s_2} = 0, \\ (\lambda_{dc} cpma(m_i, D) + \lambda_{rc} \dfrac{1}{\alpha} (\dfrac{M_{u_i}}{M_{f_i}} + \dfrac{E_{u_i}}{E_{f_i}})) \cdot N < P_{s_3} < \lambda_{s_2} \cdot r_j, \\ \rho \cdot P_{s_3} + (1-\rho) \cdot \dfrac{P_{s_1}}{N} < \alpha\rho \cdot \lambda_{s_2} + \lambda_{s_2} \dfrac{\rho \cdot (1-\alpha)}{\alpha} \cdot \dfrac{2 \cdot r_j}{N+1} \\ \qquad\qquad + \lambda_{s_1} \dfrac{(2\alpha - 1)(1-\rho)}{\alpha} (F + \theta D). \end{cases} \tag{16}$$

Proof. Here the method of inverse analysis is used. We can divide the problem into three aspects.

(1) P_{s_2} is supposed to be 0 as described in Sect. 5.1. As DUE's utility should be positive when it decides to rewards the RUEs detected the packet correctly. Therefore, according to (3) and (7), we can get the first condition as follows.

$$\begin{cases} P_{s_1} < B_{s_1} = \lambda_{s_1} \cdot (F + \theta D), \\ P_{s_2} = 0, \\ P_{s_3} < B_{s_3} = \lambda_{s_2} \cdot r_j. \end{cases} \tag{17}$$

(2) According to the Fig. 2 and the utilities of $\mathrm{RUE_i}$ defined in (12)–(15), the condition below should be satisfied to ensure the utility of "detect" is higher than "no_detect".

$$\begin{cases} \alpha U_{rue\_s_3 i} + (1-\alpha) U_{rue\_s_2 i} > 0, \\ \alpha U_{rue\_s_1 i} + (1-\alpha) U_{rue\_s_4 i} > 0. \end{cases} \tag{18}$$

Now using the utilities in (12)–(15), we can get condition two as follows.

$$\begin{cases} P_{s_1} > \lambda_{rc} \dfrac{1-\alpha}{\alpha} (\dfrac{M_{u_i}}{M_{f_i}} + \dfrac{E_{u_i}}{E_{f_i}}) \cdot N, \\ P_{s_3} > (\lambda_{dc} cpma(m_i, D) + \lambda_{rc} \dfrac{1}{\alpha} (\dfrac{M_{u_i}}{M_{f_i}} + \dfrac{E_{u_i}}{E_{f_i}})) \cdot N. \end{cases} \tag{19}$$

(3) According to the Fig. 2 and the utilities of DUE defined in (8), (9) (10) and (11), the condition below should be satisfied to ensure the utility of "pay" is higher than "no_pay".

$$\alpha(\rho \cdot U_{due\_s_3 i} + (1-\rho) \cdot U_{due\_s_1 i}) > (1-\alpha)(\rho \cdot U_{due\_s_1 i} + (1-\rho) \cdot U_{due\_s_4 i}). \tag{20}$$

Now using the utilities in (8)–(11), we can get condition 3 as follows.

$$\begin{aligned} \rho \cdot P_{s_3 i} + (1-\rho) \cdot P_{s_1 i} < \alpha\rho \cdot B_{s_3 i} + \frac{(2\alpha-1)(1-\rho)}{\alpha} B_{s_1 i} \\ - \frac{\rho \cdot (1-\alpha)}{\alpha} B_{s_2 i}. \end{aligned} \tag{21}$$

As described in Sect. 5.1, we have

$$\begin{aligned} \rho \cdot \frac{(N-i)}{N} P_{s_3} + (1-\rho) \cdot \frac{P_{s_1}}{N} < \alpha\rho \cdot \lambda_{s_2} \frac{(N-i) r_j}{N} \\ + \lambda_{s_1} \frac{(2\alpha-1)(1-\rho)}{\alpha} (F + \theta D) \\ + \lambda_{s_2} \frac{\rho \cdot (1-\alpha)}{\alpha} \cdot \frac{2 \cdot r_j \cdot (N-i)}{N(N+1)}. \end{aligned} \tag{22}$$

The final result can be calculated as follows.

$$\begin{aligned} \rho \cdot P_{s_3} + (1-\rho) \cdot \frac{P_{s_1}}{N} < \alpha\rho \cdot \lambda_{s_2} + \lambda_{s_2} \frac{\rho \cdot (1-\alpha)}{\alpha} \cdot \frac{2 \cdot r_j}{N+1} \\ + \lambda_{s_1} \frac{(2\alpha-1)(1-\rho)}{\alpha} (F + \theta D). \end{aligned} \tag{23}$$

Combining the three conditions (17), (19) and (23), we can get the final condition (16) to ensure the Nash equilibrium $s = (detect, pay)$ of the dynamic game. □

6 Experiment Evaluation

In the experiment, we adopt a taxi scenario to simulate multi-hop D2D communication where each mobile device in a taxi is a D2D UE. Data was gathered from 8:00:00 a.m. to 8:59:59 a.m. on August 13, 2015 including 10088 GPS records of 442 taxis in the Changping area in Beijing, China. During this period, we assume that: (1) Each taxi has one mobile device in it and it communicates with others via multi-hop D2D networks; (2) Distance of D2D communication is 100 m, and taxis within the scope of the communication can transmit packets with each other; (3) Energy consumption is only considered in intrusion detection and response; (4) Size of the packet is $D = 2000$. Probability of a malicious packet is $\rho = 0.5$. The potential number of RUEs $\in RP$ is $N = 10$.

