Utility-based Cooperative Decision in Cooperative Authentication

GUO Yunchuan[1,3], YIN Lihua[1,4*], LIU Licai[2], FANG Binxing[2]
[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2]Department of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China
[3]Guangxi Key Laboratory of Trusted Software (Guilin University of Electronic Technology)
[4]Beijing Key Laboratory of IOT Information Security (Institute of Information Engineering, CAS)
{guoyunchuan, yinlihua}@nelmail.iie.ac.cn

Abstract—**In mobile networks, cooperative authentication is an efficient way to recognize false identities and messages. However, an attacker can track the location of cooperative mobile nodes by monitoring their communications. Moreover, mobile nodes consume their own resources when cooperating with other nodes in the process of authentication. These two factors cause selfish mobile nodes not to actively participate in authentication. In this paper, a *bargaining-based game for cooperative authentication* is proposed to help nodes decide whether to participate in authentication or not, and our strategy guarantees that mobile nodes participating in cooperative authentication can obtain the maximum utility, all at an acceptable cost. We obtain Nash equilibrium in static complete information games. To address the problem of nodes not knowing the utility of other nodes, incomplete information games for cooperative authentication are established. We also develop an algorithm based on incomplete information games to maximize every node's utility. The simulation results demonstrate that our strategy has the ability to guarantee authentication probability and increase the number of successful authentications.**

***Index Terms*—Cooperative authentication, location privacy, games**

I. INTRODUCTION

With the explosive development of wireless technologies in recent years, the mobile ad hoc network (MANET) - recognized as a ubiquitous approach for many emerging applications (such as habitat monitoring and surveillance) - has become a research focus in recent years. In a MANET, a large number of mobile nodes with limited resources are generally interconnected through wireless links to deal with specified tasks. These tasks can be divided into data collection, processing and transmission. Moreover, open channels (such as those formed by Bluetooth, WiFi in ad hoc mode, etc.) are used in peer-to-peer wireless communications. In addition, MANETs are often deployed within openly hostile environments. Due to a limitation of resources and its openness nature, MANET is suffering from an increasing number of security attacks to include unauthorized access, wormholes, imitations and injections of false data.

In order to minimize these attacks, cooperative authentication (which involves requesting nodes cooperatively accomplish authentication tasks) are proposed in recent years. In cooperative authentication, a node proves the truth of its identity and/or messages with the cooperation of its neighboring nodes that provide authentication. By means of cooperative authentication, imitative identities or false messages are efficiently filtered as early and accurately as possible. Cooperative authentication not only drastically decreases global resource waste, but also mitigates heavy verification burdens on the data collection unit.

Although cooperative authentication can efficiently save global resources while improving global performance, individual nodes may be unwilling to cooperate in this authentication process for the reasons discussed here: (1) *Leakage of Location Privacy*. In the MANET, most nodes rely on an open wireless channel to communicate with each other. A misbehaving node easily detects other's presence and can track their locations by periodically broadcasting beacon messages and monitoring data flow, thus exposing their location privacy. An example of this is the panda-hunter game, the location of the panda may be exposed to hunters (as a result, the panda can be shot), if no location privacy-preserving mechanism is used. (2) *Limitation of Resources*. The energy, computing resources and storage resources of mobile nodes are generally limited and participating in authentication processes tends to consume resources while reducing the node's overall lifetime. As a result, the number of cooperating nodes drastically decreases, which reduces the recognition of the false identities and messages. Due to these problems, it is of great importance to study the dynamic behaviors of selfish nodes in the cooperative authentication.

In this paper, we investigate the strategic aspects of the cooperative authentication. In contrast with existing approaches, we take into consideration the individual rational nodes that decide locally whether or not to participate in cooperation authentication. Although a selfish node has minimal privacy leakage and resource consumption, it is also unable to receive any utility (thus preventing his message from being authenticated). Based on game-theoretic model theory, we propose a *bargaining-based game for cooperative authentication* to help nodes decide whether to participate in cooperative authentication, thus maximizing their benefits at an acceptable cost. The simulation results show that our proposed strategy provides incentive for the appropriate number of nodes to cooperate, thus enhancing authentication probability (the probability with which false

*YIN Lihua is the corresponding author.
978-1-4799-3360-0/14/$31.00 ©2014 IEEE

messages/identities are recognized), at acceptable levels of privacy leakage and resource consumption.

II. Related Work

Cooperative authentication. From the perspective of purpose, cooperative authentication is usually used to: 1) save resources, (such as storage, communication and computing resources) [1-3], and 2) improve reliability [4-6].

For the first purpose (resource conservation), [1] enhanced the Kerberos protocol to the ad-hoc environment to provide: 1) mutual authentication of each user with respect to the network operator, 2) authentication of each node with respect to its neighbors, and 3) services access authorization in which only legitimate nodes can access the offered services. To address the issue of large computation overhead due to the group signature implementation, [2, 3] proposed a cooperative message authentication, involving verification of a small amount of messages to alleviate the verification burden.

For the second purpose (reliability), [4] proposed a bandwidth-efficient cooperative authentication (BECAN) scheme adopting a cooperative neighbor and router (CNR) - based filtering mechanism and the cooperative bit-compressed authentication technique. This scheme detects and filters injected false data, achieving a high en-routing filtering probability of injected false data with only minor extra overheads. [5] proposed an efficient cooperative authentication scheme for VANETs to improve the ability to resist free-riding attacks.

Although these cooperative authentication mechanisms were shown to either save overhead or improve reliability, privacy leakage were not taken into consideration.

Location Privacy. In MANET, the location of mobile nodes can be tracked and exposed easily by adversaries who monitor their communications. A number of approaches were presented to protect location privacy [10-18]. Generally, these approaches can be roughly classified into 3 categories: 1) the policy-based scheme (PBS)[7], 2) the anonymity-based scheme(ABS) [8-10], and 3) the obfuscation-based scheme (OBS)[11]. In the Platform for Privacy Preferences Project [7] as one of PBS, privacy is provided in three areas - regulation, policy and access control. In the ABS, location privacy is achieved by hiding the user's real identity – that is, hiding the association between a user's identity and sensitive information. ABS can be divided into cloaking techniques such as *k*-anonymity [8] and pseudonym change [9, 10]. OBS blocks the relevance between location information and users' identities by adding noise to the user information, which degrades the accuracy with which it can be located [11].

Incentive Strategy. In order to encourage nodes to participate in cooperation, various incentive mechanisms have been proposed. These incentives can be broadly divided into the following categories: the price-based (also known as credit-based) [12-14], reputation-based[15] and hybrid mechanisms [16, 17].

