Incentive Mechanism for Cooperative Intrusion Detection: An Evolutionary Game Approach

Yunchuan Guo[1], Han Zhang[1,2], Lingcui Zhang[1], Liang Fang[1], and Fenghua Li[1,2(✉)]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
lifenghua@iie.ac.cn

[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Abstract. In Mobile Ad-Hoc Networks, cooperative intrusion detection is efficient and scalable to massively parallel attacks. However, due to concerns of privacy leak-age and resource costs, if without enough incentives, most mobile nodes are often selfish and disinterested in helping others to detect an intrusion event, thus an ef-ficient incentive mechanism is required. In this paper, we formulate the incentive mechanism for cooperative intrusion detection as an evolutionary game and achieve an optimal solution to help nodes decide whether to participate in detection or not. Our proposed mechanism can deal with the problems that cooperative nodes do not own complete knowledge about other nodes. We develop a game algorithm to maximize nodes utility. Simulations demonstrate that our strategy can efficiently incentivize potential nodes to cooperate.

Keywords: Mobile Ad-Hoc Networks
Cooperative intrusion detection · Privacy · Evolutionary game

1 Introduction

The Mobile Ad-Hoc Networks (MANETs), equipped with wireless transceivers that can communicate with one another without the aid of any centralized infrastructure, are complex networks and widely used in various applications, *e.g.*, military surveillance, commercial sector and personal area networks [1]. However, due to the limitation of resources and openness nature, MANETs are suffering from an increasing number of security intrusions e.g., DDoS, wormhole and sybil attack [2]. To prevent and mitigate these intrusions, one important thing that should be done is to design intrusion detection systems (IDS) to identify intruders, intrusion time/location and intrusion activity. The existing IDSs are roughly divided into two categories: non-cooperative IDS (NCIDS), and cooperative IDS (CIDS) [3]. Because no interaction between multiple NCIDSs takes

Y. Shi et al. (Eds.): ICCS 2018, LNCS 10860, pp. 83–97, 2018.
https://doi.org/10.1007/978-3-319-93698-7_7

place, NCIDSs cannot detect sophisticated and distributed attacks. To address this problem, CIDS has been proposed. In CIDS, if an IDS node detects an intrusion with weak or inconclusive evidence, then it initiates a global detection procedure and invites other nodes that run IDS agents to cooperatively participate in the detection. Compared with NCIDSs, CIDSs with high accuracy, high scalability and low computation overhead have been widely used.

Motivation: In spite of the above advantages, the existing CIDS scheme cannot efficiently work in MANETs, because most nodes in MANETs are selfish and disinterested in helping others to detect an intrusion event for the following reasons: (1) *Resource limitation*. Most nodes in MANETs own the limited resources (including computation resources and communication resources); they have to save these resources for their own communications. (2) *Privacy issues*. Most nodes depend on open wireless channels to communicate. As a result, an attacker easily detects other nodes presence, recognizes their identifications and tracks their locations by periodically monitoring data traffic. Thus, without enough incentives a selfish node cannot cooperate timely and the number of cooperators drastically decreases, thus intrusion detection rate is greatly reduced. Therefore, we should design an incentive mechanism to incentivize nodes to cooperate timely and ensure that, once a detection task is released, potential cooperators will immediately participate in task.

From the aspect of *methodology* being used to incentive participation, the existing work can be roughly divided into two categories [4]: *game-theoretical* approaches and *non-game-theoretical* approaches. In most of *non-game-theoretical* approaches, a center platform is often designed to allocate incentive resources (*e.g.*, digital cash) to cooperators and maximize its utility. However, these approaches often ignore the optimal utility of cooperators. To address this problem, the *game-theoretical* approaches are proposed. In these approaches, each potential cooperator is usually assumed to be rational. That is, individual users make their strategic choice on a wholly rationally determined evaluation of probable outcomes to maximize their utility. However, this assumption is not reasonable enough for MANETs, because MANETs have a large number of mobile nodes and their network topology frequently changes. As a result, most nodes do not know the global topology completely in practice. Namely, compared with the adequate rationality assumption in traditional game theory, it is more realistic to consider the nodes in MANETs to be with bounded rationality.

Contribution: In this paper, we assume that nodes in MANETs are not adequate rationality but bounded rationality, and the game aspects of CIDSs are investigated. Our main contributions are as follows.

(1) Considering bounded rationality of users and dynamics of cooperative intrusion detection, we formulate the incentive mechanism for cooperative detection as an evolutionary game.

(2) We design a budget-assignment mechanism to encourage nodes to timely cooperate and achieve the Evolutionary Stable Strategy (ESS) in our evolutionary game.
(3) We design an ESS-based algorithm and carry out the simulation. The results show that our proposed strategy can efficiently incentivize nodes to participate in cooperation.

