On Non-Cooperative Location Privacy: A Game-Theoretic Analysis

Julien Freudiger[†], Mohammad Hossein Manshaei[†], Jean-Pierre Hubaux[†], and David C. Parkes[‡]

[†] School of Computer and Communication Sciences, EPFL, Switzerland
{julien.freudiger, hossein.manshaei, jean-pierre.hubaux}@epfl.ch
[‡] School of Engineering and Applied Science, Harvard University, USA
parkes@eecs.harvard.edu

ABSTRACT

In mobile networks, authentication is a required primitive of the majority of security protocols. However, an adversary can track the location of mobile nodes by monitoring pseudonyms used for authentication. A frequently proposed solution to protect *location privacy* suggests that mobile nodes collectively change their pseudonyms in regions called mix zones. Because this approach is costly, self-interested mobile nodes might decide not to cooperate and could thus jeopardize the achievable location privacy. In this paper, we analyze the non-cooperative behavior of mobile nodes with a game-theoretic model, where each player aims at maximizing its location privacy at a minimum cost. We first analyze the Nash equilibria in n-player complete information games. Because mobile nodes in a privacy-sensitive system do not know their opponents' payoffs, we then consider incomplete information games. We establish that symmetric Bayesian-Nash equilibria exist with simple threshold strategies in n-player games and derive the equilibrium strategies. By means of numerical results, we show that mobile nodes become selfish when the cost of changing pseudonym is small, whereas they cooperate more when the cost of changing pseudonym increases. Finally, we design a protocol - the PseudoGame protocol - based on the results of our analysis.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection (e.g., firewalls)*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Algorithms, Design, Economics, Security, Theory

Keywords

Location Privacy, Game Theory, Mobile Networks

CCS'09, November 9–13, 2009, Chicago, Illinois, USA.

1. INTRODUCTION

Mobile ad hoc networks such as networks of directly communicating hand-held devices [1, 2, 3], vehicular networks [31, 56] and delay tolerant networks [20] have brought new security challenges due to their mobile and infrastructureless nature. In particular, in order to verify the identity of communicating parties, to revoke misbehaving nodes and to establish secure associations, ad hoc networks typically require an authentication feature. To do so, each mobile node is preloaded with an asymmetric key pair and all messages it sends are signed with the same private key. As receivers use the public key of a sender to verify the signature, the public key is usually sent along with the messages. However, much to the detriment of privacy, external parties can monitor public keys to learn the locations of mobile nodes.

Hence, when privacy-conscious nodes authenticate themselves to others, they must avoid revealing privacy-sensitive information. The *multiple pseudonym* approach [15], suggested in the context of Internet communications, assigns a set of asymmetric key pairs to every node that are used alternatively in order to protect their privacy.[1] Both industry [4] and academia [7, 9, 37, 43, 50] have adopted this approach in order to achieve *location privacy* in mobile ad hoc networks. A set of pseudonyms is usually preloaded into mobile devices by an off-line certification authority [51]. Then, over time, mobile nodes change the pseudonym used to send messages. To impede an adversary from linking old and new pseudonyms, a change of pseudonym should be spatially and temporally coordinated among mobile nodes [7]. More specifically, a node cannot free-ride on the pseudonym change of others to achieve location privacy as its pseudonym can still be tracked. Hence, location privacy is not achieved by itself but requires a collective effort from neighboring mobile nodes.

The coordination of pseudonym changes has become a central topic of research with various approaches proposed. One solution [9] consists in changing pseudonyms periodically, at a pre-determined frequency. The mechanism works if at least two mobile nodes change their pseudonyms in proximity, a condition that is rarely met (as the probability of a synchronous change is low). Base stations can be used as coordinators to synchronize pseudonym changes [37], but this solution requires the help of the infrastructure. The approach in [27] enables mobile nodes to change their pseu-

[1]The public key serves as an identifier of the nodes and is usually referred to as the *pseudonym.*

donyms at specific time instances (e.g., before associating with wireless base stations). However, this solution achieves location privacy only with respect to the infrastructure. Another approach [7, 22, 24] coordinates pseudonym changes by forcing mobile nodes to change their pseudonyms within pre-determined regions called *mix zones*. However, this approach lacks flexibility because the locations of mix zones are fixed by a central authority and must be learned by mobile nodes prior to entering the network. Several researchers advocated the use of a distributed solution [36, 37, 43], where mobile nodes coordinate pseudonym changes to dynamically obtain mix zones. To do this, a mobile node simply broadcasts a pseudonym change request to its neighbors. This solution is particularly appealing in mobile ad hoc networks because it does not require the help of the infrastructure nor prior knowledge of the location of mix zones.

Nevertheless, the multiple pseudonym approach has drawbacks that affect the performance of current solutions. First, a pseudonym change causes considerable overhead, thus reducing networking performance: for example, routing algorithms must update their routing tables [51]. Second, given the cost of pseudonym generation and management by the central authority, mobile nodes are usually assigned a limited number of pseudonyms that can quickly become a scarce resource if changed frequently. Pseudonyms are thus costly to acquire and use. Third, mix zones have a cost because they impose limits on the services available to mobile users: in order to protect against spatial correlation of location traces, mix zones can conceal the trajectory of mobile nodes by not allowing nodes in the mix zone to communicate [36]. Hence, the number of mix zones traversed by mobile nodes must be kept small. Finally, even if the distributed solution synchronizes pseudonym changes, it does not align incentives between mobile nodes: because the achieved location privacy depends on both the node density and the unpredictability of node movements in mix zones [7], a selfish mobile node might decide to not change its pseudonym in settings offering low location privacy guarantees.

In contrast with existing approaches, we consider *selfish* mobile nodes that locally decide whether to change their pseudonyms or not. With this paradigm shift, we tackle one of the main issues that to date has hindered the use of multiple pseudonym schemes. Although selfish behavior can reduce the cost of location privacy based on multiple pseudonyms, it can also jeopardize the welfare achieved with a location privacy scheme. Hence, we investigate whether the multiple pseudonym approach achieves location privacy in non-cooperative scenarios.

To the best of our knowledge, this paper is the first to investigate the game-theoretic aspects of location privacy in mobile networks. We propose the first *user-centric location privacy model* capturing the evolution of the location privacy level of mobile nodes over time. Mobile nodes measure with the model their location privacy level in order to determine when to change pseudonyms. We define a game-theoretic model - the *pseudonym change game* - that models the decisions of mobile nodes in a mix zone. We first analyze the game with *complete information* (i.e., every node knows the user-centric location privacy level of other nodes) and we obtain both pure and mixed Nash equilibria [44]. We show that nodes should coordinate their strategies: nodes should either cooperate when there is a sufficient number of neighbors with low privacy, or defect. Then, because mobile nodes will in general not have good knowledge of the payoffs of other nodes, we study the *incomplete information* scenario using a Bayesian approach [30]. We evaluate both theoretically and numerically the game model, and derive the Bayesian Nash equilibria for a class of threshold strategies in which nodes decide whether to change their pseudonym based on comparing their privacy level to a threshold value. We find a symmetric equilibrium, in which all nodes cooperate with the same probability, as determined with respect to a distribution over privacy levels. We compare the game-theoretic approach with random and socially-optimal strategies and show that using the Bayesian Nash equilibrium, players reduce their consumption of pseudonyms while still achieving high location privacy. Finally, we design the PseudoGame protocol that implements the pseudonym change game. This paper is part of the recent trend of blending game theory with security/cryptographic mechanisms when selfish parties are involved [10, 29, 38, 39, 45, 47].

This paper is organized as follows. In Section 2, we discuss the state of the art of location privacy and the economics of privacy. In Section 3, we present the system and threat models considered throughout the paper. In Section 4, we propose the user-centric location privacy model. In Section 5, we present the game model that we then investigate with complete information in Section 6 and incomplete information in Section 7. Section 8 describes the pseudonym change game protocol. We conclude the paper in Section 9.

2. RELATED WORK

Previous works on location privacy [6, 34, 42] show that the adversary can implicitly obtain the true identity of the owner of a mobile node from the analysis of its location. Using location traces collected from an office environment or using GPS traces from vehicles, several studies [6, 34, 42] correctly identified most drivers. Hence, pseudonyms are not sufficient to protect the location privacy of mobile nodes and should be changed *over time* to avoid such attacks. But even if location traces of mobile nodes do not contain any pseudonyms, Hoh and Gruteser [32] were able to reconstruct the tracks of mobile nodes using a multiple target tracking (MTT) algorithm. Hence, location traces should also be altered *spatially*. In other words, the spatial and temporal correlation between successive locations of mobile nodes must be carefully eliminated to prevent external parties from compromising their location privacy. In this paper, location privacy is achieved by changing pseudonyms in regions called *mix zones* [6], where the location of mobile nodes cannot be eavesdropped.

Note that mobile nodes make use of long-term identifiers, such as MAC (Medium Access Control) addresses, to communicate on the data link. For example, in IEEE 802.11, the MAC addresses are 48-bit values included in frames to identify the source or destination of a frame. MAC addresses can be anonymized to serve uniquely for short term communications. To do so, one approach [27] consists in changing the MAC address every time a pseudonym is changed. Another possibility [26] is to obscure the MAC address and use an identifier-free link layer protocol.

