Modeling Cooperative, Selfish and Malicious Behaviors for Trajectory Privacy Preservation Using Bayesian Game Theory

Xinyu Jin[1], Niki Pissinou[2], Sitthapon Pumpichet[1], Charles A Kamhoua[3] and Kevin Kwiat[3]

[1]Dept. of ECE, Florida International University, {FirstName.LastName}@fiu.edu
[2]School of CIS, Florida International Univserity, pissinou@fiu.edu
[3]Air Force Research Lab, Information Directorate Cyber Assurance Branch, {FirstName.LastName}@rl.af.mil

***Abstract*—As new mobile Wireless Sensor Networks (mWSNs) for location-aware applications are emerging, trajectory privacy invasion is becoming an indispensable issue. Many promising techniques are under development. Considering the decentralized network architecture, most of Trajectory Privacy Preservation (TPP) techniques rely on the cooperation from peer nodes, cluster headers, or a third party. However, only a few works have addressed the issue of selfish behaviors in such cooperation required techniques. Nevertheless, the problem of facing selfish and compromised nodes in the noncooperative and hostile environment is rarely touched.**

In this paper, we apply Bayesian game theory to model cooperative, selfish and malicious behaviors of autonomous mobile nodes in decentralized mWSNs. We formulate and analyze the TPP game among peer nodes in both strategic and dynamic forms. The equilibrium strategies for users to evaluate the degree of trust in participating in in-network TPP activities are provided and analyzed in theoretical and simulation results.

I. Introduction

In recent years, there has been an explosive growth of location-aware sensing devices. The age of combining sensing, processing and communication in one device, gives rise to a vast number of applications leading to endless possibilities and a realization of mobile Wireless Sensor Network (mWSNs) applications. As computing, sensing and communication become more ubiquitous, trajectory becomes a critical piece of information and an important factor for secure and private communications.

While some researchers have addressed issues related to Trajectory Privacy Preservation (TPP) in sensor networks (readers may refer to [1], [2] for a brief survey), the autonomy of sensor nodes in decentralized/distributed networks has been generally overlooked. Many sensor network applications consist of temporary, on the fly connections among typically autonomous sensing devices where each device decides whether and to what extent it wishes to participate in the network. In pursuit of their own interests, participating devices could therefore misbehave-either by being selfish or by being malicious.

This project is partially supported by the National Science Foundation and U.S. Department of Homeland Security.

Approved for Public Release; Distribution Unlimited: 88ABW-2013-0750, 14-Feb 2013.

A. Motivating Applications

Let's examine the following scenarios: a cardiopath patient carries a wearable sensor for monitoring her heart rate. This sensor sends measurements back to the hospital periodically for the doctor to evaluate her health condition and respond with corresponding diagnoses. In an emergency, the sensor sends an alarm to the doctor for first aid assistance. In this case, the doctor can locate the patient immediately based on the sensors trajectory information. However, besides these positive usages, invasion by unauthorized or malicious entities into the private trajectory of a user, such as when and where she shops, when and where she spends vacations, may seriously threaten personal safety. Therefore, the user would like to be "invisible" in privacy sensitive areas and opt out any TPP interactions with other nodes in uncertain situations.

Trajectory information can reveal personal preferences and habits, which can be used for consumer profiling. While some sensors are embedded into vehicles for sensing traffic and road conditions for better traffic management avoiding traffic congestion, insurance companies can utilize trajectory information to analyze frequent routes of clients. They might charge higher premiums from the clients that often visit high accident locations. In this case, clients would rather stay "quiet" and not cooperate with other vehicles or the base station in such locations.

The aforementioned scenarios necessitate the decentralized control of the network in which sensor nodes make autonomous decisions regarding their network usage and preserving their trajectory privacy, based on their individual needs.

B. Related Work

We have previously proposed a privacy-aware routing protocol to hide source's trajectories in the presence of eavesdropping attacks [3]. It can effectively mislead the adversary by masking the exact location where a particular packet started its journey. This algorithm works relying on the cooperation among sensor nodes. In decentralized mWSNs where nodes

978-1-4799-0537-9/13/$31.00 ©2013 IEEE

are autonomous entities, the cooperation among nodes is not guaranteed. Furthermore, the internal attack is of great importance to be considered into TPP in mWSNs due to the risk of node compromise. In fact, any protocols or techniques involving cooperation among autonomous nodes need to have the mechanism to consider trust among nodes. In the context of TPP, it is even more challenging to balance between resource sharing for cooperation and privacy protection.

Game theory is an important tool to model behaviors and strategies of interacting entities. It has been applied to study the TPP related issues recently. Shokri et al. used Stackelberg Bayesian game to formalize the mutual optimization of user-adversary objectives [4]. They aimed to enable the system administrator to find the optimal mechanism for trajectory privacy preservation. Humbert et al. studied the problem of designing mix zones in the presence of local eavesdroppers [5]. The work proposed in [6], [7] mainly focused on the incentive designs to provide the required trajectory privacy level for individual users as well as the desired granularity for service providers/mobile commerce companies. The above works attempted to address the optimal strategies for two competing entities, user-adversary or user-service provider. A few other works have been proposed to study the interactions between peer nodes. Researchers used game theory to model the cooperation behaviors while taking the selfishness of autonomous nodes into consideration in the noncooperative network environment [2], [8], [9]. In such networks, each node aims to maximize its own payoff while determining whether it cooperates TPP activities to gain (or assist other nodes to gain) trajectory privacy. To study the malice of compromised nodes, researchers have presented comprehensive analysis in intrusion detection games in mobile networks [10], [11]. These previous works are of great inspiration in discussing the degree of trust in cooperation among peer nodes. However, solely considering selfishness or malice is insufficient for vulnerable networks composed of autonomous nodes.