The rest of this paper is organized as follows. In Sect. 2, we discuss the related work. In Sect. 3, we introduce our system model. Section 4 formulates the incentive scheme as an evolutionary game and analyzes the factors that affect nodes benefit. We conduct game analysis in Sect. 5. Simulations and their analysis are given in Sect. 6. We draw a conclusion in Sect. 7.

2 Related Work

2.1 Cooperative IDS

In our paper, selfishness of nodes in MANETs is assumed to be caused by the privacy issues and concerns of resource overhead; thus, in this subsection, we discuss the related work from the aspects of privacy protection and resource overhead.

Privacy Protection. A large number of techniques (*e.g.* Bloom filter [5], multi-party computation [6,7] and different privacy [8]) have been proposed to address the privacy requirements in intrusion detection. For example, Shu *et al.* [5] designed a privacy protection scheme by combining Bloom filters along with a trusted list of participant peers. In *GrIDS* [3], a cooperator can only observe intrusion activity restricted within its boundaries to protect privacy. Using additive homomorphic encryption, Do and Ng [7] designed a privacy-preserving scheme for sharing and processing intrusion alert data. Jin *et al.* [9] formulated privacy protection in cooperative IDS as a Stackelberg game and obtained Stackelberg-Nash equilibrium. Although these approaches try their best to protect privacy, privacy information might be still leaked in practice [10]. Thus, a selfish node might be disinterested in helping others to detect abnormal behaviors.

Resource Overhead. In CIDSs, a cooperative node has to exchange its local observations with others, thus, incurring high resource overhead. To reduce overhead, several solutions have been proposed. For instance, Hassanzadeh and Stoleru [11] formulated optimal monitoring in CIDS as a multi-objective optimization problem and developed a genetic algorithm to decrease computation complexity. Gil Perez *et al.* [12] introduced the notion of trust diversity among to increase both in detection quality and reduce communication overhead. Subba et al. [13] used a packet header anomaly detector to analyze the data packets header and minimize the computational overhead. Undoubtedly, if a node cooperates, its consumed resources could not be ignored. Thus, a selfish node does not cooperate still.

2.2 Incentive Mechanism

Although a large number of efforts have been spent on incentivizing selfish nodes to cooperate, little work focuses on the incentives in IDS. Thus, in this subsection, incentive mechanisms, designed for participatory sensing (which can be potentially used in CIDS) are overviewed. From the aspect of *methodology*, the existing incentive mechanism can be roughly divided into the two categories [4]: *non-game-theoretical* approaches and *game-theoretical* approaches.

The *non-game-theoretical* approaches, designed for specific or general applications can be divided into three categories: QoI (quality of information)-aware mechanisms [14,15], resource-aware mechanisms [4,16] and privacy-aware mechanisms [17]. Guo et al. [14] designed an incentive mechanism for IoT searches to collect real-time data. Considering data quality, Peng et al. [15] paid the participants as how well they do, to motivate the rational participants to efficiently perform tasks. Zheng et al. [16] studied on the coverage problem for incentive-compatible mobile crowd-sensing and proposed a budget feasible and strategy-proof incentive mechanism for weighted coverage maximization. Ma et al. [17] leveraged a conditional random field to model the spatio-temporal correlations among the contexts, and proposed a speed-up algorithm to preserve privacy while maximizing the amount of data collection. Although these approaches efficiently maximize the data quality at acceptable costs, they do not maximize the participant utility.

To address this problem, the *game-theoretical* approaches are proposed. In these approaches, each player is assumed to be rational and selfish and interested in maximizing its own utility. Yang et al. [18] used a Stackelberg game to design an incentive mechanism and show how to compute the unique Equilibrium. Guo et al. [19] and Lv et al. [18] used coalitional game theories to evaluate cooperation in MANETs and VANETs, respectively. Mukhopadhyay et al. [20] proposed a truthful quality adaptive participatory sensing in an online double auction environment. However, these efforts focus on the short-term utility of cooperators and ignore the long-term benefit. To address this problem, the repeated game for MONs is proposed [21]. Yin et al. [21] use the "dissemination interesting" to motivate nodes to forward advertisement. Obviously, notation "dissemination interesting" is not suitable for intrusion detection.

In these approaches, players are assumed to be completely rational. These assumptions are not reasonable enough for MANETs, because nodes in MANETs moves over time and network topology frequently changes. As a result, the global topology is unknown by most nodes in practice. This means that nodes in MANETs are not adequate rationality but bounded rationality. Additionally, in these approaches, the *real-time* requirement is not considered. Obviously, this requirement is critical for intrusion detection and if, without timely detection, cooperative detection will not come to fruition.