The basic idea of price-based schemes involves providing incentives by way of virtual currency paid to nodes for offering services (and which they must in turn pay for obtaining services). A great deal of price-based incentive strategies were proposed to stimulate selfish nodes to participate in cooperation. [12] considered a bandwidth exchange (BE) as payment to provide the incentive for cooperation. [13] proposed an incentive paradigm, Controlled Coded packets as virtual Commodity Currency (C4), to induce cooperative behaviors and reduce overhead in MWNs. [14] presented a coverage extension based on incentive scheduling (CEI) to combine the percentage of cooperation and QoS parameters, thus encouraging nodes to cooperate and extend coverage.

The reputation-based mechanism uses the historical behaviors of nodes to assess their reputation, and then distinguishes the cooperative nodes from malicious nodes (selfish nodes) by setting a reputation threshold. For example, [15] introduced a time-slotted mechanism and proposed an adaptive reputation-based incentive mechanism to monitor the changes of node behavior quickly and accurately.

Despite the fact that both the price-based and the reputation-based mechanisms have significant advantages, they have some disadvantages. The price-based mechanism provides no incentive to the rich and selfish nodes to cooperate. The nodes who use reputation mechanisms tend to maintain their reputation only as necessary, and typically just over the reputation threshold. A few studies were presented to address this problem. For example, [16, 17] presented a hierarchical account-aided reputation management system (ARM) and an integrated incentive system, both of which combine the operations and advantages of both reputation-based and price-based mechanisms to efficiently and effectively provide cooperation incentives for MANET.

Game Theory. Game theory is adept at modeling conflict situations and predicting the decisions of participants. In 2011, [18] overviews existing research on security and privacy in computer networks using game-theoretic approaches. In the last 3 years, important progresses have been made in this field. For example, [10] analyzed the conflict between location privacy protection and costs of pseudonym changes in MANET and achieved the balance between maximum location privacy at a minimum cost. [19] used coalitional game theories to evaluate cooperation in vehicular Ad Hoc networks, while presenting a scheme to stimulate cooperation in message forwarding. [17] used game theory to analyze the cooperation incentives provided by both the price-based mechanism and the reputation-based mechanism. [21] considered one seller and one buyer, and designed a bargaining based incentive protocol for opportunistic networks. Different from their work, we consider one seller and one group of potential buyers and propose a utility-based scheme to improve authentication probability and increase the number of successful authentications in cooperative authentication.

III. Preliminaries

In this section, we mainly introduce the fundamentals of the cooperative authentication. The main goal of cooperative authentication is to recognize the false identities and/or messages by a group of cooperative nodes. Figure 1 shows a basic cooperative authentication [4] (Note: In our work, routing

is not considered). In Figure 1, if source node n_0 wants to prove the truth of a message m to destination node n_d, it first sends m to its k neighboring nodes (NNs)(for simplicity, the k NNs are denoted as $n_1 \ldots n_k$, where $k < N$ and N is the number of NNs) and requests them to cooperatively authenticate m. The k NNs return the one-bit authentication code (which denotes whether or not m is true) to n_0, respectively. After receiving the message authentication codes (MACs), n_0 sends m and the k-bit MACs to n_d, which decides whether or not m is true according to the MACs: if all k NNs believe that m is true, then n_d also believes it is true. Otherwise, it is false. As shown in [4], any false identity/data will be recognized if the following conditions are satisfied simultaneously: (1) at least one uncompromised NN participates in the authentication and (2) adversaries cannot correctly guess the MACs generated by uncompromised NNs.

However, nodes may be compromised by adversaries. Without loss of generality, we assume that the compromised probability for each node is ρ, Authentication Probability (AP, which denotes the probability with which the false messages/ identities are successfully recognized) is

$$AP = 1 - \sum_{i=0}^{k} \binom{k}{i} \rho^i \times (1-\rho)^{k-i} \times \frac{1}{2^{k-i}} \quad (1)$$

From (1), for a given ρ, more k equals the higher AP; for a given k, less ρ implies lower AP. Given AP and ρ, we can calculate the least k satisfying the AP via (1).

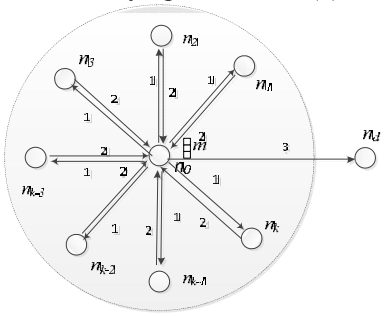


Figure 1. Cooperative Authentication

IV. System Model

We consider cooperative authentication with a source node n_0 and N NNs, denoted by $\mathcal{N}$=$\{n_1, \ldots, n_N\}$. Here, a "source node" refers to the node wanting to prove the truth of its identity/message, and an NN of n_0 is the node within one-hop in the communication range from n_0, as shown in Figure 1.

In cooperative authentication, the privacy information and resource of a participating NN will be exposed and consumed. Thus, selfish nodes are typically unwilling to participate. In order to encourage the appropriate number of NNs to cooperate, a bargaining-based mechanism is proposed in this paper. In our mechanism, the *authentication service* represents the "goods" (here, "*authentication service*" refers to the authentication of a given message/identity provided by $n_1 \ldots n_N$). Two roles are distinguished: 1) a buyer and 2) a group of sellers, where n_0 is the potential buyer (who purchases the *authentication services*) and $\mathcal{N}$=$\{n_1, \ldots, n_N\}$ is the group of potential sellers (who provide the *authentication services*). If n_0 produces a piece of a message requiring authentication, then n_0 must calculate a reservation price and offer a bidding price. At the same time, each of the sellers in $\mathcal{N}$ also calculates reservation prices and offers their own asking price. If the bidding prices are less than the asking prices, then the bargain fails. Next, we discuss the factors affecting the reservation/asking/bidding price in cooperative authentication.

A. Factors affecting the set-price

● *Leakage amount of location privacy.* In the cooperative authentication, NNs worry about their location privacy. The more location privacy leaks that could potentially occur during cooperation, the higher the NNs' reservation/asking price.