C. Paper Summary and the Outline

In this paper, we formulate in-network TPP activities by applying the Bayesian game, named the *TPP* game, to model the cooperation and trust behaviors of autonomous nodes with taking both selfishness and malice of sensor nodes into account in decentralized/distributed mWSNs. The selfishness is modeled by deploying trajectory privacy sensitivity customization. We analyze the TPP game from static and dynamic point of view and provide the suggested equilibrium strategy for nodes to trust neighbors to preserve their trajectory privacy.

The rest of the paper is organized as follows. An introduction to our TPP game model is provided in section II, followed by the analysis details and simulation results in section III, IV and V. Finally, we conclude this work in section VI.

II. Trajectory Privacy Preservation Game Preliminaries

We aim to investigate the game theoretic approach to model and analyze the cooperative, selfish and malicious behaviors of autonomous nodes in TPP activities. Therefore, nodes seeking TPP cooperations can evaluate the degree of trust and tolerate node compromise attacks in mWSNs.

A. System and Attack Models

The system we consider is composed of mobile sensor nodes and one or more base stations/sinks. Nodes are aware of their locations and transmit sensing data (and spatio-temporal data by needs) through one-hop or multi-hop communications with the sink and other peer nodes. Access points/gateways, where data are collected and primarily processed (e. g. basic data cleaning and reduction) before they are forwarded to the sink, are not restricted in the system. We assume access points (if they exist) and sinks have adequate transmission and computing capabilities or necessary hardware units to counter security and privacy attacks. Additionally, cryptographic techniques are deployed to secure data transmissions.

The adversary is capable of launching an eavesdropping attack. Although proper cryptographic techniques can prevent such attacks from breaching nodes' data privacy, they are vulnerable when the adversary has certain background knowledge of the target. Additionally, the adversary can compromise nodes in the network and launch internal attacks. For instance, compromised nodes are used to track the target or reveal its trajectories to eavesdroppers or other compromised nodes. This attack model is set up on top of the attack model in [3]. We have solely addressed eavesdropping attacks in the previous work. However, when node compromise attack is considered among autonomous sensor nodes, the noncooperative and malicious nodes behaviors must be studied to cope with the noncooperative network environment, which is our focus in this work.

B. Sensitivity Customization

The trajectory privacy sensitivity (noted as sensitivity through this paper) represents the privacy requirement levels of a node in the specific area at particular time. Sensitivity is determined by two trajectory contexts, spatial and temporal information.

The network area is divided into small subareas. We categorize subareas into two types: open areas (OAs) and sensitive areas (SAs) according to the sensitivity required by a node in different subareas. When the node is traveling in its OAs, trajectories are relatively open to other network entities and there is no additional protections besides security techniques. On the other hand, when the node is traveling in its SAs, trajectories need to be highly protected from untrustworthy or compromised nodes. For example, OAs can be users' working places since such information is easy to obtain from public resources in most cases. SAs can be the restaurants or hospitals that users occasionally visit. The above customization only involves spatial information which is insufficient in practice. For example, if a user goes to the office after working hours, he/she may want to keep such information as privacy which makes that office a SA. Therefore, the sensitivity of an area needs to be assigned along with the specific time span.

Sensitivity is a customized TPP parameter regarding individual nodes. In an autonomous network, before nodes join/rejoin the network or while on the move, users can determine the sensitivity and make the selection on OAs and SAs that comply with a certain trajectory privacy level θ. θ is defined as the ratio of the traveling time in SAs over the overall traveling time of each node. The overall traveling time is the life time or a refreshing period of a node. Individual nodes can have different θ values. However, there is a maximum requirement defined by the network administrator, denoted as Θ. For example, node i's trajectory privacy level $\theta_i \leq \Theta$. From the individual user's point of view, greater θ value indicates higher trajectory privacy. From the network's point of view, the user's trajectory privacy level needs to be limited to Θ since nodes in SAs prioritize their trajectory privacy and may prefer hiding from any other node rather than cooperating in TPP activities. It is worth noting that the trajectory privacy level θ of a node does not involve any private trajectory information. Therefore, neighboring nodes can easily retrieve this information through queries to peers.

III. Trajectory Privacy Preservation Game

The TPP game is conducted between two neighboring nodes, node i and node j, in the network. Node i is in SAs and needs cooperation from node j in preserving i's trajectory privacy during data transmissions. However, node i does not know if node j will cooperate, defect, or even attack (node j may be a compromised node) due to the unknown type of node j. We use a Bayesian game formulation to model the interactions between two nodes in TPP activities. The set of players is $\mathcal{N} = \{i, j\}$. i has one type which is a regular node in SAs. That means $t_i \in \mathcal{T}_i = \{S\}$. i can choose whether to trust j in cooperating in TPP activities. Actions available to i are $a_i \in \mathcal{A}_i$ ={*Trust, Not Trust*}. j has three types which are regular nodes in OAs, denoted as Open nodes; regular nodes in SAs, denoted as Selfish nodes, and Malicious nodes. That means $t_j \in \mathcal{T}_j = \{O, S, M\}$. We differentiate selfish nodes from open nodes to remark that nodes in SAs prioritize their trajectory privacy. Actions available to j are $a_j \in \mathcal{A}_j$ ={*Cooperate, Defect, Attack*}. Open nodes and selfish nodes can play either *Cooperate* or *Defect*, while malicious can choose to play *Cooperate*, *Defect*, or *Attack*.