3 Basic Idea and System Model

In CIDSs for MANETs, a potential cooperator that runs an IDS agent participates in the global intrusion detection, as follows. If a node (named initiator, *e.g.*, n_0) detects an intrusion even with weak or inconclusive evidence, then it initiates a global detection procedure and sends a detection request (or detection task) to potential cooperators $\mathcal{N} = \{n_1, \ldots, n_N\}$, where N is the number of potential cooperators. Once receiving this request, cooperators start local detections and report the detected abnormal behaviors to the initiator. After receiving r detection reports, the initiator clusters, merges and correlates these abnormal behaviors. If the initiator confirms an intrusion with sufficient evidence, then it alerts the whole networks regarding an attack. Generally, the more nodes participate in the detection, the higher is the intrusion detection rate. Without loss of generality, we assume that detection rate for each node is ρ. If r nodes participate in cooperating, then the overall detection rate *odr* is

$$odr(r, \rho) = 1 - (1 - \rho)^r \tag{1}$$

As shown in Sect. 1, if a node participates in detecting an intrusion, its privacy might be exposed and its resource might be consumed. Thus, selfish nodes are typically disinterested in helping others. To encourage nodes to timely cooperate, an auction approach is used in this paper. In detail, we regard the detection service as goods, each potential cooperator that detects an intrusion event acts as an offer, sells its service and wins virtual credits, and the initiator n_0 acts as a bidder and pays for the service to cooperators.

More specially, for each potential intrusion event to be detected, node n_0 divides the whole detection time into slices with the same length, indexed by natural numbers. In a time slice, a sub-auction is performed. In each sub-auction, the detection service that a potential cooperator provides is called a sub-service. Before each sub-auction (*i.e.*, at the first time-slice) starts, the initiator n_0 constructs a sub-auction pool. Before the sub-auction ends, each potential cooperator can enter the pool. When the auction starts, the initiator n_0 broadcasts the total of budget $\gamma \in R$ that n_0 will pay for the total detection service. A potential cooperator $n_i\,(1 \leq i \leq \mathrm{N})$ calculates its cost for the service and evaluates its possible benefit. Based on the cost and the benefit, cooperator n_i decides whether to make an offer or not. When a time-slice ends (*i.e.*, this sub-auction ends), the winning neighboring nodes provide the sub-services. After completing the service, the potential cooperator obtains the rewards from initiator n_0 and the next sub-auction starts. Note: the intrusion event to be detected in the next sub-auction is the same with the intrusion of the previous sub-auction. The whole auction ends if all time-slices are exhausted or *odr* is greater than the threshold value given by initiator n_0.

4 Budget and Cost

In this section, we discuss the budget of the initiator and the cost of potential cooperators in cooperative detection.

4.1 Total Budget

In our work, we use virtual credits to motivate nodes to cooperate. That is, virtual credits are paid to cooperators after a detection task is completed. The total reward for the whole detection relies on budget. Because the main goal of an initiator is to improve the intrusion detection rate, a higher detection rate required means a more budget that initiator n_0 should pay to cooperators. In our work, for an intrusion event to be detected, we use γ to denote the budget that n_0 is willing to pay for the detection. Let odr' be the actual detection rate provided by the neighboring nodes after the total auction ends. The total reward paid to all cooperators for the whole detection is $odr' \times \gamma$. Note: the total reward depends on the budget γ and the actual odr', and the entire budget does not have to be used up. This approach is rational. For example, assume that initiator n_0 offers the higher budget to encourage more cooperators, but only one node cooperates. Obviously, in this case, it would be inappropriate for n_0 to assign the total budget to the only cooperator.

4.2 Budget Assignment

It is of importance to design an appropriate mechanism to assign the budget to the cooperators. In cooperative detection, one of important concerns is the real-time. That is, an assignment mechanism should ensure that, once initiator n_0 requests its potential cooperators to help it detect its data, these cooperators will immediately participate in detection and no one will be in a "wait and see" state. If a node is in this state, data provided by this node are the old ones. To address this problem, the designed budget-assignment scheme should guarantee that, a cooperator who timely participates in detection receives more rewards than a procrastinator. That is, the earlier a node participates in a cooperation, the more its reward is.

Let r_i denote the number of nodes who cooperatively complete the detection at the end of sub-auction i. Thus, the number r_i^{co} of cooperators in sub-auction i is $r_i^{\mathrm{co}} = r_i - r_{i-1}$. The reward $reward(i)$, paid to a cooperative node in sub-auction i, is defined as follows.

$$reward\,(i) = \gamma \times \frac{odr(r_i, \rho) - odr(r_{i-1}, \rho)}{r_i^{co}} \tag{2}$$

Proposition 1. If $0 \leq \rho < 1$ and the arriving rate is the same, the $reward(i)$ paid to the cooperator of sub-auction i is always greater than $reward(i+j)$ paid to the node of sub-auction $i + j (i, j > 0)$.