Similarly, it is possible to identify devices relying on their distinctive characteristics (i.e., fingerprints) at the physical, link and application layer. At the physical layer, the wireless transceiver has a wireless fingerprint that can identify wireless devices in the long term using modulation-based tech-

niques [8], transient-based techniques [19], amplitude-based techniques [53] or a combination of features [28, 46]. However, these techniques are only evaluated with specific technologies and countermeasures could be developed. Hence, in mobile networks, it remains unclear how much identifying information can be extracted from the physical layer. At the link layer, it is possible to distinguish between a number of devices and drivers [21]. At the application layer, devices can also be identified based on clock skews [40]. However, such techniques require an active adversary and can be countered by ignoring the requests sent by the adversary. Similarly, a reduction of the differences between drivers would limit the effectiveness of such attacks. Note that independently from the presence of fingerprinting attacks, higher layer privacy mechanisms such as mix zones remain useful. Some applications may for example require keeping location traces for a while (e.g., for congestion analysis).

There are several techniques besides the multiple pseudonym approach to achieve location privacy. *Group signatures* [16] allow a group member to sign on behalf of a group without revealing the identity of the signer. The main drawback of group signatures is that they require a group manager to add and revoke group members. The size of the group determines the achieved privacy of its member. Similary, *Ring signatures* [49] allow to sign on behalf of an ad hoc group of nodes without the help of a central coordinator. However, the location privacy provided by ring signatures is still an open problem [23]. *Anonymous credential systems* (e.g., Idemix [12]) allow mobile nodes to anonymously authenticate to third parties with the help of an online credential issuer. The online availability of a credential issuer is often not possible in wireless networks. To circumvent the issue, techniques based on unclonable identifiers, such as e-tokens [13], allow nodes to anonymously authenticate themselves a given number of times per period. However, such techniques do not work in the case of a prolonged absence of the credential issuer.

Game theory has been used to evaluate the strategic behavior of mobile nodes in ad hoc networks for node revocation [47]. It has also been used to study privacy. Acquisti [5] explores the reasons why decentralized anonymity infrastructures are still not in wide use today. Varian [54] depicts the role of privacy in economic transactions, showing that because of the advantages of price discrimination, consumers may be less inclined to protect their privacy. In this paper, we study a new aspect of privacy by evaluating how privacy can be achieved among non-cooperative nodes.

3. PRELIMINARIES

We focus exclusively on the peer-to-peer communications between nodes and do not consider communications with the infrastructure (such as cellular networks or WLAN).

3.1 System Model

We study a network where mobile nodes are autonomous entities equipped with WiFi or Bluetooth-enabled devices that communicate with each other upon coming in range. In other words, we describe a pervasive communication system (a mobile ad hoc network) such as a vehicular network [31], a delay tolerant network [20], or a network of directly communicating hand-held devices [1, 2, 3] in which mobile nodes in proximity automatically exchange information.

As commonly assumed in such networks, we consider an offline Certification Authority (CA) run by an independent trusted third party that pre-establishes the credentials for the devices. In line with the multiple pseudonym approach to protect location privacy, we assume that prior to entering the network, every mobile node i registers with the CA that preloads a set of M *public/private key* pairs $\{Pub_i^k, Prv_i^k\}_{k=1}^{M}$ to provide verification and signature functionalities, respectively. Note that the CA verifies the identity of each user upon registration. A public key Pub_i^k serves as the identifier of node i and is referred to as its *pseudonym*. The private key Prv_i^k enables node i to digitally sign messages, and the digital certificate validates the signature authenticity.

We consider a discrete time system with initial time $t = 0$. At each time step t, mobile nodes move in the network. We assume that mobile nodes automatically exchange information (unbeknownst to their users) as soon as they are in communication range of each other. Note that our evaluation is independent from the communication protocol. Still, we align our communication model with common assumptions of pervasive communication systems: mobile nodes advertise their presence by periodically broadcasting proximity beacons (e.g., every 100ms over a range of 300m in vehicular networks) containing the node's authenticating information (as well as the position and speed in vehicular networks). Due to the broadcast nature of wireless communications, beacons enable mobile nodes to discover their neighbors. When a node i receives a beacon, it controls the legitimacy of the sender by checking the certificate of the public key of the sender. After that, i verifies the signature of the beacon message. Subsequently, if confidentiality is required, a security association is established (e.g., with Diffie-Hellman). Note that there is ongoing work in the literature [11, 14] to reduce the cryptographic overhead induced by the processing of all messages.

3.2 Threat Model

We assume that an adversary $\mathcal{A}$ aims to track the location of mobile nodes. We consider that $\mathcal{A}$ can have the same credentials as mobile nodes and is equipped to eavesdrop communications. In practice, the adversary can thus be a rogue individual, a set of malicious mobile nodes, or may even deploy its own infrastructure by placing eavesdropping devices in the network. In the worst case, $\mathcal{A}$ obtains complete coverage and tracks nodes throughout the entire network. We characterize the latter type of adversary as *global*.

$\mathcal{A}$ collects identifying information (i.e., pseudonyms) from the entire network and obtains *location traces* that allow him to track the location of mobile nodes. Hence, the problem we tackle in this paper consists in protecting the *location privacy* of mobile nodes, that is, to prevent other parties from learning a node's past and current location [7]. Finally, we assume that the key-pair generation and distribution process cannot be altered or controlled by the adversary.

4. USER-CENTRIC LOCATION PRIVACY

In this section, we evaluate the amount of location privacy provided by the use of multiple pseudonyms. We then propose a user-centric model of location privacy to capture the location privacy of a node over time.

4.1 Location Privacy

There are several techniques to mitigate the tracking of mobile nodes, as discussed in the related work Section. In

this paper, we consider the use of *multiple pseudonyms*: mobile nodes change over time the pseudonym to sign messages, thus reducing their long term linkability. To avoid spatial correlation of their location, mobile nodes in proximity coordinate pseudonym changes in regions called mix zones. In order to thwart Sybil attacks, we assume that as soon as a node changes pseudonym, the old pseudonym expires and is removed from the node's memory. Mix zones can also conceal the trajectory of mobile nodes to protect against the spatial correlation of location traces, e.g., by using (i) silent mix zones [36, 43], (ii) a mobile proxy [50], or (iii) regions where the adversary has no coverage [9]. Without loss of generality, we assume silent mix zones: mobile nodes turn off their transceivers and stop sending messages for a certain period of time. If at least two nodes changing pseudonym in a silent mix zone, a mixing of their whereabouts occurs and the mix zone becomes a *confusion point* for the adversary.

Consider a mobile network composed of N mobile nodes. At time t, a group of $n(t)$ mobile nodes are in proximity. One node among the $n(t)$ nodes can initiate the pseudonym change using the one-round protocol suggested in [43] (i.e., the Swing protocol): a mobile node broadcasts an initiation message to start the pseudonym change. The $n(t)-1$ mobile nodes in proximity receive the message and enter a silent period during which they decide whether to change their pseudonyms or not. During the silent period, nodes cannot observe each other messages. At the end of the silent period, it appears that all pseudonym changes occur simultaneously. Mobile nodes must thus decide to change pseudonym without knowing the decision of other nodes in proximity.

The adversary $\mathcal{A}$ observes the set of $n(T)$ nodes changing pseudonyms, where T is the time at which the pseudonym change occurs. $\mathcal{A}$ compares the set B of pseudonyms before the change with the set D of pseudonyms after the change and, based on the mobility of the nodes, predicts the most probable matching [7, 43]. Let $p_{d|b} = Pr(\text{“Pseudonym } d \in D \text{ corresponds to } b \in B\text{”})$, that is the probability that a new pseudonym $d \in D$ corresponds to an old pseudonym $b \in B$. As is standard in the literature [52], the uncertainty of the adversary, and thus for our purposes the location privacy level of node i involved in a successful pseudonym change at time T, is

$$A_i(T) = -\sum_{d=1}^{n(T)} p_{d|b} \log_2(p_{d|b}) \tag{1}$$

The achievable location privacy depends on both the number of nodes $n(T)$ and the unpredictability of their whereabouts in the mix zone $p_{d|b}$. If a node i is the only one to change its pseudonym, then its identity is known to the adversary and its location privacy level is defined to be $A_i(T) = 0$. The entropy is maximum for a uniform probability distribution $p_{d|b}$, which would provide node i with a location privacy level of $log_2(n(T))$. This can be achieved, for example, after a coordinated pseudonym change by all players. We denote T_i^ℓ the time of the *last* successful pseudonym change of node i, i.e. when at least one other node changed its pseudonym.

4.2 User-Centric Model

The entropy metric evaluates the location privacy achieved in mix zones of the network. However, the location privacy needs of individual users vary depending on time and location. It is thus desirable to protect the location privacy in a user-centric manner, such that each user can decide when and where to protect its location privacy. Hence, we consider a user-centric model of location privacy. *User-centric location privacy* [33, 35, 43] is a distributed approach where each mobile node locally monitors its location privacy level over time. The user centric approach is easily scalable and permits a more fine-grained approach to maintaining location privacy. Each mobile node can evaluate the distance over which it is potentially tracked by an adversary (i.e., the *distance-to-confusion* [33]) and act upon it by deciding whether and when to change its pseudonym. A network wide metric, on the other hand, measures average location privacy and might ignore that some nodes have a low location privacy level and are traceable for long distances.

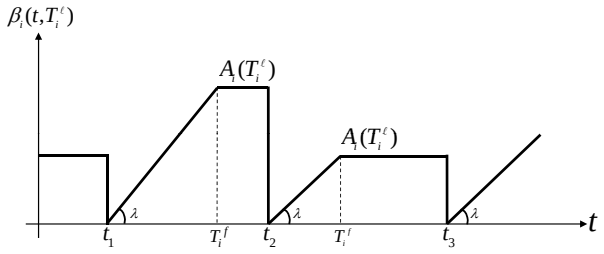

Figure 1: Location privacy loss function $\beta_i(t, T_i^\ell)$. At t_1, node i changes pseudonym and updates its time of last successful pseudonym change: $T_i^\ell := t_1$. The function $\beta(t, T_i^\ell)$ increases according to the user sensitivity λ and estimates the time at which mobile i becomes unsatisfied with its location privacy (T_i^f). At t_2, node i changes pseudonym again and updates $T_i^\ell := t_2$.