The payoff matrices of the game is presented in table I. G_r denotes the cooperation payoff of j (e.g. cooperative credit gain) when it cooperates in TPP. C_p is the participation cost. G_p is the trajectory privacy gain of i when j cooperates.G_θ is the trajectory privacy leakage of j when $t_j = S$ and j cooperates. C_A is the cost of a malicious node to $Attack$. We also denote β as the attack success rate. Except that the type of j is uncertain to i, other information is known to each player and both players know this fact.

Due to the high priority of trajectory privacy of selfish nodes, we restrict that $G_\theta > G_r$. Additionally, we focus on discussing TPP issues in this project. Therefore, we assume that G_p is relatively far greater than other payoff elements.C_p and C_A are comparable and relatively less than other payoff elements. In the next section, we present the equilibrium analysis of the TPP game.

TABLE I
Payoff matrix of the TPP game

	i	
j	Trust	Not Trust
Cooperate	$G_r - C_p, G_p - C_p$	$G_r, 0$
Defect	$0, -C_p$	$0, 0$

(a) node j is open, $t_j = O$

	i	
j	Trust	Not Trust
Cooperate	$G_r - C_p - G_\theta, G_p - C_p$	$G_r - G_\theta, 0$
Defect	$0, -C_p$	$0, 0$

(b) node j is selfish, $t_j = S$

	i	
j	Trust	Not Trust
Cooperate	$G_r - C_p, G_p - C_p$	$G_r, 0$
Defect	$0, -C_p$	$0, 0$
Attack	$G_p - C_A, -G_p - C_p$	$-C_A, 0$

(c) node j is malicious, $t_j = M$

A. Equilibrium Analysis in the Strategic Form

We begin the equilibrium analysis with considering this TPP game as a static Bayesian game. We assumed that both players are rational. Their objectives are to maximize their own expected payoffs. Bayesian Nash Equilibria (BNE) specify actions or randomized strategies of each type of player, which would be maximizing the expected payoffs for each player in the strategic form [12]. Therefore, our equilibrium analysis here is to find existing BNE. In the TPP game, the type of i is certain to both players and i is uncertain about j's type. i has the initial belief about j's type, which is the probability distribution over all possible types of j. j is malicious with the probability of $(1 - P)$, selfish with the probability of $P\theta_j$ and open with the probability of $P(1 - \theta_j)$.

From the payoff matrices of the game, it is not difficult to eliminate some strategies from possible BNE by dominance. *Defect* is dominated for $t_j = O$ and $t_j = M$. *Cooperate* is dominated for $t_j = S$. Therefore, j has two possible pure-strategy BNE: $\sigma_j \in \{$(*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Cooperate* if $t_j = M$), (*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Cooperate* if $t_j = M$)$\}$.

- Case 1: $\sigma_j =$ (*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Cooperate* if $t_j = M$).
  In this case, the expected payoff of i if $\sigma_i =$ *Trust* is

$$\begin{aligned}\mathscr{U}_i(T) &= (G_p - C_p)P(1 - \theta_j) + (G_p - C_p)(1 - P) \\ &\quad +(-C_p)P\theta_j. \end{aligned} \tag{1}$$

  $(G_p - C_p)P(1 - \theta_j) + (G_p - C_p)(1 - P)$ is the payoff of obtaining cooperation from j to gain trajectory privacy.

$(-C_p)P\theta_j$ is the payoff when j is selfish and defects. The expected payoff of i if $\sigma_i =$ *Not Trust* is

$$\mathscr{U}_i(NT) = 0. \quad (2)$$

Therefore, if (1) > (2), i. e. $P < \frac{G_p - C_p}{G_p \theta_j}$, the best response for i is always *Trust*. In this case, if $t_j = M$, j will deviate from *Cooperate* to *Attack* since j will breach i's privacy and get higher expected payoffs. Thus, there is no pure-strategy BNE when $P < \frac{G_p - C_p}{G_p \theta_j}$. If (1) < (2), i. e. $P > \frac{G_p - C_p}{G_p \theta_j}$, the best response for i is always *Not Trust*. Correspondingly, j's best response is *Cooperate* if $t_j = M$. Hence, $(\sigma_j, \sigma_i) = \{$(*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Cooperate* if $t_j = M$), *Not trust*$\}$ is a possible pure-strategy BNE if $P > \frac{G_p - C_p}{G_p \theta_j}$.

- Case 2: $\sigma_j =$ (*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Attack* if $t_j = M$).
  In this case, the expected payoff of i if $\sigma_i =$ *Trust* is

$$\begin{aligned}\mathscr{U}_i(T) &= (G_p - C_p)P(1-\theta_j) + (-C_p)P\theta_j \\ &\quad +(-G_p - C_p)(1-P)\beta \\ &\quad +(-C_p)(1-P)(1-\beta). \end{aligned} \quad (3)$$

  $(-G_p - C_p)(1-P)\beta$ is the payoff of being successfully attacked by j. $(-C_p)(1-P)(1-\beta)$ is the payoff when j fails in attacking. The expected payoff of i if $\sigma_i =$*Not Trust* is

$$\mathscr{U}_i(NT) = 0. \quad (4)$$

  So if (3) < (4), i. e. $P < \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}$, the best response for i is always *Not Trust*. In this case, if $t_j = M$, j will deviate from *Attack* to *Cooperate* to get higher expected payoffs. Thus, there is no pure-strategy BNE when $P < \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}$. If (3) > (4), i. e. $P > \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}$, the best response for i is always *Trust*. Correspondingly, j's best response is *Attack* if $t_j = M$. Hence $(\sigma_j, \sigma_i) = \{$(*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Attack* if $t_j = M$), *Trust*$\}$ is a possible pure-strategy BNE if $P > \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}$.