Proof. According to Formula (2), the second derivative of $odr(x, \rho)$ with respect to variable x is

$$\frac{\partial^2 odr(x,\rho)}{\partial x^2} = -\gamma \left((1-\rho)^x (\ln(1-\rho))^2 \right) \tag{3}$$

Due to $0 \leq \rho < 1$ and $\gamma > 0$, $\frac{\partial^2 odr(x,\rho)}{\partial x^2} < 0$ holds. This means that $odr(x, \rho)$ is convex regarding variable x. Because $odr(r, \rho)$ is the discrete version of $odr(x, \rho)$, $reward(i) > reward(i + j)$ holds. We can reach this proposition.

Note: This budget-assignment scheme guarantees that, the benefit of an early cooperator is greater than or equals the benefit of the later one, but not "strictly greater than" (because all cooperators in a sub-auction averagely share the rewards paid for this sub-auction). If there is only one cooperator in each sub-auction, the benefit of an early cooperator is strictly greater than the benefit of the later one. We do not adopt this scheme because of privacy protection, discussed in the next subsection.

4.3 Privacy Cost

As shown in Sect. 1, privacy is a key element that affects a potential cooperator whether to participate in cooperation. To mitigate privacy leakage, several techniques (*e.g.*, pseudonyms and different privacy [8]) have been designed. In our work, pseudonyms technique is used to protect privacy: in a sub-auction, cooperators simultaneously and silently change their pseudonym. We use *uncertainty*, describing a situation involving ambiguous and/or unknown information, to measure a privacy level [22], as follows.

Assume that r_i^{co} cooperators simultaneously and silently change their pseudonym while detecting an intrusion. Then the privacy level of each cooperator is defined as $\log_2(1 + r_i^{co})$. When $r_i^{co} = 1$ (that is, only one node changes its pseudonym), the privacy level reaches minimum and equals 1. In this case, an adversary can accurately relate the new pseudonym with the old one, thus, privacy cost reaches the highest. In our model, privacy cost $pc(i)$ of a cooperator in sub-auction i inversely proportional to its current privacy level, defined as follows.

$$pc(i) = \begin{cases} \frac{\lambda}{\log_2(1+r_i^{\mathrm{co}})} \; if \; r_i^{\mathrm{co}} > 0 \\ 0 \qquad\quad \text{otherwise} \end{cases} \tag{4}$$

where $\lambda > 0$ is the cost of a pseudonym. From Formula (4), we can see that, privacy cost equals λ, if there is only one cooperator.

5 Evolutionary Cooperation Game and Its Analysis

We model cooperative detection in an inadequate rational environment as an evolutionary game. We refer to this model as *Evolutionary Cooperation game*. The key aspect of the game-theoretic analysis is to consider benefit and cost of a potential cooperator. For a potential cooperator, if its benefit is greater than its cost, it will cooperate. Next we define our game.

5.1 Evolutionary Cooperation Game

Evolutionary Cooperation game is defined as a triplet $G = (\{n_0\} \cup \mathcal{N}, \mathcal{S}, \mathcal{U})$, where $\mathcal{N} = \{n_1, \ldots, n_N\}$ is the set of a potential cooperators, $\mathcal{S} = \{S_j\}_{j=1}^{N}$ is the set of strategies of nodes, where $S_j = \{C, D\}$ denotes the strategy chosen by $n_j (1 \leq j \leq N)$, C and D stand for *Cooperation* and *Defect*, respectively. For simplicity, the strategy chosen by node j is denoted by s_j and strategies of all nodes but j are denoted by set $\mathbf{s_{-j}}$. $\mathcal{U} = \{u_{i,1}(s_1, \mathbf{s_{-1}}), \ldots, \mathbf{u_{i,N}}(\mathbf{s_N}, \mathbf{s_{-N}})\}$ is the set of payoff functions of nodes at sub-auction i, where the payoff $u_{i,j}(s_j, \mathbf{s_{-j}})$ of node j in sub-auction i is the difference between its gain and its cost, defined as follows.

- If there are $r_i^{co} > 0$ cooperators in sub auction i, then the payoff $u_{i,j}(s_j, \mathrm{s_{-j}})$ for cooperator j is $u_{i,j}(s_j, \mathrm{s_{-j}}) = reward(i) - pc(i)$

$$= \gamma \times \frac{(1-\rho)^{r_{i-1}} \left(1-(1-\rho)^{r_i^{\mathrm{co}}}\right)}{r_i^{\mathrm{co}}} - \frac{\lambda}{log_2(1+r_i^{\mathrm{co}})} \tag{5}$$

- Otherwise, the payoff $u_{i,j}(s_j, \mathbf{s_{-j}})$ for defector j equals 0.