As described in Sect. 4.2, we define the values of parameters as follows. For the aspect of RUE, we assume that the multi-pattern matching algorithm is Aho-Corasick algorithm [2], thus $cpma(m_i, D)$ can be calculated as $m_i \cdot D$.

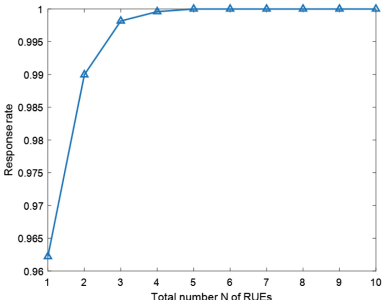

Fig. 3. Response rate.

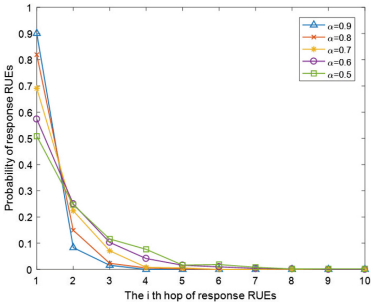

Fig. 4. Timeliness of response.

The remaining parameters are as follows. λ_{dc} and λ_{rc} are (5×10^{-6}) and 25, respectively. The detection rate is $\alpha = 0.9$. The number of attack patterns for match is $m_i = 1000$. The memory and energy utilization for undertaking countermeasures are $M_{u_i} = 20$ and $E_{u_i} = 10$, respectively. The free memory and energy are $M_{f_i} = 100$ and $E_{f_i} = 100$, respectively. For the aspect of DUE, the parameters are as follows. λ_{s1} and λ_{s2} are 10 and (2×10^3), respectively. The risk is a constant $r_j = 0.9$. Fixed benefit F is 25, and interest factor θ is 2.5×10^{-3}. Therefore, according to Theorem 1, the value of P_{s_1} and P_{s_3} can be set as 150 and 1000, respectively. Without the special statement, we set the parameters value described above as default.

Response Rate: We pick different number N in order to show the proportion of total response number in the number of malicious packet in D2D communication. Figure 3 shows the change of response rate over the total number N, respectively. From Fig. 3, we can see that, given the detection rate $\alpha = 0.9$, the rate of response increases with the growth of RUEs' number N if the intrusion happens. Figure 3 shows the compensation for the single detection node.

Timeliness of Response: We pick different detection rate α and the result is presented in Fig. 4. The abscissa in Fig. 4 is the ith hop of the response RUE and the ordinate is the probability of response RUEs at specific hop i. If the probability that RUE responds to the malicious packet is high, intrusion activity could be blocked in time. From Fig. 4, we can see that, with the growth of the detection rate α, more malicious packet is responded by the RUE with smaller hops. This means that intrusion will be blocked in a timely way before the malicious packets arrive DUE.

7 Conclusion

Multi-hop D2D communication may be exposed to many intrusions for its inherent properties, such as openness and weak security protection. To mitigate the intrusions in time, in this paper, we formulate an incentive mechanism for CIRS in multi-hop D2D communication as a dynamic game and achieve an optimal

solution to help RUEs decide whether to participate in detection or not. Theoretical analysis shows that the only Nash equilibrium exists for the proposed game. To mitigate the false-reporting attack, we proposed a spot-check mechanism on the basis of binary reputation score. Simulations demonstrate that our mechanism can efficiently motivate potential RUEs to participate in intrusion detection and response, and can also block intrusion propagation in time.