With a user-centric model, mobile nodes can request a pseudonym change from other nodes in proximity when their local location privacy level is lower than a desired level. Nodes in proximity will then choose to cooperate when their location privacy level is low as well. The drawback of the user-centric model is that nodes may have misaligned incentives (i.e., different privacy levels) and this can lead to failed attempts to achieve location privacy.

In this work, we formalize this problem and introduce a *user-centric location privacy model* to capture the evolution of user-centric location privacy level over time. The user-centric location privacy level of each mobile node i is modeled via a *location privacy loss function* $\beta_i(t, T_i^\ell) : (\mathbb{R}^+, \mathbb{R}^+) \rightarrow \mathbb{R}^+$ where t is the current time and $T_i^\ell \leq t$ is the time of the last successful pseudonym change of mobile i. The maximum value of $\beta_i(t, T_i^\ell)$ equals the level of location privacy achieved at the last pseudonym change. The privacy loss is initially zero, and increases with time according to a sensitivity parameter, $0 < \lambda_i < 1$, which models the belief of node i about the tracking power of the adversary. The higher the value of λ_i, the faster the rate of privacy loss increase. For simplicity, we consider that $\lambda_i = \lambda$, $\forall i$. For a given T_i^ℓ, we write:

$$\beta_i(t, T_i^\ell) = \begin{cases} \lambda \cdot (t - T_i^\ell) & \text{for } T_i^\ell \leq t < T_i^f \\ A_i(T_i^\ell) & \text{for } T_i^f \leq t \end{cases} \tag{2}$$

where $T_i^f = \frac{A_i(T_i^\ell)}{\lambda} + T_i^\ell$ is the time when the function reaches the maximal privacy loss (i.e., the user-centric lo-

Table 1: List of symbols.

Symbol	Definition
t	Time
T_i^ℓ	Time of last successful pseudonym change
$A_i(t)$	Location privacy of node i at time t
$\beta_i(t, T_i^\ell)$	Location privacy loss function
λ	Location privacy sensitivity
γ	Cost of changing pseudonym
T_i^f	Time for which $\beta(t, T_i^\ell)$ is maximum
$\alpha_i(t, T_i^\ell)$	Counter of wasted pseudonyms
N	Total number of nodes in the system
$n(t)$	Number of nodes in transmission range at time t
P_i	Player i of the pseudonym change game
$p_{d\|b}$	Probability that pseudonym d corresponds to b
$u_i(t, T_\ell, s_i, s_{-i})$	Payoff function
θ_i	Type of player
$f(\theta_i)$	Probability density function of type
$\tilde{\theta}_i$	Threshold to change type
s_i	Pure-strategy of node i
s_{-i}	Pure-strategy of other nodes besides i
$n_C(s_{-i})$	Number of cooperative nodes besides i
S_i	Space of pure-strategies
S_i^Θ	Space of pure-strategies in Bayesian game

cation privacy is null). Figure 1 illustrates how the function evolves with time. Given this location privacy loss function, the user-centric location privacy of node i at time t is:

$$A_i(t) = A_i(T_i^\ell) - \beta_i(t, T_i^\ell),\ t \geq T_i^\ell \tag{3}$$

Time T_i^f is the time at which node i's location privacy will be zero unless it is successful in changing its pseudonym at a new confusion point. Based on the time of the last successful pseudonym change T_i^ℓ, mobile nodes rationally estimate when to change pseudonym next.[2] Note that, in practice, nodes cannot compute $A_i(T_i^\ell)$ precisely. Hence, we consider that nodes use an approximation such as the upperbound $\log_2(n)$.

In our model, a node's location privacy does not accumulate over time. Rather, it depends only on the number of nodes that cooperate in the last successful pseudonym change. Moreover, mobile nodes are given the ability to control the length of path that is revealed to an adversary before the next pseudonym change. If a mix zone is a strong confusion point (i.e., $A_i(T_i^\ell)$ is large), then a node can choose to reveal a longer distance before changing pseudonym again. If a mix zone is a weak confusion point, a node can attempt another pseudonym change as soon as possible. In doing so, a node has autonomy to control the period of time over which its location can be tracked. Because the achievable location privacy defined by Eq. (1) is logarithmic and the location privacy loss function is linear, the user-centric location privacy level will decrease quickly. In our future work, we plan to analyze the effect of other loss functions (e.g., super-linear functions).

5. PSEUDONYM CHANGE GAMES

In this section, we present the game-theoretic aspects of achieving location privacy with multiple pseudonyms in a selfish environment. We introduce a game-theoretic model that we refer to as the *pseudonym change game G*. Table 1 summarizes the notation used throughout the paper. Upon receiving a pseudonym change request, mobile nodes must decide whether to collaborate and change pseudonyms. The key point of the game-theoretic analysis is to consider costs and the potential location privacy gain when making a pseudonym change decision.

On one hand, pseudonyms are costly to acquire and use because they are owned in limited number and require contacting a central authority for refill. Similarly, routing [51] becomes more difficult and requires frequent updates of routing tables. In addition, while traversing silent mix zones, mobile nodes cannot communicate and momentarily lose access to services. We take into account the various costs involved in changing pseudonym in a parameter γ that can be expressed as: $\gamma = \gamma_{acq} + \gamma_{rte} + \gamma_{sil}$, where γ_{acq} is the cost of acquiring new pseudonyms, γ_{rte} is the cost of updating routing tables, and γ_{sil} is the cost of remaining silent while traversing a mix zone. The cost is expressed in privacy units (e.g., bits), causing a decrease in the achieved privacy. Thus, rational mobile nodes might refuse to change pseudonym in order to reduce their costs. Moreover, selfish behavior might jeopardize the achievable location privacy.

On the other hand, the available location privacy gain (upperbounded by the density of nodes and their whereabouts unpredictability) and the user-centric location privacy level might encourage selfish mobile nodes to change pseudonym and obtain a satisfactory location privacy level. Hence, using a game-theoretic analysis, we investigate whether location privacy can emerge in a non-cooperative system and despite the cost incurred by a node in changing its pseudonym, differentiated privacy levels, and the need for coordinated pseudonym changes to achieve a confusion point. We consider rational mobile nodes that maximize their payoff function, which depends on the current location privacy and the associated pseudonym management cost.

5.1 Game Model

Game theory allows for modeling situations of conflict and for predicting the behavior of participants. In our *pseudonym change game G*, nodes must decide upon meeting in the network whether to change pseudonym or not. We model the pseudonym change game as a *static* game because mix zones are silent and thus a node is unable to sense its wider environment when deciding whether or not to change its pseudonym. This modeling decision also keeps our analysis tractable, while conforming to a simple, but game-theoretic, model of node rationality. The game G is defined as a triplet $(\mathcal{P}, \mathcal{S}, \mathcal{U})$, where $\mathcal{P}$ is the set of players, $\mathcal{S}$ is the set of strategies and $\mathcal{U}$ is the set of payoff functions. At any time t, several games are played in parallel (but nodes participate in a single game at a time).

• **Players:** The set of players $\mathcal{P} = \{P_i\}_{i=1}^{n(t)}$ corresponds to the set of mobile nodes in transmission range of each other at time t. For a valid game we require $n(t) > 1$. We assume that each node knows the number of other nodes in the mix zone. To achieve a consensus on this number, each node could adopt a neighbor discovery protocol [55] to detect its neighbors.

• **Strategy:** Each player has two possible moves s_i: *Cooperate* (C) or *Defect* (D). By cooperating, a mobile node changes its pseudonym. The set of strategies of node i is thus $S_i = \{C, D\}$ and the set of strategies in the game is $\mathcal{S} = \{S_i\}_{i=1}^{n(t)}$.

[2]In a user-centric model, users are actually not involved: the devices make decisions on their behalf.