Several critical techniques are used to ensure the location privacy of nodes. Among these techniques, the basic concept is distinguishability; that is, adversaries cannot differentiate the true locations of nodes from false nodes or other observed locations. In order to measure location privacy, metrics (for example, uncertainty, inaccuracy and incorrectness [20]) have been proposed by researchers. In our model, the uncertainty approach is used. Let $p(loc_d|loc_i)$ denote the probability with which loc_d corresponds to loc_i ($1 < i < N$). That is, given an adversary and true location loc_i of node i, the adversary believes that node i is located at loc_d with probability $p(loc_d|loc_i)$. The location privacy level of node i is calculated with the adversary's uncertainty:

$$Priv_i = -\sum_{d=1}^{M} p(loc_d|loc_i)\log_2(p(loc_d|loc_i))$$

where M is the number of locations. The achievable location privacy depends on both M and the conditional probability $p(loc_d|loc_i)$. If the conditional probability is of a uniform distribution, then the location privacy level of node i reaches the maximum, denoting as $Priv^i_{max}$, where $Priv^i_{max} = \log_2 M$.

Given node i, its $Priv_i$ and $Priv^i_{max}$, the degree of privacy preservation denoted as PP_i is defined as $PP_i = Priv_i / Priv^i_{max}$. According to information theory, $0 \le PP_i \le 1$ is always true. In addition, $Priv^i_{cons}$ is used to denote the leakage amount of location privacy for a single authentication. $Priv^i_{cons}$ varies in term of the length of messages requiring authentication.

● *Node energy* is another important factor impacting the number of NNs participating in cooperation. In our model, we use three metrics to measure the energy of node i: the initial resource E^i_{max}, the current remaining resource E^i_{remn} and the consumed resource E^i_{cons} for each cooperation. Let $E_i = E^i_{remn}/E^i_{max}$ denote the fraction of the remaining resource. Generally, the less E_i and the more E^i_{cons}, the less cooperative willingness nodes have. Given message m and its length l_m, E^i_{cons} can be defined as a function of l_m, for example, as $E^i_{cons} = \alpha_m + \beta_m \times l_m$, where α_m and β_m are weight.

● *Bandwidth.* When a NN cooperatively authenticates the other's message, its bandwidth is consumed. Thus, *Bandwidth*

is another factor influencing the reservation price. Given message m requiring authentication, the required bandwidth, denoted as $bandwidth_m$, is defined as $bandwidth_m = l_m/TTL_m$, where TTL_m is m's time to live.

● *Required number of cooperative nodes.* In order to guarantee that authentication probability AP reaches a given threshold value, we must ensure that a given number of nodes cooperates in the process of authentication. Note: higher numbers of cooperation nodes do not necessarily imply a better service quality: too many nodes participating causes that too many resources are consumed. Given authentication probability AP, the required number of cooperating nodes can be obtained via formula (1) with the number represented by $minCN$.

● *Fortune.* We use ft_i to denote the fortune owned by node i. Generally, a higher ft_i value implies that node i can bid at a higher price. In order to depict this, we introduce the fortune level fl_i for node i, defined as

$$fl_i = \begin{cases} ft_i / wl & \text{if } ft_i > wl \\ ft_i / pl & \text{if } ft_i < pl \\ 1 & \text{else} \end{cases}$$

Where wl and pl denote the "*wealth line*" and the *"poverty line"*, and $wl>pl$.

B. Bid price

If the buyer n_0 requests its NNs to authenticate its message, n_0 must offer a bidding price b_0 (which depends on the reservation price r_0). Here, the buyer's reservation price refers to the highest virtual currency he is willing to pay for these services. Given a message requiring authentication, r_0 generally relies on the following factors: the required bandwidth, the message length, the required number of cooperation nodes, and n_0's fortune level, defined as follows

$$r_0 = w_{r_0} \times minCN \times l_m \times bandwidth_m \times wl_0 \quad (2)$$

Where w_{r_0} is a weight. According to (2), the buyer's reservation price is positively correlated with $minCN$, l_m, wl_0 and $bandwidth_m$. For a buyer, the higher the reservation price r_0, the higher the bidding price b_0. b_0 can be regarded as an increasing function of r_0, with the constraint of $r_0 \geq b_0$ and $ft_0 \geq b_0$.

C. Ask price

Before every NN n_i ($1 < i < N$, the seller) participates in authentication, it must first offer a asking price s_i. Generally, s_i depends on the reservation price r_i. Here, n_i's reservation price refers to the smallest virtual currency he will accept in exchange for participating in authentication. Given message m requiring authentication, two kinds of attributes affect r_i: 1) the 'message itself', including required bandwidth $bandwidth_m$ and length l_m; and 2) the 'node self', including its current remaining resource E_i, current privacy degree PP_i, the value of $Priv^i_{cons}$ representing the privacy leakage for a single cooperation and the value of E^i_{cons} representing the resource consumption for that cooperation. According to the above factors, similar to [21], the reservation price r_i ($1 < i < N$) is defined as

$$r_i = w_{s_{i0}} \times l_m \times bandwidth_m \times (1 - E_i) \times (1 - PP_i) \times (w_{s_{i1}} \times E^i_{cons} + (1 - w_{s_{i1}}) \times Priv^i_{cons}) \quad (3)$$

Where $w_{s_{i0}}$ and $w_{s_{i1}}$ represent weight, $0 < w_{s_{i0}}$, $0 \leq w_{s_{i1}} \leq 1$. w_{s_1} reflects the weight of E^i_{cons}. Specially, if n_i cares only about E^i_{cons}, then w_{i_1} is set to 1. Similarly, if n_i cares only about $Priv^i_{cons}$, and doesn't care E^i_{cons}, then w_{i_1} is set to 0. Generally, w_{i_1} is set to 0.5. For seller n_i, the higher its reservation price r_i, the higher its asking price s_i. Without loss of generality, s_i can be regarded as an increasing function of r_i, satisfying $r_i \leq s_i$.

D. Bargaining procedure

When n_0 requests its NNs $\mathcal{N}$ to authenticate the message m, the bargain starts and is conducted as follows.

a) n_0 (the buyer) first calculates its reservation price r_0 according to formula (2) and selects its bidding price b_0 satisfying $r_0 \geq b_0$. Then n_0 broadcasts the related parameter (l_m and $bandwidth_m$) of message m to $\mathcal{N}$ (Note: the broadcast message doesn't include r_0 and b_0).

b) After every n_i ($1 < i < N$, the seller) receives l_m and $bandwidth_m$, reservation price r_i is calculated r_i according to formula (3), and asking price s_i is selected.

c) n_0 and all NNs who are willing to cooperate submit their sealed offers b_0 and s_i ($1 < i < N$), respectively. Let $\mathcal{C} = \{C \in 2^{\mathcal{N}} | \sum_{n_i \in C} s_i \leqslant b_0 \text{ and } |C| \geq minCN\}$ be a set of coalitions, where C is called coalition. If there exists a unique coalition C in $\mathcal{C}$ (that is, $|\mathcal{C}|$=1), then the coalition C are chosen to bargain (that is, all members of C participate in authentication). If $|\mathcal{C}|$=0, then the bargain fails. If $|\mathcal{C}|$>1, then one coalition in $\arg\min_{C^j \in \mathcal{C}} |C^j|$ is chosen. Once a coalition C is chosen (this coalition is called *C-Coalition*), then the bargain is struck at agreeing price $P = \varepsilon \times b_0 + (1 - \varepsilon) \times \sum_{n_i \in C} s_i$, where $0 < \varepsilon < 1$.