Now we further analyze the conditions under which the pure-strategy BNE exists. Given $0 < P < 1$ and $0 < \theta_j < 1$, the condition that $P > \frac{G_p - C_p}{G_p \theta_j}$ can establish is $1 - \frac{C_p}{G_p} < \theta_j < 1$. On the other hand, the condition that $P > \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}$ can establish is $0 < \theta_j < 1 - \frac{C_p}{G_p}$. θ_j is retrieved by j through sending queries to i if there is no previous local records.

From the above analysis, we can finally summarize the existence of pure-strategy BNE: the TPP game has one pure-strategy BNE when P is greater than a certain value $P_0 \in \{\frac{G_p - C_p}{G_p \theta_j}, \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}\}$. That is to say if $1 - \frac{C_p}{G_p} < \theta_j < 1$, there exists a pure-strategy BNE $(\sigma_j, \sigma_i) = \{$(*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Cooperate* if $t_j = M$), *Not trust*$\}$ when $P > \frac{G_p - C_p}{G_p \theta_j}$; if $0 < \theta_j < 1 - \frac{C_p}{G_p}$, there exists a pure-strategy BNE $(\sigma_j, \sigma_i) = \{$(*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Attack* if $t_j = M$), *Trust*$\}$ when $P > \frac{G_p\beta + C_p}{G_p(1-\theta_j) + G_p\beta}$. This conclusion verifies that in order to have stable status that encourages cooperation among nodes in TPP activities, θ_j needs to be restricted to an upper bound of Θ.

We have analyzed the pure-strategy BNE of the TPP game. However, under pure strategies, i either cannot gain trajectory privacy by trusting other nodes or can frequently be attacked by malicious nodes where high expected payoffs encourage malicious nodes to attack. Therefore, we need to find the mixed-strategy BNE of the TPP game. Such BNE exists when $P < P_0$. Let ϕ be the probability of $\sigma_i =$ *Trust*. Let ψ be the probability of $\sigma_j =$ *Attack* when $t_j = M$. The mixed-strategy BNE is derived as follows. The expected payoffs of i when $\sigma_i =$ *Trust* and when $\sigma_i =$ *Not Trust* are respectively:

$$\begin{aligned}\mathscr{U}_i(T) &= (G_p - C_p)P(1-\theta_j) + (-C_p)P\theta_j \\ &\quad +(1-\psi)(G_p - C_p)(1-P) \\ &\quad +\psi(1-P)((-G_p - C_p)\beta \\ &\quad +(-C_p)(1-\beta)). \end{aligned} \quad (5)$$

$$\mathscr{U}_i(NT) = 0. \quad (6)$$

The expected payoffs of j when $\sigma_j =$ *Cooperate* and when $\sigma_j =$ *Attack* are respectively:

$$\mathscr{U}_j(C) = (G_r - C_p)\phi + G_r(1-\phi). \quad (7)$$

$$\begin{aligned}\mathscr{U}_j(A) &= (G_p - C_A)\phi\beta + (-C_A)\phi(1-\beta) \\ &\quad +(-C_A)(1-\phi). \end{aligned} \quad (8)$$

To derive a mixed-strategy BNE, j's attacking rate needs to satisfy $\mathscr{U}_i(T) = \mathscr{U}_i(NT)$ if $t_j = M$. Thus, j's equilibrium strategy is to attack with probability $\psi^* = \frac{G_p(1-P\theta_j) - C_p}{G_p(1-P)(1+\beta)}$. Similarly, i's equilibrium strategy is to trust with probability $\phi^* = \frac{G_r + C_A}{G_p\beta + C_p}$. Therefore, the static TPP game has a mixed-strategy BNE when $(\sigma_j, \sigma_i) = \{$(*Cooperate* if $t_j = O$, *Defect* if $t_j = S$, *Attack* with probability ψ^* if $t_j = M$), *Trust* with probability $\phi^*\}$.

IV. Dynamic TPP Game and Perfect Bayesian Equilibrium

Thus far, we have analyzed the TPP game which is viewed as a one-stage game. The challenge of applying such a game model is assigning i a proper initial belief of j's type. In mWSNs, nodes are highly distributed. Relying on the centralized administrator to provide the regular nodes' rate P is costly. Therefore, i needs to dynamically update its belief of j's type in a distributed manner in the multi-stage TPP game.