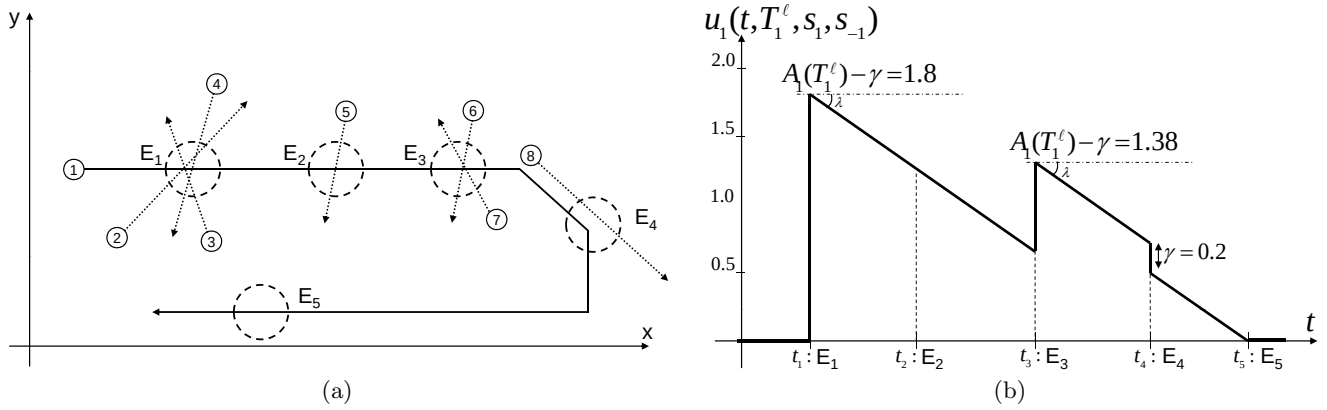

Figure 2: Example of pseudonym change. (a) 7 nodes move on the plane (x, y). (b) Evolution of the payoff of node 1 over time. At t_1 (event E_1 in (a)), nodes 2, 3, and 4 meet in a mix zone and cooperate with node 1. Their payoff u_i and the time of the last successful pseudonym change are updated: $u_i = A_i(T_i^\ell) - \gamma = \log_2(4) - \gamma = 1.8$, and $T_i^\ell := t_1$, $i \in \{1, 2, 3, 4\}$. The payoff of node 1 then decreases according to β_1 with slope λ. At t_2 (event E_2), node 1 defects. At t_3 (event E_3), node 1 cooperates with nodes 6 and 7. Consequently, the 3 nodes update their payoff and the time of the last successful pseudonym change. At t_4, (event E_4) node 1 cooperates but nodes 8 does not. Hence, the payoff of node 1 decreases by γ. Finally, at $T_1^f = t_5$, the payoff of node 1 reaches 0 (event E_5).

• **Payoff Function:** We model the *payoff* function of every node i as $u_i(t) = b_i(t) - c_i(t)$, where the benefit $b_i(t)$ depends on the level of location privacy of node i at time t, whereas the cost $c_i(t)$ depends on the privacy loss function and the cost of changing pseudonym at time t. If at least two nodes change pseudonyms, then each participating node improves its location privacy for the cost of a pseudonym change γ. If a node is alone in changing its pseudonym, then it still pays the cost γ and, in addition, its location privacy keeps decreasing according to the location privacy loss function. If a node defects, its location privacy continues to decrease according to its location privacy loss function. Formally, we have:

If $(s_i = C) \wedge (n_C(s_{-i}) > 0)$,

$$T_i^\ell := t \tag{4}$$

$$\alpha_i(t, T_i^\ell) := 0 \tag{5}$$

$$u_i(t, T_i^\ell, C, s_i) := \max\left(A_i(T_i^\ell) - \gamma, u_i^- - \gamma\right) \tag{6}$$

If $(s_i = C) \wedge (n_C(s_{-i}) = 0)$,

$$u_i(t, T_i^\ell, C, s_i) := \max\left(0, u_i^- - \gamma\right) \tag{7}$$

$$\alpha_i(t, T_i^\ell) := \alpha_i(t, T_i^\ell) + 1 \tag{8}$$

If $(s_i = D)$,

$$u_i(t, T_i^\ell, D, s_i) := \max\left(0, u_i^-\right) \tag{9}$$

where $u_i^- = A_i(T_i^\ell) - \gamma - \beta_i(t, T_i^\ell) - \gamma\alpha_i(t, T_i^\ell)$ is the payoff function at time t^-, which is the time immediately prior to t, s_{-i} is the strategy of the other players, $n_C(s_{-i})$ is the number of cooperating nodes besides i, and $\alpha_i(t, T_i^\ell)$ is the number of pseudonyms wasted by node i since its last successful pseudonym change T_i^ℓ. (Note that in contrast with the equality sign $=$, the sign $:=$ refers to the assignment of a new value to a variable.)

We can represent the static pseudonym change game in normal form. Table 2 shows an example for 2 players in power range of each other. Each player has two strategies: C or D. The value pairs in the cell represent the payoff of the player 1 and 2, respectively. We assume $u_i^i > \gamma$ for both players and can dispense with the $\max(0, \cdot)$ component of player payoff after an unsuccessful pseudonym change.

Table 2: Normal form of the two-player pseudonym change game.

$P_1 \backslash P_2$	C	D
C	$(A_1(T_1^\ell) - \gamma, A_2(T_2^\ell) - \gamma)$	$(u_1^- - \gamma, u_2^-)$
D	$(u_1^-, u_2^- - \gamma)$	(u_1^-, u_2^-)

Figure 2 (a) shows seven users moving in a network and playing a total of four pseudonym change games. Table 2 corresponds to the game played in event E_3 in Figure 2 (a). Figure 2 (b) illustrates the evolution of the payoff of node 1 playing the four games. Because we analyze only a single strategic interaction between players in this paper, we simplify notation and write $n = n(t)$, $\beta_i = \beta_i(t, T_i^\ell)$, $\alpha_i = \alpha_i(t, T_i^\ell)$, and $u_i(s_i, s_{-i}) = u_i(t, T_i^\ell, s_i, s_{-i})$.

• **Type:** Upon meeting other players, the strategy of a player depends on its knowledge of its opponent payoff function. As both the time of the last pseudonym change and the corresponding location privacy gain are unknown to other players, each player has *incomplete information* about its opponents payoffs. To solve the problem, Harsanyi [25] suggests the introduction of a new player named *Nature* that turns an incomplete information game into an *imperfect information game*. To do so, Nature assigns a type θ_i to every player i according to a *probability density function* $f(\theta_i)$ known to all players, where θ_i belongs to space of types Θ. The type of the players captures the private information of the player, that is, $\theta_i = u_i^-$, where u_i^- is the payoff to player i at time t^- just prior to the current opportunity to change

pseudonym. Because γ is common and known to all nodes, this completely defines the payoff of the node.

5.2 Equilibrium Concepts

In this section, we introduce the game-theoretic concepts that will help us get an insight into the strategic behavior of mobile nodes. In a complete information game, a pure-strategy for player i is $s_i \in S_i$, where $S_i = \{C, D\}$ is the pure-strategy space. A strategy profile $s = \{s_i\}_{i=1}^n$ defines the set of strategies of the players. Let us write $br_i(s_{-i})$, the best response of player i to the opponent's strategy s_{-i}.

DEFINITION 1. *The best response $br_i(s_{-i})$ of player i to the profile of strategies s_{-i} is a strategy s_i such that:*

$$br_i(s_{-i}) = \arg\max_{s_i} u_i(s_i, s_{-i}) \tag{10}$$

If two strategies are mutual best responses to each other, then no player has the motivation to deviate from the given strategy profile. This leads us to the concept of Nash Equilibrium [44].

DEFINITION 2. *A strategy profile s^* is a* Nash equilibrium *(NE) if, for each player i:*

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \forall s_i \in S_i \tag{11}$$

In other words, in a NE, none of the players can unilaterally change his strategy to increase his payoff. A player can also play each of his pure strategies with some probability using *mixed strategies*. A *mixed strategy* x_i of player i is a probability distribution defined over the pure strategies s_i.

In an incomplete information game, a pure-strategy for player i is a function $\underline{s}_i : \theta_i \rightarrow S_i$ where $S_i = \{C, D\}$. The pure-strategy space is denoted S_i^Θ. A strategy profile $\underline{s} = \{\underline{s}_i\}_{i=1}^n$ is the set of strategies of the players. In incomplete information games, the NE concept does not apply as such because players are unaware of the payoff of their opponents. Instead, we adopt the concept of Bayesian Nash equilibrium [25, 30]. Consider that Nature assigns a type to every player according to a common probability distribution $f(\theta_i)$. Because the type of a player determines its payoff, every player computes its best move based on its belief about the type (and thus the strategy) of its opponents.

DEFINITION 3. *A strategy profile $\underline{s}^* = \{\underline{s}_i^*\}_{i=1}^n$ is a pure-strategy* Bayesian Nash equilibrium *(BNE) if, for each player i:*

$$\underline{s}_i^*(\theta_i) \in \arg\max_{s_i \in S_i} \sum_{\theta_{-i}} f(\theta_{-i}) \cdot u_i(s_i, \underline{s}_{-i}^*(\theta_{-i})), \forall \theta_i \tag{12}$$

6. ANALYSIS OF COMPLETE INFORMATION GAME

We begin the analysis with a complete information model called the pseudonym change $\mathcal{C}$-game ($\mathcal{C}$ stands for complete information). Each player chooses a strategy simultaneously, and with common knowledge about the type of all players (i.e. $\mathcal{C}$-game). We obtain NE for the 2-player game, and generalize the results for n-player $\mathcal{C}$-games. We consider that upon a pseudonym change, every node achieves the same level of privacy and thus we consider the upperbound $A_i = \log_2(k)$, where $k \leq n$ is the number of cooperating nodes.

6.1 2-player $\mathcal{C}$-game

The strategic representation of the two player $\mathcal{C}$-game is shown in Table 3. Two players P_1 and P_2 meeting in a mix zone at time t take part in a pseudonym change game. Each mobile node decides independently whether to change its pseudonym without knowing the decision of its opponent. The game is played once and the two players make their moves simultaneously. The value in the cells represents the payoff of each player. As usual, the players want to maximize their payoff. We assume here that $u_i^- > \gamma$ for both players, so that $u_i^- - \gamma > 0$. Since u_i^- is itself bounded from above by $\log_2(2) - \gamma = 1 - \gamma$ in a 2-player game, we require $\gamma < 1/2$, so that the cost is bounded.

Table 3: 2-player $\mathcal{C}$-game.

$P_1 \backslash P_2$	C	D
C	$(1-\gamma, 1-\gamma)$	$(u_1^- - \gamma, u_2^-)$
D	$(u_1^-, u_2^- - \gamma)$	(u_1^-, u_2^-)

Each player knows u_{-i}^-, i.e. the payoff of the other player immediately before the game, which is sufficient to define its payoff for different strategy profiles because the cost γ is common knowledge. Theorem 1 identifies the potential equilibrium strategies for the players. The proof is provided in Appendix A.