In Formula (5), a potential cooperator easily obtain parameters γ, ρ, λ and r_{i-1}. If a node knows the number r_i^{co} of cooperators in Formula (5) in advance, then it can easily make an optimal decision. Namely, for node j, if $u_{i,j}(s_j, \mathbf{s_{-j}})$ ¿0, then its optimal section is to participate in cooperation; otherwise it will reject cooperation. However, in practice, no node apart from the initiator knows r_i^{co} because r_i^{co} is the private information of the initiator. To address this problem, we formulate the game as evolutionary game. Namely, a potential cooperator plays game repeatedly and its behavior evolves over time. At time t, a potential cooperator chooses strategy s $(s \in \{C, D\})$ with probability X $(X \in [0, 1])$; at time $(t+1)$, it adjusts the probability with the growth rate $X\frac{\mathrm{d}X}{\mathrm{d}t}$, where is proportional to the difference between its current payoff $u(s)$ that adopts strategy s and the current average payoff $\overline{u(s)}$ of all nodes. Given parameters γ, ρ, λ and r_{i-1}, if probability X converges to evolutionary stable strategy (ESS) x regardless the initial value of X, then the optimal decision for the potential cooperator is to cooperate with probability x. To calculate the ESS, we define replicator dynamics as follows.

5.2 Replicator Dynamics

To specify replicator dynamics, we first define the notations as shown in Table 1, where $u(C) = \gamma \frac{odr(r_{i-1}+XN,\rho) - odr(r_{i-1},\rho)}{XN} - \frac{\lambda}{\log_2(1+XN)}$ and $\overline{u(C)} = Xu(C)$. Replicator dynamic express which describes how X change with time t, can be defined as follows.

$$\begin{aligned}\frac{\mathrm{d}X}{\mathrm{d}t} &= X(u(C) - \overline{u(C)}) \\ &= X(1-X)\left(\frac{\gamma(1-\rho)^{r_{i-1}}\left(1-(1-\rho)^{XN}\right)}{XN} - \frac{\lambda}{\log_2(1+XN)}\right)\end{aligned} \tag{6}$$

Table 1. Notations in replicator dynamics.

X	Probability with which nodes use the *cooperation* strategy
N	Number of potential cooperators
$u(C)$	Benefit of a cooperator
$\overline{u(C)}$	Average benefit of cooperators

5.3 Replicator Dynamics

An evolutionary stable strategy (ESS) is a strategy which if adopted by a population cannot be invaded by any competing alternative strategy[1]. Namely, strategy X is an ESS if the following two conditions are satisfied [23]: (1) an individual adopting strategy X must do better against another individual adopting strategy X than any other strategy; and (2) should a new strategy evolve (X') that does equally well against strategy X for X to be an ESS, an individual employing strategy X must do better than an individual employing strategy X'. Formally, let $u(s,t)$ represent the utility for playing strategy s against strategy t, the strategy pair (s,s) is an ESS in a two player game if and only if one of the following conditions is true for both players and for all $t \neq s$:

1. $u(s,s) > u(t,s)$, or
2. $u(s,s) = u(t,s)$ and $u(s,t) > u(t,t)$

Next, we conduct an ESS analysis.

Let $f(X) = \frac{\mathrm{d}X}{\mathrm{d}t} = 0$. We have $X = 0, 1$ or X which satisfy the following equation:

$$\frac{\gamma(1-\rho)^{r_{i-1}}\left(1-(1-\rho)^{XN}\right)}{XN} = \frac{\lambda}{\log_2(1+XN)} \tag{7}$$

The derived function of $f(X)$ is
$f'(X) = (1-2X)(\frac{\gamma(1-\rho)^{r_{i-1}}(1-(1-\rho)^{XN})}{XN}) + X(1-X)g(X)$, where

$$g(X) = \frac{\lambda N \frac{\log_2 e}{1+XN}}{(\log_2(1+XN))^2} + \frac{\gamma(1-\rho)^{r_{i-1}}((1-\rho)^{XN}(-NX\ln(1-\rho)+1)-1)}{X^2N}$$

[1] https://en.wikipedia.org/wiki/Evolutionarily_stable_strategy.

– Consider $X = 1$. If $f^{'}(1) = -\left(\frac{\gamma(1-\rho)^{r_{i-1}}\left(1-(1-\rho)^{N}\right)}{N} - \frac{\lambda}{\log_2(1+N)}\right) < 0$, then $X = 1$ can be ESS. That is, if $\frac{\gamma}{\lambda} > \frac{N}{\log_2(1+N)(1-\rho)^{r_{i-1}}(1-(1-\rho)^{N})}$, then $X = 1$ is ESS.
– Consider $X = 0$. Because the derived function of $f(X)$ is not well-defined at 0, we consider the limit of derived function at 0.
$\lim_{X\to 0^+} f^{'}(X) = Z_1 + Z_2 + Z_3$, where

$$Z_1 = \lim_{X\to 0^+}(1-2X)\left(\frac{\gamma(1-\rho)^{r_{i-1}}\left(1-(1-\rho)^{XN}\right)}{XN} - \frac{\lambda}{\log_2(1+XN)}\right)$$
$$= -\gamma(1-\rho)^{r_{i-1}}\ln(1-\rho) - \lim_{X\to 0^+}\frac{\lambda(1-2X)}{\log_2(1+XN)}$$
$$Z_2 = \lim_{X\to 0^+} X(1-X)\frac{\lambda N\frac{\log_2 e}{1+XN}}{(\log_2(1+XN))^2}$$
$$Z_3 = \lim_{X\to 0^+} X(1-X)\frac{\gamma(1-\rho)^{r_{i-1}}((1-\rho)^{XN}(-NX\ln(1-\rho)+1)-1)}{X^2N} = 0$$