Next, we discuss special cases surrounding the price P. ε equaling 1 means that P is determined solely by n_0, and the optimal strategy for n_0 involves submitting offer b_0=r_0. This bargain is struck if and only if there exists at least $minCN$ NNs, such that the sum of their asking prices is not greater than r_0. Similarly, ε equaling 0 denotes that P is determined by all n_i ($1 < i < N$), not by n_0.

d) After the bargain is completed, the currency is transferred from n_0 to cooperation node $n_i \in C$. Every node in C gets the virtual currency: $s_i + \frac{P - \sum_{n_i \in C} s_i}{|C|}$, and other nodes receive no currency.

V. GAME FOR COOPERATIVE AUTHENTICATION

We present the game-theoretic aspects of achieving cooperative authentication with location privacy leakage in a

rational environment, referring to the game-theoretic model as the game for cooperative authentication. The key aspect of the game-theoretic analysis is to consider the costs and the gain prior to making a decision.

Definition 1. *Game* G for cooperative authentication is defined as a triple $(\mathbb{NODE}, \mathbb{S}, \mathbb{U})$, where

- $\mathbb{NODE}=\{n_0\}\cup\mathcal{N}$ is a set of players, n_0 denotes the source node and n_i $(1\le i\le N)$ represents the i^{st} NN. Generally, any node can obtain the number of NNs by adopting a neighbor discovery protocol.
- $\mathbb{S}=\{s_{node_i}\}_{i=0}^{N}$ is a set of strategies, where s_{node_i} is the strategy of node i. When n_0 has the message m requiring authentication, it has two options: $\underline{CooPeration}$ and $\underline{Defect}$. When n_0 chooses CP, it sends m to $\mathcal{N}$; However when choosing D, it refuse to send any message to $\mathcal{N}$. Each NN n_i $(1<i<N)$ also has two option: $CooPeration$, or $\underline{Defect}$. If CP is chosen, n_i participates in authenticating$m$; If D is chosen, n_i refuse to authenticate m. Thus, the set S_{node_i} for strategies of n_i $(0<i<N)$ is $\{CP, D\}$. For simplicity, the strategy chosen by n_i is denoted by s_{node_i}, while strategies chosen by other nodes are denoted by a strategy set $\mathbf{s_{node_{-i}}}$. The strategies chosen by all nodes can be rewritten as $\mathbb{S}=(s_{node_i},\mathbf{s_{node_{-i}}})$.
- $\mathbb{U}=\{u_i\}_{i=0}^{N}$ is a set of utility functions, where $u_i(s_{node_i}, s_{node_{-i}})$ denotes the utility function of node i given the strategies used by other nodes. $u_0(s_{node_o}, \mathbf{s_{node_{-0}}})$ is defined as follows:

$$u_0(s_{node_o},\mathbf{s_{node_{-0}}})=\begin{cases} r_0\text{-}P \text{ if } \begin{pmatrix} s_{node_0}=CP \text{ and } \exists C\in 2^{\mathcal{N}} \text{ such that} \\ \sum_{n_i\in C} s_i \le b_0 \text{ and } |C|\ge \min CN \end{pmatrix} \\ 0 \quad else \end{cases} \tag{4}$$

The utility $u_i(s_{node_i}, s_{node_{-i}})$ of n_i $(1<i<N)$ is defined as

$$u_i(s_{node_i},\mathbf{s_{node_{-i}}})=\begin{cases} -r_i & \text{if } s_{node_i}=CP \text{ and } n_i\notin C \\ s_i+\dfrac{P-\sum_{n_i\in C} s_i}{|C|}-r_i & \text{if } s_{node_i}=CP \text{ and } n_i\in C \\ 0 & \text{if } s_{node_i}=D \end{cases} \tag{5}$$

Formula (4) shows the profit earned by n_0 as measured by the difference between the reservation and agreeing prices when the bargain is successful. If the bargain fails, n_0 is unable to obtain any profit. Formula (5) shows: (1) if a NN belonging in a coalition participates in authentication, then its utility is $s_i+\frac{P-\sum_{n_i\in C} s_i}{|C|}-r_i$; (2) if a NN participates in authentication, but doesn't belong to any coalition, it is not paid any virtual currency and its utility is negative because it consumes the resource. (Note: while this utility seems unreasonable, it is realistic in cooperative authentication: the participation of too many nodes results in consumption of too many resources. Thus the negative utility is given to nodes outside of the coalition to inhibit this behavior); (3) If a node refuses to participate in authentication, its utility equals 0.

In the authentication game, each rational node intends to choose a strategy that maximizes its utility for the given strategies chosen by other nodes. That is, the best response (written as $s^*_{node_i}$) of node i to the $\mathbf{s_{node_{-i}}}$ is $\arg\max_{s_{node_i}} u_i(s_{node_i}, \mathbf{s_{node_{-i}}})$.

Definition 2. A strategy profile $\mathbb{S}^*$ is Nash Equilibrium (NE) if $u_i(s^*_{node_i}, \mathbf{s}^*_{\mathbf{node_{-i}}}) \ge u_i(s_{node_i}, \mathbf{s}^*_{\mathbf{node_{-i}}})$ for all i $(0<i<N)$ and all $s_{node_i}\in S_{node_i}$. Informally, a NE is strategy set where any individual rational node cannot unilaterally change strategy to increase its utility.

In our game, a necessary condition of at least $minCN$ NNs participating in authentication is the rational utility allocation to each node in the coalition.

Definition 3. Let $v(\mathcal{T})$ represent the collective Pareto-optimal utility, where $\mathcal{T}\subset\mathcal{N}$ is a subset of total nodes, and $v(i)$ is characteristic function of node i in a single member coalition. Let x_i be the utility received by node i in coalition $\mathcal{T}$. A vector $\bar{x}=(x_1,...x_{|\mathcal{T}|})$ is rational utility allocation if $x_i\ge v(i)$ and $\sum_{i=1}^{|\mathcal{T}|} x_i = v(\mathcal{T})$.

Lemma 1. Given coalition C defined in subsection IV.D, the utility allocation of formula (5) is rational.