THEOREM 1. *The 2-player pseudonym change $\mathcal{C}$-game has two pure-strategy Nash equilibria (C, C) and (D, D) and one mixed-strategy Nash equilibrium (x_1, x_2) where $x_i = \frac{\gamma}{1-u_{-i}^-}$ is the probability of cooperation of P_i.*

We observe that the pseudonym change game is a *coordination game* [18] because $log_2(2) - \gamma > u_i^- > u_i^- - \gamma$. Coordination games model situations in which all parties can realize mutual gains, but only by making mutually consistent decisions. Coordination games always have three NE as obtained with Theorem 1. (C, C) is the Pareto-optimal strategy and thus the preferred equilibrium. If the probability of cooperation x_i of each player equals 1, then the mixed equilibrium equals (C, C). Figure 3 illustrates the best response correspondence of the two players. For example, if both players have a low u_i^- (meaning a high propensity to cooperate), the mixed-strategy equilibrium approaches $(0, 0)$. In such scenario, the basin of attraction of the (C, C) NE (i.e., the surface of the rectangle between the mixed NE and the (C, C) NE) is larger than that of the (D, D) NE. In other words, (C, C) would be the most likely NE in settings where players find their best response with an adaptive behavior. The complete information pseudonym change game is *asymmetric* because the payoff of each player depends on its private type. For example, the mixing probability is different for each node (i.e., $x_1 \neq x_2$).

6.2 n-player $\mathcal{C}$-game

We extend the 2-player $\mathcal{C}$-game by considering a set of $n \leq N$ players meeting in a mix zone at time t. Each player has complete information and knows the payoff function u_i^- of its $n-1$ opponents. Let C^k and D^{n-k} denote the sets of k cooperating players and $n-k$ defecting players, respectively. The proofs of lemmas and theorems are provided in the Appendix. Lemma 1 identifies the existence of an All Defection NE.

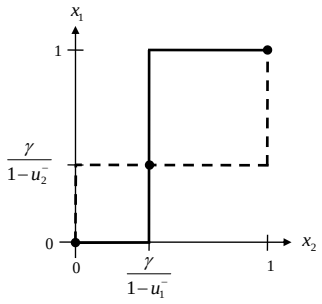

Figure 3: Best response correspondence for the 2×2 pseudonym change $\mathcal{C}$-game. The best response function of player P_1 is represented by the dashed line; that of player P_2 is represented by the solid one. The NE are where the two players' best responses cross.

LEMMA 1. *The All Defection strategy profile is a pure-strategy Nash equilibrium for the n-player pseudonym change $\mathcal{C}$-game.*

Lemma 2 identifies the existence of a NE with cooperation.

LEMMA 2. *Let C^{k^*} be a maximal set of cooperating nodes s.t. $\forall P_i \in C^{k^*}$, $\log_2(|C^{k^*}|) - \gamma > u_i^-$. If there exists such a C^{k^*}, then the strategy profile $s^* = \{s_i^* | s_i^* = C \text{ if } P_i \in C^{k^*}, s_i^* = D \text{ if } P_i \in D^{n-k^*}\}$ is the unique pure-strategy Nash equilibrium of the n-player pseudonym change $\mathcal{C}$-game, in which at least two players cooperate.*

Considering Lemma 1 and 2, and since there does not exist any NE in which only one player cooperates, we immediately have the following theorem

THEOREM 2. *The n-player pseudonym change $\mathcal{C}$-game has at least 1 and at most 2 pure-strategy Nash equilibria.*

To illustrate the above results, we consider the set of all possible strategy profiles in a 3-player $\mathcal{C}$-game. Assume that $N = 10$, the payoff of each P_i before playing the game is in the interval $[0, \log_2(10) - \gamma]$, depending on the number of nodes that have cooperated with P_i in the past (at T_i^ℓ) as well as the number of failed attempts and the rate of privacy loss. The set of all strategy profiles of this 3-player $\mathcal{C}$-game is: $s = \{(s_1, s_2, s_3) | s_i \in \{C, D\}\}$.

Lemma 1 proves that (D, D, D) is always a NE. From Lemma 2, (C, D, D), (D, D, C), and (D, C, D) are not NE, because $|C^{k^*}|$ must be strictly larger than 1 to satisfy $\log_2(|C^{k^*}|) - \gamma > u_i^-$. Among the remaining strategy profiles, there might be a single NE as defined by Lemma 2. The existence of this equilibrium depends on the payoff of each player. Assume that P_3 cooperated with 6 nodes at T_3^ℓ and its payoff is $\log_2(7) - \gamma - \beta_3 - \gamma\alpha_3$ that is bigger than $\log_2(2) - \gamma$ before playing the game. Consider that the payoff of P_1 and P_2 is less than $\log_2(2) - \gamma$ before playing the game. Then, the NE strategy profile is (C, C, D), corresponding to $|C^{k^*}| = 2$.

6.3 Discussion

In $\mathcal{C}$-games, each mobile node tries to reduce its consumption of pseudonyms by: (i) changing pseudonyms only when necessary (i.e., low user-centric location privacy level) and (ii) when the other encountered nodes are willing to cooperate as well. In the 2-player $\mathcal{C}$-game, we proved the existence of two pure and one mixed NE. The payoff to both players in (C,C) is higher than in all other outcomes of the game and thus (C,C) is pareto-optimal. Because the payoffs in the n-player scenario are more asymmetric than those of the 2-player game (i.e., with a larger difference across players), a NE with cooperation does not always exist. Still, the All Defection equilibrium always exists because one player cannot gain by cooperating alone. Moreover, it can be easily proved that the NE with cooperation is Pareto-optimal if it exists.

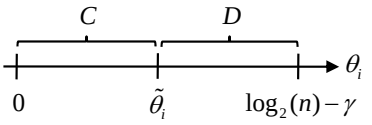

Figure 4: Description of the threshold equilibrium in the 2-player $\mathcal{I}$-game. There is a threshold $\tilde{\theta}_i$ that determines the best response of player i.

7. ANALYSIS OF INCOMPLETE INFORMATION GAME

In this section, we consider games of incomplete information, which we call $\mathcal{I}$-games ($\mathcal{I}$ stands for incomplete information): the players do not know the payoff type of their opponents. The incomplete information assumption better models the knowledge of mobile nodes. The proofs are provided in the Appendix.

7.1 Threshold Equilibrium

In an $\mathcal{I}$-game, players decide their move based on their belief about their opponent's type. Recall that a player's type is defined as: $\theta_i = A_i - \beta_i - \gamma\alpha_i - \gamma$, which defines the payoff immediately before the game. We establish an equilibrium in which each player adopts a strategy based on a threshold: if the type of a player is above a *threshold* $\tilde{\theta}_i$, it defects, otherwise it cooperates. Hence, the space of types is divided into two regions (Figure 4). A player that has $0 \leq \theta_i \leq \tilde{\theta}_i$ always cooperates, whereas a player with $\tilde{\theta}_i < \theta_i \leq \log_2(n) - \gamma$ always defects. With this *threshold equilibrium*, we define the probability of cooperation of node i as:

$$F(\tilde{\theta}_i) = Pr(\theta_i \leq \tilde{\theta}_i) = \int_0^{\tilde{\theta}_i} f(\theta_i) d\theta_i \tag{13}$$

and $1 - F(\tilde{\theta}_i)$ is the probability of defection. The equilibrium strategy at BNE of player i, denoted by $\underline{s}^* = (\tilde{\theta}_1^*; ...; \tilde{\theta}_n^*)$, depends only on the thresholds. In the next section, we obtain the threshold equilibrium for the 2-player $\mathcal{I}$-game.

Remark: In identifying a symmetric BNE with threshold strategies we do not constrain the game so that these are the only strategies available. Rather, we show that a node's best-response is a threshold strategy across all strategies when every other node plays a threshold strategy; i.e., it continues to be a best response even if a node can play a non-threshold strategy, such as playing C for some range of θ_i, then D, then C, and then D again.

7.2 2-player $\mathcal{I}$-Game

Each player predicts the type of its opponent based on the probability distribution $f(\theta_i)$. To determine the threshold values that define a BNE, fix a threshold strategy $\underline{s}_2$ associated with threshold $\tilde{\theta}_2$ for player 2, and define the average payoff to player 1 for C and D, given type θ_1, as

$$E[u_1(C,\underline{s}_2)|\theta_1] = F(\tilde{\theta}_2)(1-\gamma) + (1-F(\tilde{\theta}_2)) \cdot \max(0,(\theta_1-\gamma)) \quad (14)$$

$$E[u_1(D,\underline{s}_2)|\theta_1] = \theta_1, \quad (15)$$

and similarly for player 2. A necessary condition for a threshold equilibrium is that when a player's type is its threshold type it is indifferent between C and D. This is by continuity of payoffs.

So, we can consider the effect of requiring that $E[u_i(C,\underline{s}_{-i})|\tilde{\theta}_i] = E[u_i(D,\underline{s}_{-i})|\tilde{\theta}_i]$ for each player $i \in \{1,2\}$, directly imposing this condition on the threshold types. This yields a system of two non-linear equations on the two variables $\tilde{\theta}_1$ and $\tilde{\theta}_2$. The following lemma establishes that this is also sufficient: solving for thresholds with this property defines a BNE for the 2-player $\mathcal{I}$-game.