A. Belief System

We consider a dynamic Bayesian game which is a repeated one-stage TPP game with no discount factor to model the multi-stage TPP game. The game is infinite since players cannot predict when neighboring nodes leave the network. The static TPP game is repeated in each time slot. We continue to use notations in the static TPP game with minor revisions. $a_j(t)$ denotes j's action at stage t. $\tilde{a}_j(t)$ denotes i's observation of j's action. i observes j's actions with the observation rate α_t, the action false active rate γ_t and the attack false alarm rate β_t. Additionally, let $\mu_i(t_j | h_j^t)$ be i's belief of j, where h_j^t is the action history profile j at the

beginning of stage t, i. e. $h_j^t = (a_j(0), a_j(1), ..., a_j(t-1))$. Given j's action history profile h_j^t and type t_j, $P(a_j(t)|t_i, h_j^t)$ is the probability that $a_j(t)$ is observed at stage t. Based on Bayes' rule, i's posterior belief of j is calculated by:

$$\mu_i(t_j|(h_j^t, \tilde{a}_j(t))) = \frac{\mu(t_j|(h_j^t))P(\tilde{a}_j(t)|h_j^t, t_j)}{\sum_{\tilde{t}_j \in \mathcal{T}_j} \mu_i(\tilde{t}_j|h_j^t)P(\tilde{a}_j(t)|h_j^t, \tilde{t}_j)}. \quad (9)$$

where $\mu_i(\tilde{t}_j|h_j^t) > 0$.

In our game model, with an altering of notation, we have:

$$\begin{aligned}
P(\tilde{a}_j(t) = Cooperate|t_j = O) &= \alpha_t(1-\beta_t) \\
P(\tilde{a}_j(t) = Defect|t_j = O) &= 1-\alpha_t \\
P(\tilde{a}_j(t) = Attack|t_j = O) &= \alpha_t\beta_t \\
P(\tilde{a}_j(t) = Cooperate|t_j = S) &= \gamma_t(1-\beta_t) \\
P(\tilde{a}_j(t) = Defect|t_j = S) &= 1-\gamma_t \\
P(\tilde{a}_j(t) = Attack|t_j = S) &= \gamma_t\beta_t \\
P(\tilde{a}_j(t) = Cooperate|t_j = M) &= \alpha_t(1-\beta_t)(1-\psi) \\
P(\tilde{a}_j(t) = Defect|t_j = M) &= 1-\alpha_t \\
P(\tilde{a}_j(t) = Attack|t_j = M) &= \alpha_t(\psi + (1-\psi)\beta_t).
\end{aligned} \quad (10)$$

Formulae (9) and (10) form the belief system [13] for i to update its belief of j in each stage of the game as the game is played sequentially. With both this belief system and the initial belief that i holds, i is able to compute its updated belief. It might be confusing that the action history has been omitted in Formula (9). In fact, the observed actions contribute to the belief update in each stage during the game sequentially. It is worth noting that in applications requiring high trajectory privacy levels, i can apply the Grim Trigger strategy once an attack is observed. However, keeping the dynamic updated belief on all types of nodes for further possible cooperation is plausible in sparse networks. Details of how to apply the Grim Trigger strategy are beyond the scope of this paper and will be presented in our extension work.

B. Perfect Bayesian Equilibrium (PBE)

We have found BNE of the static TPP game in previous sections. However, when the game involves sequential multiple stages, Nash Equilibrium needs to be strengthened with the notion of subgame perfection. The relevant notion of equilibrium will be PBE. PBE requires each player's strategy to specify optimal actions, given the player's beliefs and the strategies of all other players, and the beliefs are consistent with Bayes' Rule whenever it is applicable. It specifies a feasible strategy profile for players to optimize the expected payoffs in the multi-stage game. We now show that there exist PBE in the dynamic TPP game.

We first prove that the proposed dynamic TPP game satisfies the Bayesian condition B(i)-B(iv) and P [14]. Then we determine the PBE in such games.

Lemma 4.1: The proposed dynamic TPP game satisfies Bayesian conditions B(i)-B(iv) and P:

B(i): Posterior beliefs are independent, and all types of player i have the same beliefs.

B(ii): Baye's rule is used to update beliefs whenever possible.

B(iii): Players do not signal what they do not know.

B(iv): Posterior beliefs are consistent for all nodes with a common joint distribution on the type of another player given h^t.

P: For each player i, type t_i, player i's alternative strategy σ_i' and history h^t,

$$\mathscr{U}_i(\sigma|h^t, t_i, \mu(\cdot\,|h^t)) \geq \mathscr{U}_i((\sigma_i', \sigma_{-i})|h^t, t_i, \mu(\cdot\,|h^t)). \quad (11)$$

Proof: B(i) is satisfied because i only has one type. The proposed belief update system was derived according to Baye's rule. Thus, B(ii) is satisfied. B(iii) is satisfied because j's signal is j's action which is observed by i, and B(iv) is satisfied since this is a two-player game.

According to the rationality of the players, given i's updated belief of j, $\mu_i(t_j|h_j^t)$, and h_j^t, i's optimal behavior strategy σ_i^* is to maximize his expected payoff based on i's belief. Therefore, σ_i^* satisfies:

$$\begin{aligned}
&\mathscr{U}_i(\sigma_j, \sigma_i^*)|h_j^t, t_i, \mu_i(t_j|(h_j^t, a_j(t))) \\
&\geq \mathscr{U}_i((\sigma_j, \sigma_i'|h_j^t, t_i, \mu_i(t_j|(h_j^t, a_j(t))).
\end{aligned} \quad (12)$$

Similarly, j's optimal behavior strategy σ_j^* satisfies:

$$\begin{aligned}
&\mathscr{U}_j(\sigma_j^*, \sigma_i)|h_i^t, t_j, \mu_j(t_i|(h_i^t, a_i(t))) \\
&\geq \mathscr{U}_j((\sigma_j', \sigma_i|h_i^t, t_j, \mu_j(t_i|(h_i^t, a_i(t))).
\end{aligned} \quad (13)$$

σ' denotes the alternative strategy of the player. In this two-player game, Formulae (12) and (13) show the sequential rationality of each player, which satisfies P. ■