So, $\lim_{X\to 0^+} f^{'}(X) = Z_1 + Z_2$

$$= -\gamma(1-\rho)^{r_{i-1}}\ln(1-\rho) - \lim_{X\to 0^+}\frac{\lambda(1-2X)}{\log_2(1+XN)} + \lim_{X\to 0^+} X(1-X)\frac{\lambda N\frac{\log_2 e}{1+XN}}{(\log_2(1+XN))^2}$$

Due to $\lim_{X\to 0^+} X(1-X)\frac{\lambda N\frac{\log_2 e}{1+XN}}{(\log_2(1+XN))^2} - \lim_{X\to 0^+}\frac{\lambda(1-2X)}{\log_2(1+XN)} = \frac{-\lambda(N-2)}{2N}\ln 2$, we have the following results.

$$\lim_{X\to 0^+} f^{'}(X) = -\gamma(1-\rho)^{r_{i-1}}\ln(1-\rho) + \frac{-\lambda(N-2)}{2N}\ln 2$$

Namely, when $\gamma(1-\rho)^{r_{i-1}}\ln(1-\rho) > \frac{\lambda(N-2)}{2N}\ln 2$ holds, $X = 0$ is ESS.
– Given ρ, λ, γ, N and r_{i-1}, if the solution of equation exists (let it be X') and $f^{'}(X) < 0$, then $X = X'$ is an ESS.

Given ρ, λ, γ, N and r_{i-1}, we can easily obtain its solutions of Formula (7) using either bisection or Newton's method [24]. Based on the ESS, we can design algorithms (as shown in Algorithms 1 and 2) to incentivize inadequately rational nodes to maximize their benefit.

Algorithm 1. Game for Initiator

Initiating phase: given a potential intrusion event to be detected, n_0 selects a budget γ, the round rd of the allowed sub-auctions, the allowed auction period apd for each sub-auction and the expected overall detection rate $\overline{odr}$; n_0 sets the initial number of cooperators $r_0 = 0$, the initial overall detection rate $odr = 0$ and the current auction round $i = 1$;
Auction phase:
while $i \leq$ rd *and* $odr < \overline{odr}$ **do**
  n_0 broadcasts i, γ and $r_i - 1$ to its all potential cooperators;
  $i = i + 1$;
  for *(;;)* **do**
    n_0 records the number r_i^{co} of bidders;
    if *the sub-auction period* $>$ apd **then**
      break;
    end
  end
  $r_i = r_{i-1} + r_i^{co}$;
  Computing $odr = odr(r_i, \rho)$ according to Formula (1);
end
Pay-off phase: After completing detection, n_0 allocates *rewards* to each bidder according to Formula (3).

6 Experiment Evaluation

In the simulation, without the special statement, we set the default value of the parameters to $\rho = 0.5$, $\lambda = 1$, $\gamma = 100$, and $N = 15$.

Evolution Process. We fixed parameters ρ, λ, and N, and then picked different γ and initial cooperation probability x of a neighboring node in order to check how the evaluation process is conducted. The evolution was updated in the following manner: $x = x + \frac{\mathrm{d}x}{\mathrm{d}t} \times t$, where $\mathrm{t} = 0.001$ is a step size. From Fig. 1, we can see that for a given total budget γ, the replication dynamics always converges to the ESS x^* regardless the initial probability x.

Cost v.s. Cooperation Probability. Figure 2 presents the change of cooperation probability over pseudonyms cost. From Fig. 2, we can see that, given the number of potential cooperators N, the cooperation probability x decreases as the pseudonyms cost λ increases, and increases as budget γ increases. This phenomenon is reasonable: if privacy cost increases or budget decreases, then the benefit of a node in each cooperation decreases, thus, it is disinterested in cooperation.

Algorithm 2. Game for Potential Cooperator

Initiating phase: Each potential cooperator first sets ρ, λ and observes the number N of potential cooperators;
Auction phase:
The potential cooperator receives i, γ and r_{i-1} from the initiator;
if $\frac{\gamma}{\lambda} > \frac{N}{\log_2(1+N)(1-\rho)^{r_{i-1}}(1-(1-\rho)^N)}$ **then**
  the potential cooperator participates in detecting the intrusion event;
end
else if $-\gamma(1-\rho)^{r_{i-1}}\ln(1-\rho) < \frac{\lambda(N-2)}{2N}\ln 2$ *holds* **then**
  the potential cooperator refuses to cooperate;
end
else
  Calculate the probability X by solving Formula (7)
  if $f'(X) < 0$ *holds* **then**
    the potential cooperator participates in detecting the intrusion event with probability X;
  end
  else
    the potential cooperator refuses to cooperate.
  end
end

Pay-off Phase: If the potential cooperator bids, then it participates in detection. After detecting the intrusion, it gets rewards from the initiator.