LEMMA 3. *The threshold strategy profile $\underline{s}^* = (\tilde{\theta}_1^*, \tilde{\theta}_2^*)$ is a pure-strategy Bayesian Nash equilibrium of the 2-player, incomplete information pseudonym change $\mathcal{I}$-game if*

$$\begin{cases} E[u_1(C,\underline{s}_2^*)|\tilde{\theta}_1^*] = E[u_1(D,\underline{s}_2^*)|\tilde{\theta}_1^*] \\ E[u_2(C,\underline{s}_1^*)|\tilde{\theta}_2^*] = E[u_2(D,\underline{s}_1^*)|\tilde{\theta}_2^*] \end{cases} \quad (16)$$

Theorem 3 guarantees the existence and symmetry of the 2-player $\mathcal{I}$-game BNE. As before, we continue to require $\gamma < 1/2$ to make the 2 player game interesting (so that a player retains non-zero privacy value for more than one period after a successful pseudonym change.) For stating the result we assume continuous type distributions, so that probability density $f(\theta_i) > 0$ for all $\theta_i \in [0, 1-\gamma]$.

THEOREM 3. *The 2-player pseudonym change $\mathcal{I}$-game has All Cooperate and All Defect pure-strategy Bayesian-Nash equilibrium, and every threshold equilibrium $\underline{s}^* = (\tilde{\theta}_1^*, \tilde{\theta}_2^*)$ is symmetric for continuous type distributions.*

In simulations we find an intermediate, symmetric threshold equilibrium in almost all cases, where players don't simply always cooperate or always defect.[3]

To illustrate the results of the theorem we consider the following example. Consider that the distribution on types is uniform, with $\theta_i \sim U(0, 1-\gamma)$, and cumulative probability function $F(\theta_i) = \theta_1/(1-\gamma)$. Looking for an equilibrium with a threshold, $\tilde{\theta}_i^* \geq \gamma$, so that the $\max(0,\cdot)$ term in defining the payoff of the cooperation action can be dropped, we can simplify Eq. (16) and obtain the system of equations: the threshold:

$$\tilde{\theta}_i^* \triangleq 1 - \frac{\gamma}{F(\tilde{\theta}_{-i}^*)}, i = 1,2 \quad (17)$$

Imposing symmetry and solving, we obtain $(\tilde{\theta}_i^*)^2 - \tilde{\theta}_i^* + \gamma(1-\gamma) = 0$ for $i \in \{1,2\}$, which leads to the following solutions:

$$\tilde{\theta}_i^* \in \{\gamma, 1-\gamma\} \quad (18)$$

[3]Note that previous works [17, 48] obtain similar results showing the existence and symmetry of the BNE for this type of games (infinite games of incomplete information).

Recall that we assume $\gamma < 1/2$, so that $\gamma < 1-\gamma$. The solution $\tilde{\theta}_i^* = 1-\gamma$ corresponds to an *All Cooperation* BNE because $\theta_i \leq 1-\gamma$ in a two player game. Looking at the intermediate equilibrium when $\tilde{\theta}_i^* = \gamma$, we see that $E[u_1(C,\underline{s}_2^*)|\theta_1] = F(\tilde{\theta}_2^*)(1-\gamma) + (1-F(\tilde{\theta}_2^*)) \cdot 0 = \tilde{\theta}_2^* = \tilde{\theta}_1^*$ while $E[u_1(D,\underline{s}_2^*)|\theta_1) = \theta_1$, and can confirm that C is the best response for $\theta_1 < \tilde{\theta}_1^*$ and D is the best response for $\theta_1 > \tilde{\theta}_1^*$. By further analysis of Eq. (16) for the case of $\tilde{\theta}_i^* < \gamma$, there are a multiplicity of symmetric threshold equilibrium in this problem, for *any* $\tilde{\theta}_1^* = \tilde{\theta}_2^* < \gamma$, including $(\underline{s}_1^*, \underline{s}_2^*) = (0,0)$ which is the *All Defection* BNE. These results are in line with Theorem 3.

We numerically solve Eq. (16) to find symmetric threshold equilibrium for three different probability distributions (using *fsolve()* in Matlab). We consider the beta distribution $\mathcal{B}(a,b)$, a family of continuous probability distributions defined on the interval $[0,1]$ and parameterized by two positive shape parameters a and b. If $\theta \sim \mathcal{B}(2,5)$, nodes have a small θ with high probability (i.e., long-tail distribution), whereas with $\theta \sim \mathcal{B}(5,2)$, nodes have a large θ with high probability. If $\theta \sim \mathcal{B}(2,2)$, θ is symmetric and centralized around 0.5. Figure 5 shows the BNE $\tilde{\theta}_i^*$ and the related probability of cooperation $F(\tilde{\theta}_i^*)$ as a function of the cost γ. For each distribution of type, we obtain three BNE: $\tilde{\theta}_{i,1}^*$ is an All Defection equilibrium, $\tilde{\theta}_{i,2}^*$ is an intermediate equilibrium, and $\tilde{\theta}_{i,3}^*$ is an All Cooperation equilibrium. With the BNE $\tilde{\theta}_{i,1}^*$ and $\tilde{\theta}_{i,3}^*$, nodes always play the same strategy. With $\tilde{\theta}_{i,2}^*$, we observe that as γ increases, the probability of cooperation $F(\tilde{\theta}_{i,2}^*)$ increases as well, indicating that players should cooperate more when the cost of changing pseudonyms increases. In other words, with a high γ, users care more about the coordination success with others. If γ is small, then the cooperation success becomes less important and nodes become selfish.

The probability of cooperation also depends on the type of Beta distribution. With a lower type distributions $\mathcal{B}(2,5)$, the probability of cooperation at equilibrium is smaller than other distribution types. In other words, selfish nodes cooperate less because whenever they must change pseudonym, they know that the majority of their neighbors also needs to change pseudonym. On the contrary, for $\mathcal{B}(5,2)$, selfish nodes cooperate more to maintain high privacy.

Table 4: Welfare of system $E[u_i]$, fraction of interactions in which a pseudonym is changed FC, and fraction of successful coordinations (CS).

Strategy	$E[u_i]$ | FC | CS		
	$\mathcal{B}(2,5)$	$\mathcal{B}(2,2)$	$\mathcal{B}(5,2)$
$\tilde{\theta}_{i,2}^*$, $\gamma = 0.3$	0.20|0.08|0.84	0.39|0.44|0.50	0.56|0.70|0.58
$\tilde{\theta}_{i,2}^*$, $\gamma = 0.5$	0.15|0.09|0.85	0.29|0.49|0.50	0.46|0.91|0.85
$\tilde{\theta}_{i,2}^*$, $\gamma = 0.7$	0.09|0.08|0.85	0.17|0.49|0.49	0.28|0.91|0.85
Random	$(1-\gamma)/2$ | 0.5 | 0.5		
Socially Opt.	$1-\gamma$ | 1 | 1		

In considering the welfare achieved in the pseudonym change game, we focus on the performance under the intermediate BNE $\tilde{\theta}_{i,2}^*$. This is more interesting to study than the *All Cooperation* or *All Defection* equilibrium. We simulate the 2-player $\mathcal{I}$-game in Matlab. The results are averaged