Proof. Given $n_i\in C$, its utility is

$$\begin{aligned} u_i &= s_i+\frac{P-\sum_{n_i\in C} s_i}{|C|}-r_i \\ &= s_i+\frac{\varepsilon\times b_0-\varepsilon\times\sum_{n_i\in C} s_i}{|C|}-r_i \end{aligned} \tag{6}$$

because $s_i-r_i\ge 0$ and the precondition of bargain succeeding is $b_0-\sum_{n_i\in C} s_i \geqslant 0$, we have $u_i\ge 0$. Since the utility of the single member coalition equals either 0 or $-r_i$, according to (6), we arrive at the lemma.

Note: if the utility of a member in C is changed from u_i to $u_i'=P/|C|-r_i$, then the utility allocation isn't rational because it isn't true that $P/|C|-r_i\ge 0$.

VI. Analysis of the Game

In this section, we study several types of games for cooperative authentication with complete and incomplete information.

A. Game with complete information

In the game with complete information, we assume that each node having common knowledge about the strategy spaces and the gains of all other nodes chooses a strategy simultaneously. This is a realistic assumption in the environment where nodes have a long-term cooperation.

Lemma 2. The All Cooperation strategy profile in *C-Coalition* is a pure-strategy Nash equilibrium for N-player game if the sum of the asking prices of all NNs is not greater than the bidding price of the source node. In other words, if $\sum_{n_i \in \mathcal{N}} s_i \leqslant b_0$, then $(CP_0, CP_1, ..., CP_N)$ is a pure-strategy Nash equilibrium, where $N = minCN$, $n_1 \ldots n_N$ are members of the chosen *C-Coalition* and CP_i $(0 \leq i \leq N)$ represents that the strategy of node i is CP.

Proof. If n_0 unilaterally deviates from cooperation to defect, then its utility is equal to 0, which is always smaller than $r_0 - P$ (Because $r_0 \geq b_0 > \varepsilon \times b_0 + (1-\varepsilon) \times \sum_{n_i \in \mathcal{N}} s_i = P$). Similarly, when n_i $(1 < i < N)$ cooperates, its utility is $u_i = s_i + \frac{P - \sum_{j \in N} s_j}{|N|} - r_i \geq 0$. When n_i defects, its utility $(1 < i < N)$ is not greater than 0, so no NN unilaterally deviates from cooperation to defect. Thus $(CP_0, CP_1, ..., CP_N)$ is a pure-strategy Nash equilibrium when $\sum_{n_i \in \mathcal{N}} s_i \leqslant b_0$.

Lemma 3. The All Defection strategy profile is a pure-strategy Nash equilibrium for an N-player game when the asking prices of any NNs is greater than the bidding price of the source node.

Proof. If n_i $(0 < i < N)$ unilaterally deviates from defection, then its utility is less than 0, which is always smaller than its utility when defecting.

Theorem 1. There is at least one pure-strategy Nash equilibrium for the N-player game when coalition C exists such that $\sum_{n_i \in C} s_i \leqslant b_0$ and $|C| \geq minCN$.

Proof. Given coalition C, we can always find a coalition C^*=$\arg\min_{C^j \subseteq C} |C^j|$, where C^j is coalition. As a result, CP is the best choice for node 0, that is, $s_0^* = CP$. Let $s_i^* = \begin{cases} CP \text{ if } n_i \in C^* \\ D \text{ else} \end{cases}$, where $1 < i < N$. In this case, $(s_0^*, s_1^*, \ldots, s_N^*)$ is a pure-strategy Nash equilibrium. The reasoning for this is as follows: should any $n_i \in C^*$ unilaterally deviates from cooperation and defects, its utility becomes 0, which is less than the utility when cooperating (because sum of their asking prices of nodes in C^* is less than the bidding price). Similarly, if any $n_i \notin C^*$ unilaterally moves from defect to cooperation, then its utility u_i changes from 0 to negative. Thus, no player unilaterally changes its strategy.

B. Game with incomplete information

In the game with complete information, we assume that all nodes know the reservation price of other nodes. In some cases, however, this is not true. For example, nodes participating in short-term cooperation might not know the reservation price of other nodes. Thus, an incomplete information assumption is more suitable for short-term cooperation.

In the incomplete information assumption, although nodes (including the source node and all NNs) do not know the asking/bidding price of other nodes, their probability density functions are the common knowledge of all nodes (Assuming for the purpose that "nature" provides all nodes this common knowledge[18]). In detail, buyer n_0 regards s_i and r_i as two random variables with probability density functions $f_{n_i}(.)$ and $g_{n_i}(.)$, respectively, where $1 < i \leq N$; Seller n_i also regards b_0 and r_0 as two random variables with probability density functions $f_{n_0}(.)$ and $g_{n_0}(.)$, respectively; $f_{n_i}(.)$ and $g_{n_i}(.)$ are also known by node j, where $1 < i < N$ and $j \neq i$.

With one node knowing only its own reservation price and having no knowledge of others' reservation price, it will be more invested in ask/bid a good price in order to maximize its own utility. As a result, the incomplete information assumption involves a node's utility being a function of its bidding/asking price.

Next, we discuss a special case where $minCN = N$ (that is, all NNs are required to participate in authentication). First, we discuss the buyer n_0's utility. Generally, n_0's utility is related to its own reservation price, and bidding price, the probability density function of its opponents' asking prices, which is defined as:

$$u_0(b_0) = (r_0 - (\varepsilon b_0 + (1-\varepsilon) Q_0) \Pr(b_0 \geqslant \sum_{i=1}^{N} s_i) \quad (7)$$

where $0 < \varepsilon < 1$, $\Pr(b_0 \geq \sum_{i=1}^{N} s_i)$ is the probability with which the bidding price b_0 of n_0 is not less than the sum of the asking prices of N NNs. $Q_0 \equiv E[\sum_{i=1}^{N} s_i | b_0 \geq \sum_{i=1}^{N} s_i]$ is the expected value of the sum of all asking prices under the condition that $b_0 \geq \sum_{i=1}^{N} s_i$. Let variable $B_{-0} = \sum_{i=1}^{N} s_i$, and its joint probability density function $f_{B_{-0}}(.)$ be obtained in terms of $s_1, \ldots, s_N$. After $f_{B_{-0}}(.)$ is obtained, we can show that

$$\Pr(b_0 \geq \sum_{i=1}^{N} s_i) = \int_{\sum_{i=1}^{N} r_i}^{b_0} f_{B_{-0}}(x)dx \quad (8)$$

$$Q_0 = \frac{\int_{\sum_{i=1}^{N} \underline{r_i}}^{b_0} x f_{B_{-0}}(x)dx}{\int_{\sum_{i=1}^{N} r_i}^{b_0} f_{B_{-0}}(x)dx} \quad (9)$$