References

1. Ahmed, M., Li, Y., Waqas, M., Sheraz, M., Jin, D., Han, Z.: A survey on socially aware device-to-device communications. IEEE Commun. Surv. Tutor. **20**(3), 2169–2197 (2018)
2. Aho, V.A., Corasick, J.M.: Efficient string matching: an aid to bibliographic search. Commun. ACM **18**(6), 333–340 (1975)
3. Asadi, A., Wang, Q., Mancuso, V.: A survey on device-to-device communication in cellular networks. IEEE Commun. Surv. Tutor. **16**(4), 1801–1819 (2014)
4. Cao, Y., Jiang, T., Chen, X., Zhang, J.: Social-aware video multicast based on device-to-device communications. IEEE Trans. Mob. Comput. **15**(6), 1528–1539 (2016)
5. Chen, G., Tang, J., Coon, J.P.: Optimal routing for multi-hop social-based D2D communications in the internet of things. IEEE Internet Things J. **5**(3), 1880–1889 (2018)
6. Coskun, V., Ozdenizci, B., Ok, K.: The survey on near field communication. Sensors **15**(6), 13348–13405 (2015)
7. Feng, W., Yan, Z., Zhang, H., Zeng, K., Xiao, Y., Hou, Y.T.: A survey on security, privacy, and trust in mobile crowdsourcing. IEEE Internet Things J. **5**(4), 2971–2992 (2018)
8. Gao, Y., Xiao, Y., Wu, M., Xiao, M., Shao, J.: Dynamic social-aware peer selection for cooperative relay management with D2D communications. IEEE Trans. Commun. **67**(5), 3124–3139 (2019)
9. Guo, Y., Zhang, H., Zhang, L., Fang, L., Li, F.: Incentive mechanism for cooperative intrusion detection: an evolutionary game approach. In: Shi, Y., Fu, H., Tian, Y., Krzhizhanovskaya, V.V., Lees, M.H., Dongarra, J., Sloot, P.M.A. (eds.) ICCS 2018. LNCS, vol. 10860, pp. 83–97. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93698-7_7
10. Haus, M., Waqas, M., Ding, A.Y., Li, Y., Tarkoma, S., Ott, J.: Security and privacy in device-to-device (D2D) communication: a review. IEEE Commun. Surv. Tutor. **19**(2), 1054–1079 (2017)
11. Hu, Z., Zheng, Z., Song, L., Tao, W., Li, X.: UAV offloading: spectrum trading contract design for UAV assisted cellular networks. IEEE Trans. Wirel. Commun. **17**(9), 6093–6107 (2018)
12. Xu, J., Chen, L., Liu, K., Shen, C.: Designing security-aware incentives for computation offloading via device-to-device communication. IEEE Trans. Wirel. Commun. **17**(9), 6053–6066 (2018)
13. Liu, T., Lui, J.C.S., Ma, X., Jiang, H.: Enabling relay-assisted D2D communication for cellular networks: algorithm and protocols. IEEE Internet Things J. **5**(4), 3136–3150 (2018)
14. Liu, Y., Wang, L., Zaidi, S.A.R., Elkashlan, M., Duong, T.Q.: Secure D2D communication in large-scale cognitive cellular networks: a wireless power transfer model. IEEE Trans. Commun. **64**(1), 329–342 (2016)

15. Shamganth, K., Sibley, M.J.: A survey on relay selection in cooperative device-to-device (D2D) communication for 5G cellular networks. In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), pp. 42–46. IEEE (2017)
16. Tang, J., Xue, G., Zhang, W.: Interference-aware topology control and QoS routing in multi-channel wireless mesh networks. In: ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (2005)
17. Ten, C.W., Liu, C.C., Manimaran, G.: Vulnerability assessment of cybersecurity for scada systems. IEEE Trans. Power Syst. **23**(4), 1836–1846 (2008)
18. Wang, H.M., Xu, Y., Huang, K.W., Han, Z., Tsiftsis, T.A.: Cooperative secure transmission by exploiting social ties in random networks. IEEE Trans. Commun. **66**(8), 3610–3622 (2018)
19. Wang, M., Yan, Z.: A survey on security in D2D communications. Mob. Netw. Appl. **22**(2), 195–208 (2017)
20. Xu, C., Proulx, B., Gong, X., Zhang, J.: Exploiting social ties for cooperative D2D communications: a mobile social networking case. IEEE/ACM Trans. Netw. **23**(5), 1471–1484 (2015)
21. Yang, D., Xue, G., Fang, X., Tang, J.: Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing. In: Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, pp. 173–184. ACM (2012)
22. Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social networks: challenges and opportunities. IEEE Netw. **24**(4), 13–18 (2010)
23. Zhang, X., Xue, G., Yu, R., Yang, D., Tang, J.: You better be honest: discouraging free-riding and false-reporting in mobile crowdsourcing. In: 2014 IEEE Global Communications Conference, pp. 4971–4976. IEEE (2014)
24. Zhang, X., Xue, G., Yu, R., Yang, D., Tang, J.: Keep your promise: mechanism design against free-riding and false-reporting in crowdsourcing. IEEE Internet Things J. **2**(6), 562–572 (2015)
25. Zhang, Y., van der Schaar, M.: Reputation-based incentive protocols in crowdsourcing applications. In: 2012 Proceedings of IEEE INFOCOM, pp. 2140–2148. IEEE (2012)
26. Zhou, Q., Lu, W., Chen, S., Yang, L., Wang, K.: Promoting security and efficiency in D2D underlay communication: a bargaining game approach. In: GLOBECOM 2017–2017 IEEE Global Communications Conference, pp. 1–6, December 2017. https://doi.org/10.1109/GLOCOM.2017.8254089
27. Zhou, Z., Yu, H., Chen, X., Yan, Z., Mumtaz, S., Rodriguez, J.: Dependable content distribution in D2D-based cooperative vehicular networks: a big data-integrated coalition game approach. IEEE Trans. Intell. Transp. Syst. **19**(3), 953–964 (2018)