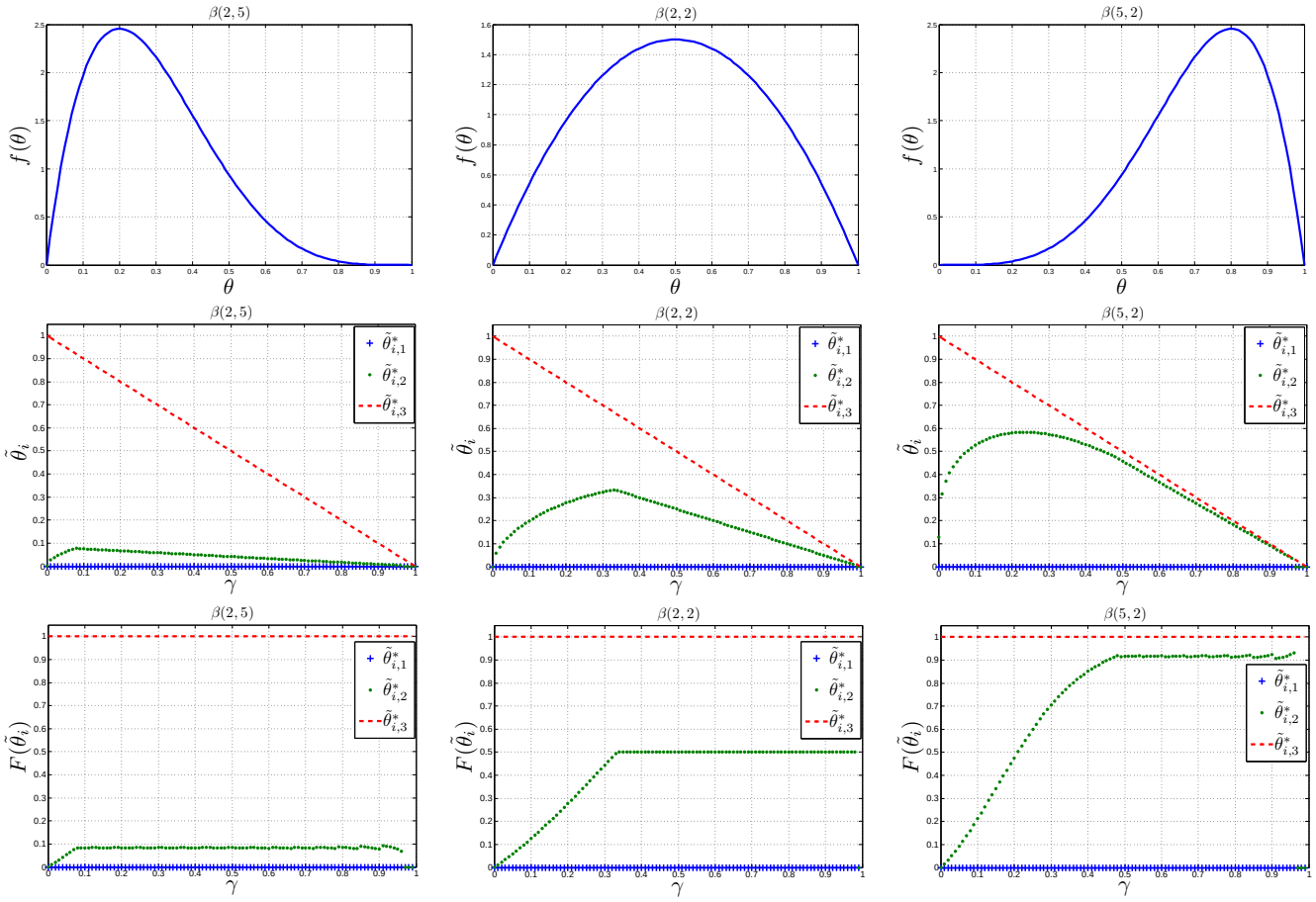

Figure 5: Probability distribution of user types $f(\theta)$, threshold $\tilde{\theta}_i^*$, and probability of cooperation $F(\tilde{\theta}_i^*)$ at the equilibrium as a function of γ for different distributions of type: $\beta(2,5)$, $\beta(2,2)$, and $\beta(5,2)$. For each type distribution, there are three BNE: $\tilde{\theta}_{i,1}^*$ corresponds to All Defection, $\tilde{\theta}_{i,3}^*$ to All Cooperation, and $\tilde{\theta}_{i,2}^*$ is an intermediate equilibrium. As the cost γ of changing pseudonyms increases, $\tilde{\theta}_2^*$ approaches $\tilde{\theta}_1^*$, meaning that the probability of cooperation increases.

over 1000 simulations. We consider three metrics: (i) The welfare of the system defined as the average achieved utility, $E[u_i]$ of the nodes; (ii) The fraction of interactions in which a pseudonym is changed FC; and (iii) The fraction of successful coordination between nodes, CS (i.e., nodes play the same action). We compare the BNE performance with a *random* strategy, in which all nodes choose their threshold randomly, and to the *socially-optimal* strategy, which is *All Cooperation*.

We observe that the welfare achieved in the BNE is less than with the socially-optimal strategy and in general similar to that of the random strategy. The difference with the random strategy is particularly large for $\mathcal{B}(5,2)$ because the probability of cooperation is then larger than that of the random strategy. It is informative to consider the ratio of welfare in the BNE with that at the socially-optimal, by analogy to the price of anarchy (which considers the performance of the worst-case NE [41]). This ratio provides a measure of the cost of non-cooperative behavior. For example in Table 4 for $\mathcal{B}(2,2)$ and $\gamma = 0.3$, we have $0.33/0.70 = 0.47$ meaning that the system performance is degraded by 53%. We notice that the system performance is only degraded by 17% in the case of $\gamma = 0.7$, showing that nodes are less selfish when the cost of a pseudonym change is large. The cost FC in Table 4 shows the fraction of interactions in which a pseudonym is changed. We observe that in general less pseudonyms are changed with $\tilde{\theta}_{i,2}^*$ (30% decrease with respect to the random strategy when $\gamma = 0.3$) showing that less pseudonyms are needed.

7.3 n-player $\mathcal{I}$-Game

Assume $n \leq N$ players meet at time t and take part in a pseudonym change $\mathcal{I}$-game. Let $Pr(K = k)$ be the probability that k nodes cooperate. We can again obtain the thresholds that define a BNE in the n-player game by comparing the average payoff of cooperation with that of defection, now defined as:

$$E[u_i(C, \underline{s}_{-i})] = \sum_{k=0}^{n-1} Pr(K = k) u_i(C, \underline{s}_{-i})$$

$$E[u_i(D, \underline{s}_{-i})] = u_i^-$$

By a similar argument to that for Lemma 3, a BNE $\underline{s}^* =$

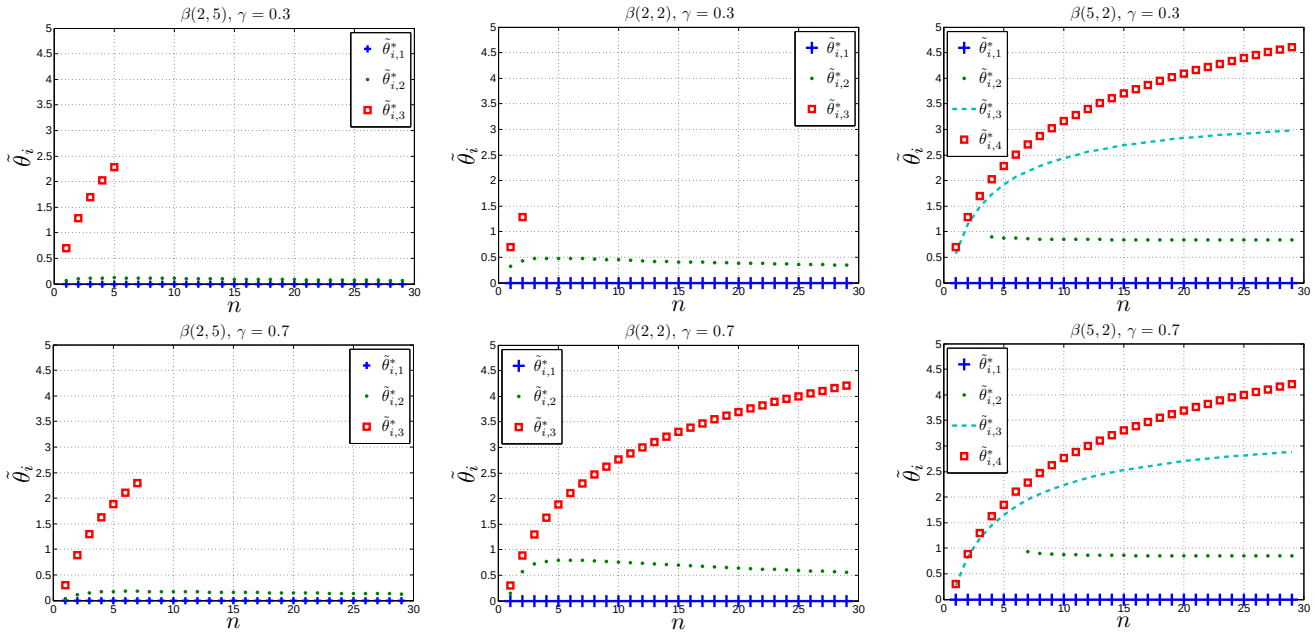

Figure 6: Threshold $\tilde{\theta}^*_i$ at the equilibrium as a function of n for different values of γ and distributions of type: $\beta(2,5)$, $\beta(2,2)$, and $\beta(5,2)$. For each type distribution, the number of BNE changes depending on the cost γ.

$(\tilde{\theta}^*_1; \cdots; \tilde{\theta}^*_n)$ can be obtained as the solution to the following system of n non-linear equations for the n variables $\tilde{\theta}_i$:

$$\sum_{k=0}^{n-1} Pr(K=k) u_i(C, \underline{s}_{-i}) = u_i^-, \quad i = 1, 2, \cdots, n \qquad (19)$$

We denote the probability of cooperation $q_i = F(\tilde{\theta}_i)$. Assume that the thresholds $\tilde{\theta}^*_i$ are all equal: We obtain $q_i = q$ and thus have a symmetric equilibrium. Consequently, the probability that k nodes cooperate is $Pr(K = k) = \binom{n}{k} q^k (1-q)^{n-k}$. For example, consider the limit values of q:

- If $q \to 0$, then $\tilde{\theta}^*_i = 0$, $Pr(K > 0) = 0$ and $Pr(K = 0) = 1$. In other words, the All Defection equilibrium exists.
- If $q \to 1$, then $\tilde{\theta}^*_i = 1$, $Pr(K < n-1) = 0$ and $Pr(K = n-1) = 1$. In other words, the All Cooperation equilibrium occurs when $\log_2(n) - \gamma > u_i^-$ for all nodes i.

For intermediate values of q, we numerically derive the thresholds $\tilde{\theta}^*_i$ by solving Eq. (19) with Matlab (Figure 6). For $\gamma = 0.3$, we observe that with a higher density of nodes n, $\tilde{\theta}^*_{i,2}$ decreases, meaning that players cooperate with a lower probability. Similarly, $\tilde{\theta}^*_{i,3}$ disappears for large vales of n, meaning that Always Cooperation is not a BNE anymore. Yet in the case of $\beta(5,2)$, the All Cooperation equilibrium $\tilde{\theta}^*_{i,4}$ persists. The reasons is that with such a distribution of types, selfish nodes need to cooperate more. For a larger value $\gamma = 0.7$, we observe a similar behavior. Note that with $\beta(5,2)$ an additional threshold equilibrium, denoted by $\tilde{\theta}^*_{i,3}$, appears in which nodes cooperate more when n increases. Moreover, All Cooperation equilibrium survives longer when γ increases.