Where r_i is the lower support of the distribution of asking prices. According to (8) and (9), n_0's utility function $u_0(b_0)$ can be rewritten as

$$u_0(b_0) = \int_{\sum_{i=1}^{N} r_i}^{b_0} (r_0 - \varepsilon b_0 - (1-\varepsilon)x) f_{B_{-0}}(x)dx \quad (10)$$

The first order condition for a maximum is

$$\frac{\mathrm{d}u_0}{\mathrm{d}b_0} = (r_0 - b_0) f_{B_{-0}}(b_0) - \varepsilon F_{B_{-0}}(b_0) = 0 \quad (11)$$

Where $F_{B_{-0}}(b_0) = \Pr(b_0 \geq \sum_{i=1}^{N} s_i) = \int_{\sum_{i=1}^{N} \underline{r_i}}^{b_0} f_{B_{-0}}(x)\mathrm{d}x$ is the cumulative distribution function of b_0.

Similarly, the utility of NN n_i $(1 \leq i \leq N)$ is related to its reservation/asking price, n_0's bidding price and other NNs' asking price. This is defined as:

$$u_i(s_i) = [s_i - r_i + \frac{E[Q_1|Q_3] - E[Q2|Q_3]}{N}] \Pr(Q_3) \quad (12)$$

where $Q_1 \equiv \varepsilon b_0 + (1 - \varepsilon) \sum_{j=1}^{N} s_j$ (13)

$$Q_2 \equiv \sum_{j=1}^{N} s_j \quad (14)$$

$$Q_3 \equiv s_i \leqslant (b_0 - \sum_{j=1, j\neq i}^{N} s_j) \quad (15)$$

$\Pr(Q_3)$ denotes the probability with which s_i is not less than $b_0 - \sum_{j=1,j\neq i}^{N} s_j$. $E[Q_1|Q_3]$ is the expected value of the agreeing price under the condition of Q_3, $E[Q_2|Q_3]$ denotes the expected value of the asking price under the condition of Q_3. In order to simplify (12), let variable $S_{-i} = b_0 - \sum_{j=1,j\neq i}^{N} s_j$ and its probability density functions be denoted as $f_{S_{-i}}(.)$ which can be obtained in term of $b_0, s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_N$.

According to (12)-(15), the utility function $u_i(s_i)$ of node i can be rewritten as

$$u_i(s_i) = \int_{s_i}^{\bar{b} - \sum_{j=1,j\neq i}^{N} r_j} (\frac{\varepsilon b_0 - \varepsilon \sum_{j=1}^{N} s_j}{N} - r_i) f_{S_{-i}}(x) \mathrm{d}x \quad (16)$$

Where $\bar{b}$ is the upper support of the distribution of bidding prices. The first order condition for a maximum is

$$\frac{\mathrm{d}u_i}{\mathrm{d}s_i} = (r_i - s_i) f_{S_{-i}}(s_i) - (1 - \varepsilon/N)(1 - F_{S_{-i}}(s_i) = 0 \quad (17)$$

Where $F_{S_{-i}}(s_i) = \Pr(s_i \leqslant (b_0 - \sum_{j=1,j\neq i}^{N} s_j))$ is the cumulative distribution function of s_i. Next, we discuss the pure-strategy Bayesian Nash equilibrium. Let random variable $R_{-i}^{s} = r_0 - \sum_{j=1,j\neq i}^{N} r_j$, $g_{S_{-i}}(.)$ and $G_{S_{-i}}(.)$ be its probability density function and cumulative distribution function, respectively. Let random variable $R_{-0}^{b} = \sum_{j=1}^{N} r_j$, $g_{B_{-0}}(.)$ and $G_{B_{-0}}(.)$ be its probability density function and cumulative distribution function, respectively. Assume that (1) every asking/bidding price relies on the reservation price, as formalized by $b_0 = Buy(r_0)$ and $s_i = Sell_i(r_i)$, where $Buy(.)$ and $Sell_i(.)$ are strict monotonically increasing functions, $1 < i < N$; (2) each offer strategy is bounded above and below and considered differentiable except possible at these bounds. Given the above assumptions, we have the following theorem.

Theorem 2. If a pure-strategy Bayesian Nash equilibrium exists, $Buy(.)$ and $Sell_i(.)$ $(1 < i < N)$ must satisfy the follow two equations

$$(Buy^{-1}(\sum_{i=1}^{N} Sell_i(y_i)) - \sum_{i=1}^{N} Sell_i(y_i)) \times g_{B_{-0}}(\sum_{i=1}^{N} y_i) \times \sum_{i=1}^{N} \frac{1}{Sell_j'(y_i)} = \varepsilon G_{B_{-0}}(\sum_{i=1}^{N} y_i) \quad (18)$$

$$(Sell^{-1}(Buy(x_0) - \sum_{j=1,j\neq i}^{N} Sell_j(x_j)) - Buy(x_0) + \sum_{j=1,j\neq i}^{N} Sell_j(x_j)) \times g_{S_{-i}}(x_0 - \sum_{j=1,j\neq i}^{N} x_j) \times (\frac{1}{Buy'(x_0)} - \sum_{j=1,j\neq i}^{N} \frac{1}{Sell_j'(x_j)}) = (1 - \varepsilon/N) G_{S_{-i}}(x_0 - \sum_{j=1,j\neq i}^{N} x_j) \quad (19)$$

Proof. Let $y_1, .., y_N$ be dummy variables such that $b_0 = \sum_{i=1}^{N} Sell_i(y_i)$, then $F_{B_{-0}}(b_0) = G_{B_{-0}}(\sum_{i=1}^{N} y_i)$. After noting that $f_{B_{-0}}(b_0) = g_{B_{-0}}(\sum_{i=1}^{N} y_i) \times \sum_{i=1}^{N} \frac{1}{Sell_j'(y_i)}$ and $r_0 = Buy^{-1}(b_0) = Buy^{-1}(\sum_{i=1}^{N} Sell_i(y_i))$, we can rewrite (11) to reach (18).

Similarly, let $x_0, .., x_{i-1}, x_{i+1}, .., x_N$ be N dummy variables such that $Buy(x_0) - \sum_{j=1,j\neq i}^{N} Sell_j(x_j) = s_i$, then $F_{Y_{-i}}(s_i) = G_{S_{-i}}(x_0 - \sum_{j=1,j\neq i}^{N} x_j)$. After noting that $f_{Y_{-i}}(s_i) = g_{S_{-i}}(x_0 - \sum_{j=1,j\neq i}^{N} x_j) \times (\frac{1}{Buy'(x_0)} - \sum_{j=1,j\neq i}^{N} \frac{1}{Sell_j'(x_j)})$, we can rewrite (17) to arrive at (19).