In this paragraph, we derive the PBE of the dynamic TPP game. At stage t, recall ϕ denotes the probability of $\sigma_i =$ *Trust* and ψ denotes the probability of $\sigma_j =$ *Attack* when $t_j = M$.

$$\begin{aligned}
\mathscr{U}_i(a_i(t) = T) &= (G_p - C_p)\mu_i(t_j = O|h_j^t) \\
&\quad +(-C_p)\mu_i(t_j = S|h_j^t) \\
&\quad +(1-\psi)(G_p - C_p)\mu_i(t_j = M|h_j^t) \\
&\quad +\psi(\mu_i(t_j = M|h_j^t)((-G_p - C_p)\beta \\
&\quad +(-C_p)(1-\beta)). \quad (14) \\
\mathscr{U}_i(a_i(t) = NT) &= 0. \quad (15) \\
\mathscr{U}_j(a_j(t) = C) &= (G_r - C_p)\phi + G_r(1-\phi). \quad (16) \\
\mathscr{U}_j(a_j(t) = A) &= (G_p - C_A)\phi\beta + (-C_A)\phi(1-\beta) \\
&\quad +(-C_A)(1-\phi). \quad (17)
\end{aligned}$$

This mixed-strategy equilibrium needs to satisfy the condition that different strategies cannot be differentiated by each player from the expected payoffs. Therefore, we derive the PBE pair based on the equivalence of Formulae (14) and (15), and the equivalence of Formulae (16) and (17). Thus, we have:

$$\begin{aligned}
\psi_t^* &= \frac{G_p(1-(1-\mu_i(t_j = M|h_j^t))\theta_j) - C_p}{G_p\mu_i(t_j = M|h_j^t)(1+\beta)} \\
\phi_t^* &= \frac{G_r + C_A}{G_p\beta + C_p}.
\end{aligned} \quad (18)$$

We now discuss the existence of pure-strategy PBE. In the case that $(14) > (15)$, i always plays *Trust* and

j always plays *Attack*. In this case ψ_t^* satisfies $\psi_t^* < \frac{G_p(1-(1-\mu_i(t_j=M|h_j^t))\theta_j)-C_p}{G_p\mu_i(t_j=M|h_j^t)(1+\beta)}$ and $\psi_t^* = 1$. The condition for such a case to exist is that $\mu_i(t_j = M|h_j^t) < \frac{G_p(1-\theta_j)-C_p}{G_p(1+\beta-\theta_j)}$ and $\theta_j < 1 - \frac{C_p}{G_p}$. Similarly, the pure-strategy pair of i always plays *Not Trust* and malicious j always plays *Cooperate* exists under the condition that $\mu_i(t_j = M|h_j^t) < \frac{G_p(\theta_j-1)+C_p}{G_p\theta_j}$ and $\theta_j > 1 - \frac{C_p}{G_p}$, which does not hold in this TPP game model. Therefore, there exists one pure-strategy PBE pair $(\psi_t^* = 1, \phi_t^* = 1)$ when $\mu_i(t_j = M|h_j^t) < \frac{G_p(1-\theta_j)-C_p}{G_p(1+\beta-\theta_j)}$ and $\theta_j < 1 - \frac{C_p}{G_p}$. In sum, given the belief $\mu_i(t_j|(h_j^t, a_j(t)))$ which can be derived by Formula (9), the PBE pair for the dynamic TPP game is (ψ_t^*, ϕ_t^*).

V. Simulation Results and Analysis

In this section, we provide simulation results to illustrate the properties of equilibrium strategies in the dynamic TPP game. We implement PBE strategies in mobile nodes. Nodes are moving in the 200X200 m^2 area within DHDN/3-degree Gauss-Kruger zone 2 (EPSG code: 31466). Nodes' trajectories are generated by using the Random Street model of BonnMotion [15]. The maximum transmission range of each node is set to be 40 m, referenced to the average maximum transmission range in our real experiments on MEMSIC sensors equipped with MTS420 boards. The default values of the payoff matrix and system parameters are $G_p = 50, G_r = 5, C_p = 1, C_A = 2, P = 0.2, \alpha_t = 0.8, \beta = 0.9, \beta_t = 0.2, \gamma_t = 0.2$.

We first analyze the probability for a node to play *Trust* in the two-node dynamic TPP game. Figure 1 shows that when attackers have a higher successful attacking rate, users need to decrease trust. The trajectory privacy gain G_p has more obvious impact on trust. When G_p has greater values, it indicates that the user weighs trajectory privacy more critically and also encourages the attacker to attack more frequently. Therefore, users' trust of others dramatically decreases.

Figure 2 and Figure 3 show the node i's belief update and node j's corresponding attacking rate when consecutive *Attacks* are observed by i in each stage t. $\theta_j = 0.5$. The figures suggest that regardless of the initial belief that i holds, observing consecutive *Attacks* gives a very fast convergence of i's belief that j is a malicious node. As a result, the attacker has to reduce the attacking rate fast. These results are obtained when we assume that two nodes are always one-hop neighboring nodes. As a comparison, Figure 5 and Figure 6 show the belief update and attacking rate when the malicious node plays *Attack* rationally according to its PBE strategy. The data are collected from different scenarios where the malicious nodes A and B have different trajectory similarities with i. Trajectories of node i, A and B are illustrated in Figure 4. Node A is always closely following i and node B is i's one-hop neighbor in half of the time. The result is based on the average value from 1,000 iterations. i's belief of node A converges slightly slower compared with the results in Figure 2 because node A also plays *Cooperate* and *Attack* is observed less frequently. Node A's attacking rate also reduces slower in order to gain more payoffs by attacking in longer time. i's belief of node B converges much slower because at some stages the TPP game cannot be conducted. In this case, the belief remains the same as the previous stage.