Number of Completed Tasks . In the experiment, we adopted a city scenario including 17937 GPS records of 1792 taxis in three representative areas of Beijing C the Guangqumen area, covering 1.885 km × 1.752 km, the Shijingshan area, covering 1.078 km × 2.532 km, and the Changping area, covering 3.144 km × 5.701 km. These records were gathered from 8:00:00 a.m. to 8:59:59 a.m. on August 13, 2015. During this period, the densities of vehicles in the Guangqumen, Shijingshan and Changping areas were high, middle and low, respectively (namely a dense scenario, a medium scenario, and a sparse scenario, respectively). The numbers N of potential coopera-tors of the three areas (which denote the numbers of taxis of the three areas) are 824, 526 and 442, respectively. We assume that: (1) each passenger in a taxi own a smartphone to collect data, (2) budget $\gamma = 50$, detection rate $\rho = 0.65$, pseudonyms cost $\lambda = 0.2$, the *odr* required by node n_0 is greater than 0.98, then according to Formula (1), at least 5 neighboring nodes cooperatively detect the data collected by n_0. Assume that Next, we discuss 5 strategies: 'selflessness' strategy (i.e., all nodes are selfless), '70%-selflessness' strategy (i.e., 70% of nodes are selfless), '30%-selflessness' strategy (i.e., 30% of nodes are selfless), 'selfishness' strategy (i.e., all nodes are selfish) and our strategy.

As shown in Fig. 3, the number of tasks completed in our approach is always greater than the number in the other approaches. For instance, when the number

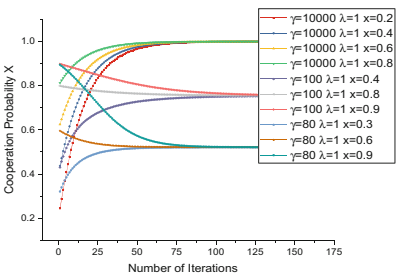


Fig. 1. Evolution process

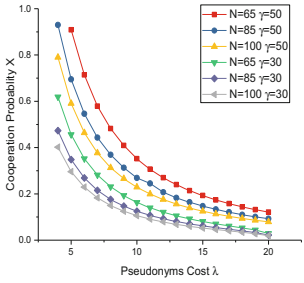
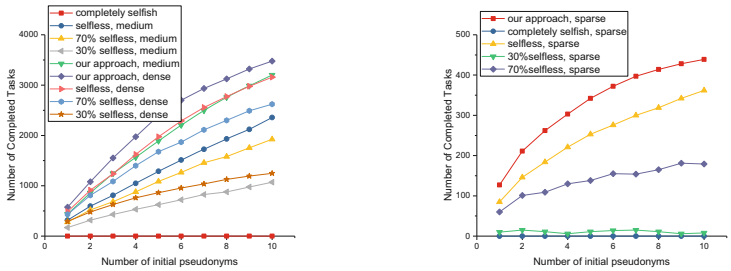


Fig. 2. Cost *v.s.* cooperation probability



(a) Dense / medium scenario

(b) Sparse scenario

Fig. 3. Number of initial pseudonyms *v.s.* number of completed tasks.

of initial pseudonyms is 10, we can see that: (1) In the dense scenario, 2622 tasks were completed if the *70%-selfless* approach was used, 3158 tasks were completed if the selfless approach was used, and 3478 tasks were completed if our approach was used. (2) In the sparse scenario, the number of tasks completed in our approach was 54 times greater than the number of tasks completed in the *30%-selfless* approach. The reason is as follows: if without incentive, once pseudonyms of a node are exhausted, it does not detect messages any more. In our approach, even if pseudonyms of a node are exhausted, it can use the obtained reward enough to purchase new pseudonyms. Therefore, our approach has overwhelming advantages over the other approaches.

7 Conclusion

We have considered the incentive mechanism for cooperative detection to motivate nodes to participate in cooperation. In detail, a game-theoretic approach is proposed to guarantee that mobile nodes participating in detection maximize their utility while reducing resource consumption. To address the problem that nodes are inadequately rational, we have established evolutionary games. We also have developed algorithms for evolutionary game to encourage nodes to

participate in cooperation. The simulation demonstrates the efficiency of our approach.

Acknowledgement. This work is supported by the National Key Research and Development Program of China (No. 2016YFB0801001) and the National Natural Science Foundation of China (No. 61672515).