Theorem 2 shows that a node's optimal price relies not only on its own reservation price and its opponents' reservations, but also on the cumulative distribution function of reservation prices for itself and its opponents'.

Above, we discuss a special case ($minCN = N$). Next, we deal with a more general case where $minCN < N$. If $minCN < N$, several coalitions may be formed when NNs ask prices. Let $\mathcal{PC} = \{PC \in 2^{\mathcal{N}} || PC| \geq minCN\}$ be a set of pseudo-coalitions formed by NNs. The definition shows that the number of members in any pseudo-coalition is not less than $minCN$. We assume that PC in $\mathcal{PC}$ is probabilistically chosen by node 0 with probability $\Pr(X = PC)$, n_i 's $(0 < i < N)$ utility function can be calculated as:

$$u_0(b_0) = \sum_{PC\in\mathcal{PC}} ((r_0 - (\varepsilon b_0 + (1 - \varepsilon) Q_0) \times \Pr(b_0 \geqslant \sum_{n_i\in PC} s_i)) \times \Pr(X = PC)), \quad (20)$$

$$u_i(s_i) = \sum_{\mathrm{PC}\in\mathcal{PC}} (s_i - r_i + \frac{E[Q_1|Q_3] - E[Q2|Q_3]}{|PC|}) \Pr(Q_3) \Pr(X = PC), \quad (21)$$

where $Q_0 \equiv E[\sum_{n_i\in PC} s_i | b_0 \geq \sum_{n_i\in PC} s_i]$,

$Q_1 \equiv \varepsilon b_0 + (1 - \varepsilon) \sum_{n_j\in PC} s_j$, $Q_2 \equiv \sum_{n_j\in PC} s_j$,

$Q_3 \equiv s_i \leqslant (b_0 - \sum_{n_j\in PC, j\neq i} s_j)$

Assume that variable X on $\mathcal{PC}$ is a uniform distribution, we can rewrite (20) and (21) as

$$u_0(b_0) = \int_{\sum_{n_i \in PC} r_i}^{b_0} (r_0 - \varepsilon b_0 - (1 - \varepsilon)x) f_{B_{-0}}(x) dx \quad (22)$$

$$u_i(s_i) = \int_{s_i}^{\bar{b} - \sum_{n_j \in PC} r_j} \left(\frac{\varepsilon b_0 - \varepsilon \sum_{n_j \in PC} s_j}{N} - r_i \right) f_{S_{-i}}(x) \mathrm{d}x \quad (23)$$

The first order conditions for maximums of (22) and (23) are

$$\frac{\mathrm{d}u_0(b_0)}{\mathrm{d}b_0} = 0 \quad (24)$$

$$\frac{\mathrm{d}u_i(s_i)}{\mathrm{d}s_i} = 0 \quad (25)$$

If pure-strategy Bayesian Nash equilibriums can be obtained by solving the equations (24) and (25), similar to (11) and (17). Note: although PC is a pseudo-coalition, it becomes a true coalition, when $b_0 \geq \sum_{n_i \in PC} s_i$. We summarize our proposed game in Algorithm 1, as follows.

Algorithm 1. Game for cooperative authentication

1. Given message m requiring authentication: n_0 selects a proper AP and calculates the $minCN$ by (1); n_0 selects a proper weight w_{r_0}; Each n_i $(1 < i < N)$ selects two proper weight $w_{s_{i0}}$ and $w_{s_{i1}}$;
2. n_0 calculates m's length l_m and the required bandwidth $bandwidth_m$, its reservation price b_0 by (2); n_0 broadcasts l_m and $bandwidth_m$ to $\mathcal{N}$;
3. For each NN $n_i \in \mathcal{N}$
   - ✧ receives l_m and $bandwidth_m$;
   - ✧ collects the related parameter(E_i, PP_i, $Priv^i_{cons}$ and E^i_{cons}) and calculates its reservation price r_i by (3);
4. n_0 calculates its bidding price b_0 by (24); Each $n_i \in \mathcal{N}$ calculates its asking price s_i determined by (25);
5. n_0 submits b_0, and each $n_i \in \mathcal{N}$ submits r_i ;Let $\mathcal{C} = \{C \in 2^{\mathcal{N}} | \sum_{n_i \in C} s_i \leqslant b_0 \text{ and } |C| \geq minCN\}$. if $|\mathcal{C}| \geq 1$, a coalition C in $\arg\min_{C^j \in \mathcal{C}} |C^j|$ is chosen to participate in authentication;
6. After completing the authentication, the utility are allocated to nodes in the coalition C according to (5).

VII. Simulation Evaluation

In our simulation study, we follow the simulation setup in [4], and consider a network topology that consists of 1000 nodes with a transmission range R=15 randomly deployed in a $200m \times 200m$ area. Assume that AP is 98% and ρ=2%. Then according to (1), $minCN$ is correspondingly set to 6.

Due to limitations of space, we only simulate the game with complete information in this section. As shown in Figure 2, if all nodes are selfish (the situation is called selfness strategy), no authentication is successful[1]. In contrast, if all nodes are selfless (called selflessness scheme), then the first 1397 authentications are always successful. In our strategy, the first 4811 authentications are shown to succeed with a successful ratio of about 3.4 times than that of the selflessness scheme. This shows that our strategy is better than the selflessness strategy, which reasons are as follows: the unconditional cooperation of nodes wastes more resource, thus decreasing the lifetime of nodes. Different from the selflessness strategy, our strategy provides incentive for the appropriate number of nodes to take part in authentication, thus maximally saving the resources, decreasing the loss of privacy and ultimately increasing the probability of successful authentication. Note: following 1397 successful authentications in the selflessness scheme (and 4811 in our strategy), the rate of successful authentications rapidly decreases as available resources exhaust.