Finally, we extend the two-node dynamic TPP game to a multi-node game in simulations by allowing each node in the network to play the TPP game with all the corresponding neighboring nodes. We simulate a mWSN composed of 200 mobile nodes and analyze the network trajectory privacy gain under different strategies of the nodes seeking TPP cooperation. There are 40 malicious nodes and 160 regular nodes, including selfish nodes and open nodes. Each regular node randomizes its trajectory privacy level with the upper bound of $\Theta = 0.7$. Malicious nodes are programmed to play the PBE strategy. Regular nodes are programmed to play one of the following three strategies: the pure strategy–always *Trust*; the mixed BNE strategy; and the PBE strategy respectively. The results are presented in Figure 7 and Figure 8. We show the average data based on 10 groups of trajectory data and 1,000 iterations for each group. When regular nodes playing mixed BNE strategy, both regular nodes and attackers get low average payoffs in the actual game within 20 stages. This is because the mixed strategy suggests regular nodes a fair probability to play *Trust* no matter how malicious nodes act. This strategy neither encourages nor discourages malicious nodes to *Attack*. On the other hand, if regular nodes always play *Trust*, it greatly encourages malicious nodes to *Attack*. Therefore, this pure strategy gives very high average payoffs to the attacker. Although malicious nodes follow the PBE strategy and reduce the attacking rate gradually, regular nodes get high average payoffs by always getting cooperation from open nodes. Finally, when both players follow the PBE strategy pair, regular nodes get even higher average payoffs but malicious nodes' payoffs dramatically reduce along with the belief convergence. This is because regular nodes take actions according to the dynamically updated beliefs of other peer nodes. The PBE strategy allows regular nodes to catch more opportunities to *Trust* open nodes to gain trajectory privacy while often playing *Not Trust* with malicious nodes.

VI. Conclusions and Future Work

In this paper, we apply Bayesian game theory to model node behaviors in trajectory privacy preservation activities in mWSNs. We formulate the characteristics of autonomous nodes, including selfish, malicious and cooperative, in the TPP game, and evaluate the trustworthiness of the unknown type node. The equilibrium strategies of the game have been derived and analyzed in both theoretical and simulation results.

Although this is a two-player game, it does not imply that only two nodes can participate into TPP activities. Each node can play the TPP game with any other node in the network. Our simulation in the mWSN has considered possible TPP interaction among all the nodes in the network. That being said, developing the multi-player TPP game is still meaningful in the sense that it is easier to model a multi-step TPP activity and track the payoff using multi-player games. Moreover,