References

1. Loo, J., Mauri, J.L., Ortiz, J.H.: Mobile Ad-Hoc Networks: Current Status and Future Trends. CRC Press, Boca Raton (2016)
2. Nadeem, A., Howarth, M.P.: An intrusion detection & adaptive response mechanism for MANETs. Ad Hoc Netw. **13**, 368–380 (2014)
3. Vasilomanolakis, E., Karuppayah, S., Muhlhauser, M., Fischer, M.: Taxonomy and survey of collaborative intrusion detection. ACM Comput. Surv. **47**, 1–33 (2015)
4. Restuccia, F., Das, S.K., Payton, J.: Incentive mechanisms for participatory sensing: survey and research challenges. ACM Trans. Sens. Netw. **12**, 1–40 (2016)
5. Shu, X., Yao, D., Bertino, E.: Privacy-preserving detection of sensitive data exposure. IEEE Trans. Inf. Forensics Secur. **10**, 1092–1103 (2015)
6. Niksefat, S., Sadeghiyan, B., Mohassel, P., Sadeghian, S.: ZIDS: a privacy-preserving intrusion detection system using secure two-party computation protocols. Comput. J. **57**, 494–509 (2014)
7. Do, H.G., Ng, W.K.: Privacy-preserving approach for sharing and processing intrusion alert data. In: Proceedings of IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 7–9 (2015)
8. Reed, J., Aviv, A.J., Wagner, D., Haeberlen, A., Pierce, B.C., Smith, J.M.: Differential privacy for collaborative security. In: Proceedings of the Third European Workshop on System Security, pp. 1–7 (2010)
9. Jin, R., He, X., Dai, H.: On the tradeoff between privacy and utility in collaborative intrusion detection systems - a game theoretical approach. In: Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp (HotSoS), pp. 45–51 (2017)
10. Niksefat, S., Kaghazgaran, P., Sadeghiyan, B.: Privacy issues in intrusion detection systems: a taxonomy, survey and future directions. Comput. Sci. Rev. **25**, 69–78 (2017)
11. Hassanzadeh, A., Stoleru, R.: Towards optimal monitoring in cooperative IDS for resource constrained wireless networks. In: Proceedings of IEEE ICCCN, pp. 1–8 (2011)
12. Gil Perez, M., Tapiador, J.E., Clark, J.A., Martnez Perez, G., Skarmeta Gomez, A.F.: Trustworthy placements: improving quality and resilience in collaborative attack detection. Comput. Netw. **58**, 70–86 (2014)
13. Subba, B., Biswas, S., Karmakar, S.: Enhancing effectiveness of intrusion detection systems: a hybrid approach. In: Proceedings of IEEE International Conference on Advanced Networks and Telecommunications Systems, pp. 1–6 (2016)
14. Guo, Y., Fang, L., Geng, K., Yin, L., Li, F., Chen, L.: Real-time data incentives for IoT searches. In: IEEE International Conference on Communications (2018)
15. Peng, D., Wu, F., Chen, G.: Data quality guided incentive mechanism design for crowdsensing. IEEE Trans. Mob. Comput. **17**, 307–319 (2018)

16. Zheng, Z., Wu, F., Tang, S.: A budget feasible incentive mechanism for weighted coverage maximization in mobile crowdsensing. IEEE Trans. Mob. Comput. **16**, 2392–2407 (2017)
17. Ma, Q., Zhang, S., Zhu, T., Liu, K., Zhang, L., He, W., Liu, Y.: PLP: protecting location privacy against correlation analyze attack in crowdsensing. IEEE Trans. Mob. Comput. **16**, 2588–2598 (2017)
18. Yang, D., Xue, G., Fang, X., Tang, J.: Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing. In: Proceedings of IEEE MOBILCOM, pp. 173–184 (2012)
19. Guo, Y., Yin, L., Liu, L., Fang, B.: Utility-based cooperative decision in cooperative authentication. In: Proceedings of IEEE INFOCOM, pp. 1006–1014 (2014)
20. Mukhopadhyay, J., Pal, A., Mukhopadhyay, S., Singh, V.K.: Quality adaptive online double auction in participatory sensing. J. Inform. Math. Sci. **9**, 571–593 (2017)
21. Yin, L., Guo, Y., Li, F., Sun, Y., Qian, J., Vasilakos, A.: A game-theoretic approach to advertisement dissemination in ephemeral networks. World Wide Web J. **21**, 241–260 (2018)
22. Yu, R., Kang, J., Huang, X., Xie, S., Zhang, Y., Gjessing, S.: MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. IEEE Trans. Dependable Secur. Comput. **13**, 93–105 (2016)
23. Cowden, C.C.: Game theory, evolutionary stable strategies and the evolution of biological interactions. Nat. Educ. Knowl. **3**, paper 6 (2012)
24. Boyd, S.P., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)