Figure 2. Probability of Successful Authentications (All Nodes)

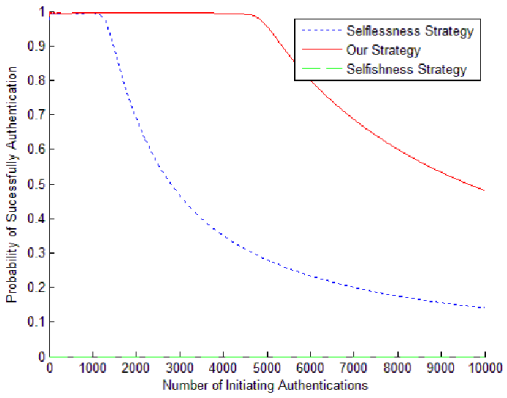
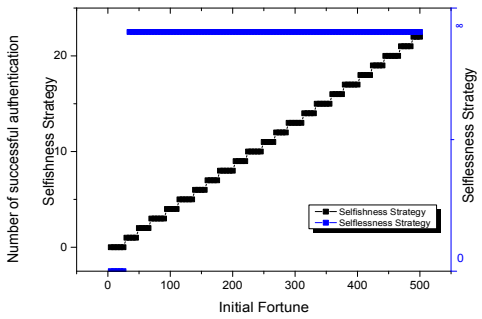


Figure 3. Number of Successful Authentications of Single Node in term of Initial Fortune



The above simulation deals with the cases in which all NNs are either selfish or selfless. Next, we simulate the special case in which one node is selfish while the others are selfless. In order to demonstrate that selfless nodes are dominant in our strategy, we assume an extreme situation that the resources owned by all nodes are infinite. Figure 3 shows the number of successful authentications in terms of initial fortune. The figures denotes that with the increase of initial fortune in the selfish scheme, the number of successful authentications also

[1] An authentication is successful if at least $minCN$ nodes participate in the cooperative authentication

increases, however, once the initial fortune has been given, the number of successful authentication is a smaller constant. That is, if a selfish node does not help to verify the messages of other nodes, even when it owns infinite resource, it cannot obtain enough virtual currency to purchase the authentication services. As a result, few NNs cooperatively authenticate messages of selfish nodes. However, for a selfless node with an initial fortune greater than 30, the number of its successful authentications becomes infinite. That is, NNs always help authenticate all messages of selfless nodes. Thus, if our scheme is adopted, any rational node becomes selfless.

VIII. CONCLUSION

We have considered the problem using incentive to obtain the participation of the appropriate number of nodes in cooperative authentication. A bargaining-based game for cooperative authentication is proposed to guarantee that mobile nodes participating in the cooperative authentication maximize their location privacy while minimizing their resource consumption. We have considered two games: complete information game and incomplete information game. In the complete information game, Nash equilibrium is obtained. Addressing the problem that nodes do not know others' utility, we have established incomplete information games. We also have developed an algorithm based on incomplete information games to maximize utility of every node. The simulation demonstrates the efficiency of our strategy. In future work, more novel game models (e.g. dynamical game) should be considered to further improve the efficiency.

ACKNOWLEDGEMENTS:

The authors would like to thank CHEN Xiuzhen for her insightful discussions on the earlier versions of the framework and for her valuable comments on the submitted manuscript. This work was supported by the National High Technology Research and Development Program of China (2013AA014002) and the National Natural Science Foundation of China (61070186, 61100181, 61100186, 61262008, 61063002).

REFERENCES

[1].H. Moustafa and G. Bourdon. Authentication and services access control in a cooperative ad hoc environment. International Conference on Broadband Communications, Networks and Systems. 2008: 32-39.

[2].Y. Hao, Y. Cheng, C. Zhou and W. Song. A distributed key management framework with cooperative message authentication in VANETs. IEEE Journal on Selected Areas in Communications, 2011. 29(3): 616-629.

[3].Y. Hao, T. Han and Y. Cheng. A cooperative message authentication protocol in VANETs. Global Communications Conference (GLOBECOM). 2012: 5562-5566.

[4].R. Lu, X. Lin, H. Zhu, X. Liang and X. Shen. Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 2012. 23(1): 32-43.

[5].X. Lin and X. Li. Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology, 2013.62(7): 3339-3348.

[6].R. Ramamoorthy, F.R. Yu, H. Tang, P. Mason and A. Boukerche. Joint authentication and quality of service provisioning in cooperative communication networks. Computer Communications, 2012. 35(5): 597-607.

[7].J. Reagle and L.F. Cranor. The platform for privacy preferences. Communications of the ACM, 1999. 42(2): 48-55.

[8].K. Vu, R. Zheng and J. Gao. Efficient algorithms for K-anonymous location privacy in participatory sensing. IEEE INFOCOM. 2012: 2399-2407.

[9].X. Liu, H. Zhao, M. Pan, H. Yue, X. Li and Y. Fang. Traffic-aware multiple mix zone placement for protecting location privacy. IEEE INFOCOM. 2012: 972-980.

[10].J. Freudiger, M. Manshaei, J. Hubaux and D. Parkes. Non-Cooperative Location Privacy. IEEE Transactions on Dependable and Secure Computing, 2013. 10(2): 84-98.

[11].C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati and P. Samarati. An obfuscation-based approach for protecting location privacy. IEEE Transactions on Dependable and Secure Computing, 2011. 8(1): 13-27.

[12].D. Zhang, R. Shinkuma and N.B. Mandayam. Bandwidth exchange: an energy conserving incentive mechanism for cooperation. IEEE Transactions on Wireless Communications, 2010. 9(6): 2055-2065.

[13].C. Zhang, X. Zhu, Y. Song and Y. Fang. C4: A new paradigm for providing incentives in multi-hop wireless networks. IEEE INFOCOM. 2011: 918-926.

[14].M. Guizani, A. Rachedi and C. Gueguen. Incentive Scheduler Algorithm for Cooperation and Coverage Extension in Wireless Networks. IEEE Transaction on Vehicular Technology 2013. 62(2): 797-808.

[15].M.T. Refaei, L.A. DaSilva, M. Eltoweissy and T. Nadeem. Adaptation of reputation management systems to dynamic network conditions in ad hoc networks. IEEE Transactions on Computers, 2010. 59(5): 707-719.

[16].Z. Li and H. Shen. A hierarchical account-aided reputation management system for large-scale manets. IEEE INFOCOM. 2011: 909-917.

[17].Z. Li and H. Shen. Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. IEEE Transactions on Mobile Computing, 2012. 11(8): 1287-1303.

[18].M. Manshaei, Q. Zhu, T. Alpcan, T. Basar and J.-P. Hubaux. Game theory meets network security and privacy. ACM transaction on Computational Logic, 2011. 5.

[19].T. Chen, L. Zhu, F. Wu and S. Zhong. Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach. IEEE Transactions on Vehicular Technology, 2011. 60(2): 566-579.

[20].R. Shokri, G. Theodorakopoulos, J. Le Boudec and J. Hubaux. Quantifying location privacy. IEEE Symposium on Security and Privacy (SP). 2011: 247-262.

[21].Y. LI, J. YU and X. YOU. An Incentive Protocol for Opportunistic Networks with Resources Constraint. Journal of Computer, 2013. 36(5): 947-956.