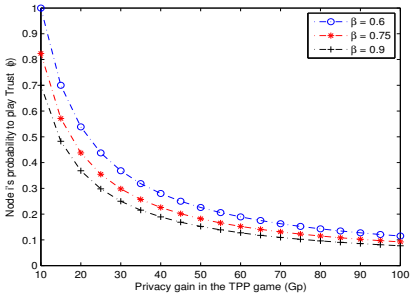

Fig. 1. Users' trust in the TPP game

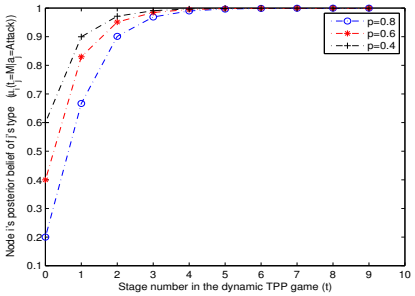

Fig. 2. Node i's posterior belief given the observation of consecutive *Attacks*

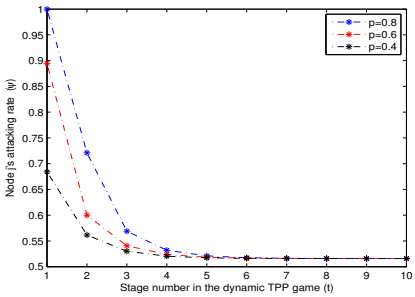

Fig. 3. Node j's attacking rate given the observation of consecutive *Attacks*

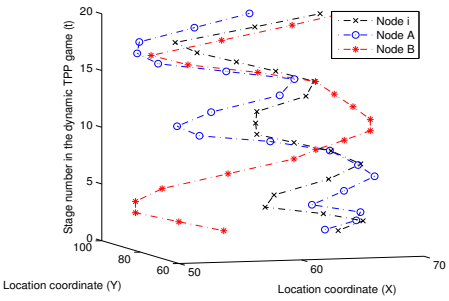

Fig. 4. The illustration of selected nodes' trajectories in the network

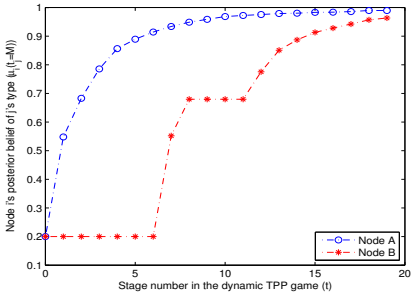

Fig. 5. Node i's belief update of the selected malicious nodes

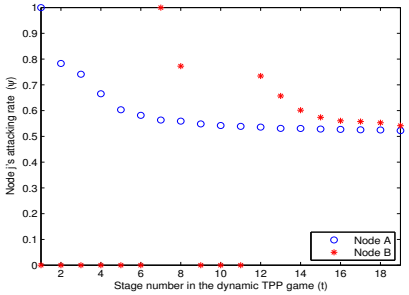

Fig. 6. The attacking rate of the selected malicious nodes

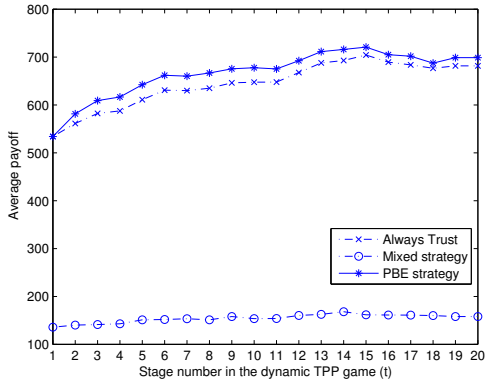

Fig. 7. The actual average payoff of regular nodes in the network

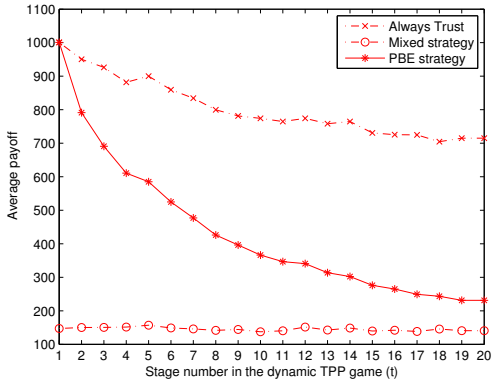

Fig. 8. The actual average payoff of malicious nodes in the network

the post detection strategy has not been discussed here. For example, the regular node can take the Grim Trigger strategy to cut off any cooperation once it observes an *Attack* from a node or has 100 percent belief in a node's malice. Another direction to improve this work is to specify the landscape to facilitate the sensitivity customization in specific applications. We will consider these issues in the extension work.

ACKNOWLEDGMENT

The authors would like to thank Francesco Pittaluga, the NSF REU fellow, for his editing contribution on this paper, and the Dissertation Year Fellowship support provided by Florida International University Graduate School.

REFERENCES

[1] X. Jin and N. Pissinou, "Trajectory Privacy Preservation – An Inevitable Issue towards Future Mobile Sensor Networks," *International Journal of Research and Reviews in Wireless Sensor Networks*, vol. 2, no. 2, 2012.

[2] J. Freudiger, M. H. Manshaei, J. P. Hubaux, and D. C. Parkes, "On Non-cooperative Location Privacy: A Game-theoretic Analysis," in *ACM Conference on Computer and Communications Security (CCS)*, 2009.

[3] X. Jin, N. Pissinou, C. Chesneau, S. Pumpichet, and D. Pan, "Hiding Trajectory on the Fly," in *Communications (ICC), 2012 IEEE International Conference on*, June 2012, pp. 403-407.

[4] R. Shokri, G. Theodorakopoulos, C. Troncoso, J. P. Hubaux, and J. Y. Le Boudec, "Protecting Location Privacy: Optimal Strategy against Localization Attacks," in *Proceedings of ACM conference on Computer and Communications Security*, 2012, pp. 617-627.

[5] M. Humbert, M. Manshaei, J. Freudiger, and J. P. Hubaux, "Tracking Games in Mobile Networks," in *Decision and Game Theory for Security*,

ser. Lecture Notes in Computer Science, T. Alpcan, L. Buttyan, and J. Baras, Eds. Springer Berlin Heidelberg, 2010, vol. 6442, pp. 38-57.

[6] N. J. Croft and M. S. Olivier, "Location Privacy: Privacy, Efficiency and Recourse through A Prohibitive Contract," *Transactions on Data Privacy*, vol. 4, no. 1, pp. 19-30, 2011.

[7] A. K. Chorppath and T. Alpcan, "Trading Privacy with Incentives in Mobile Commerce: A Game Theoretic Approach," *Pervasive and Mobile Computing*, Aug. 2012.

[8] F. De Meneses Neves Ramos Dos Santos, M. Humbert, R. Shokri, and J. P. Hubaux, "Collaborative Location Privacy with Rational Users," in *2nd Conference on Decision and Game Theory for Security (GameSec)*, 2011.

[9] C. Kamhoua, N. Pissinou, and K. Makki, "Game Theoretic Modeling and Evolution of Trust in Autonomous Multi-hop Networks: Application to Network Security and Privacy," in *Communications (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1-6.

[10] W. Wang, M. Chatterjee, and K. Kwiat, "Coexistence with Malicious Nodes: A Game Theoretic Approach," in *Game Theory for Networks, 2009. GameNets '09. International Conference on*, May 2009, pp. 277-286.

[11] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian Game Approach for Intrusion Detection in Wireless Ad hoc Networks," in *ACM International Conference Proceeding Series*, 2006.

[12] R. B. Myerson, *Game Theory: Analysis of Conflict*. Harvard University Press, 1997.

[13] M. J. Osborne, *An Introduction to Game Throy*. Oxford University Press, 2004.

[14] J. T. Drew Fudenberg, *Game Throy*. MIT Press, 1991.

[15] "Bonnmotion: A mobility scenario generation and analysis tool," http://net.cs.uni-bonn.de/wg/cs/applications/bonnmotion/, accessed: 06/01/2013.