7.4 Discussion

In summary, in $\mathcal{I}$-games, we first prove analytically the existence and symmetry of BNE in 2-player games and then obtain numerically three BNE for each possible distribution of type. We observe that the intermediate BNE $\tilde{\theta}^*_{i,2}$ reduces the number of pseudonyms used (FC in Table 4) and achieves high level of privacy. However, non-cooperative behavior affects the achievable location privacy. In particular, we notice that a larger n encourages selfish nodes not to cooperate (Figure 6) In contrast, when the cost γ of changing pseudonym is large, we observe that selfish nodes cooperate more, meaning that a high cost of pseudonyms provides an incentive to cooperate. In summary, even with incomplete information, it is possible to find an equilibrium that achieves high location privacy, while reducing the number of used pseudonyms.

8. LOCATION PRIVACY PROTOCOL

As discussed in Section 4, several mobile nodes can coordinate a pseudonym change with the Swing protocol [43]. In the Swing protocol, any node can start the pseudonym change by broadcasting an initiation message. Usually, nodes changing speed and/or direction will initiate the protocol if there is at least another node in proximity. Mobile nodes receiving the initiation message stop communicating for a silent period defined in the initiation message and decide whether to change pseudonym.

In the Swing protocol, the decision of mobile nodes (to cooperate or not) exclusively depends on their user-centric level of location privacy compared to a fixed threshold. In other words, the cost of changing pseudonym and the probability of cooperation of the neighbors are not considered. Our game-theoretic evaluation allows us to design a more sophisticated protocol - the PseudoGame protocol - that extends the Swing protocol to consider optimal strategies of mobile nodes in a non-cooperative environment. The Pseu-

doGame protocol is based on our results for n-player $\mathcal{I}$-games in Section 7.

Similar to [43], we assume that mobile nodes move in the network with speed in the range $[\underline{s}_{min}, \underline{s}_{max}]$. The nodes can choose a silent period in the range $[sp_{min}, sp_{max}]$. The duration of the silent period is attached to the initiation message. When a node is expected to change its velocity within sp_{max} time steps, the node sends the initiation message and the PseudoGame protocol is started. It lasts at most $(sp_{max} + 1)$ time steps.

All nodes in proximity that receive the initiation message use the PseudoGame protocol if the authenticity of the initiation message is verified. Their decision to change pseudonym is influenced by the number of neighbors and their probability of cooperation (related to the distribution of user types $f(\theta_i)$). As described in Protocol 1 for any node i, the PseudoGame protocol assists mobile nodes in selecting the BNE strategy. In summary, after receiving the initiation message, the nodes calculate the equilibrium thresholds using their location privacy level, the estimated number of neighbors, and their belief $f(\theta_i)$. The PseudoGame protocol extends the Swing protocol by computing the optimal threshold to determine when to change pseudonym.

Protocol 1 PseudoGame.

Require: Node i knows the probability distribution $f(\theta)$
Require: The current location privacy of node i is u_i^-
if (Change of velocity within sp_{max}) & (At least one neighbor) **then**
  Broadcast initiation message to change pseudonym.
  Goto 6
else
  if (Receive Initiation message) & (message is valid) **then**
    $n \Leftarrow estimate(n)$ //Number of neighbors
    Calculate $\tilde{\theta}_i^*$ as solution of $\sum_{k=0}^{n-1} Pr(K=k) u_i(C, \underline{s}_{-i}) - u_i^- = 0$ wrt $\tilde{\theta}_i$, where $Pr(K=k) \Leftarrow \binom{n}{k} q^k (1-q)^{n-k}$ and $q \Leftarrow \int_0^{\tilde{\theta}_i} f(\theta_i) d\theta_i$
    if $u_i^- \leq \tilde{\theta}_i^*$ **then**
      Play C
      Comply with silent period sp_{max}
    else
      Play D
  else
    Keep pseudonym

9. CONCLUSION

We have considered the problem of selfishness in location privacy schemes based on pseudonym changes. We introduced a user-centric model of location privacy to measure the evolution of location privacy over time. To evaluate the strategic behavior of mobile nodes, we proposed a game-theoretic model, the *pseudonym change game*. We first analyzed the n-player scenario with complete information and obtained NE strategy profiles. Then, using Bayesian game theory, we investigated the equilibria in the incomplete information game and derived the equilibrium strategies for each node. In other words, we derive equilibria to achieve location privacy in a non-cooperative environment. A particularly interesting result is that when the cost of pseudonyms is large, selfish nodes care more about the successful unfolding of the game and thus improve the achievable location privacy in the system. This work is the first step towards a deeper understanding of the effect of non-cooperative behavior in location privacy schemes. For future work, we intend to evaluate our model in realistic mobile scenarios and measure the achievable location privacy.

Acknowledgments

We would like to thank Tansu Alpcan, Mario Cagalj, Mark Felegyhazi, Zarko Milosevic, and Marcin Poturalski for their insights and suggestions on earlier versions of this work, and the anonymous reviewers for their helpful feedback. Special thanks go to Catherine Meadows for shepherding the paper.

10. REFERENCES

[1] http://www.aka-aki.com/.
[2] http://www.csg.ethz.ch/research/projects/Blue_star.
[3] http://reality.media.mit.edu/serendipity.php.
[4] IEEE P1609.2 Version 1. Standard for wireless access in vehicular environments - security services for applications and management messages. In *development*, 2006.
[5] A. Acquisti, R. Dingledine, and P. Syverson. On the economics of anonymity. In *Financial Cryptography*, 2003.
[6] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46–55, 2003.
[7] A. R. Beresford and F. Stajano. Mix zones: User privacy in location-aware services. In *PerSec*, 2004.
[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *MobiCom*, 2008.
[9] L. Buttyan, T. Holczer, and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *ESAS*, 2007.
[10] L. Buttyan and J.-P. Hubaux. *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2008.
[11] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux. Efficient and robust pseudonymous authentication in VANET. In *VANET*, 2007.
[12] J. Camenisch and E. Van Herreweghen. Design and implementation of the Idemix anonymous credential system. In *CCS*, 2002.
[13] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to win the clone wars: efficient periodic n-times anonymous authentication. In *CCS*, 2006.
[14] J. Camenish, S. Hohenberger, and M. O. Pedersen. Batch verification of short signatures. In *EUROCRYPT*, volume 4515, pages 246–263, 2007.
[15] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2), 1981.
[16] D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT*, 1991.
[17] S.F. Cheng, D.M. Reeves, Y. Vorobeychik, and W.P. Wellman. Notes on equilibria in symmetric games. In *Workshop on Game-Theoretic and Decision-Theoretic Agents*, 2004.
[18] R. Cooper. *Coordination Games*. Cambridge Univ. Press, 1998.

[19] B. Danev and S. Capkun. Transient-based identification of wireless sensor nodes. In *IPSN*, 2009.

[20] K. Fall. A delay-tolerant network architecture for challenged internets. In *SIGCOMM*, 2003.

[21] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Randwyk, and D. Sicker. Passive data link layer 802.11 wireless device driver fingerprinting. In *USENIX*, 2006.

[22] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P. Hubaux. Mix zones for location privacy in vehicular networks. In *WiN-ITS*, 2007.

[23] J. Freudiger, M. Raya, and J.-P. Hubaux. Self-organized anonymous authentication in mobile networks. In *SECURECOMM*, 2009.

[24] J. Freudiger, R. Shokri, and J.-P. Hubaux. On the optimal placement of mix zones. In *PETS*, 2009.

[25] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 1991.

[26] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *MobiSys*, 2008.

[27] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. *Mob. Netw. Appl.*, 2005.

[28] J. Hall, M. Barbeau, and E. Kranakis. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *CIIT*, 2004.

[29] J. Halpern and V. Teague. Rational secret sharing and multiparty computation: extended abstract. In *STOC*, pages 623–632, 2004.

[30] J. Harsanyi. Games with incomplete information played by Bayesian players. *Management Science*, 1967.

[31] H. Hartenstein and K. Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, 46(6), 2008.

[32] B. Hoh and M. Gruteser. Protecting location privacy through path confusion. In *SECURECOMM*, pages 194–205, 2005.

[33] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson. Virtual trip lines for distributed privacy-preserving traffic monitoring. In *MobiSys*, pages 15–28, 2008.

[34] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*, 5(4):38–46, 2006.

[35] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady. Preserving privacy in GPS traces via path cloaking. In *CCS*, 2007.

[36] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing wireless location privacy using silent period. In *ECNC*, 2005.

[37] L. Huang, K. Matsuura, H. Yamane, and K. Sezako. Towards modeling wireless location privacy. In *PET*, 2005.

[38] S. Izmalkov, S. Micali, and M. Lepinski. Rational secure computation and ideal mechanism design. In *FOCS*, pages 585–595, 2005.

[39] J. Katz. Bridging game theory and cryptography: Recent results and future directions. In *TCC*, 2008.

[40] T. Kohno, A. Broido, and K.C. Claffy. Remote physical device fingerprinting. *TDSC*, 2, 2005.

[41] E. Koutsoupias and C. Papadimitriou. Worst-case equilibria. In *STACS*, 1999.

[42] J. Krumm. Inference attacks on location tracks. In *Pervasive*, 2007.

[43] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran. Swing & swap: User centric approaches towards maximizing location privacy. In *WPES*, 2006.

[44] J. Nash. Non-cooperative games. *Annals of Mathematics*, 1951.

[45] S. J. Ong, D. C. Parkes, A. Rosen, and S. Vadhan. Fairness with an honest minority and a rational majority. In *Sixth Theory of Cryptography Conference (TCC)*, 2009.

[46] B. Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *SECURECOMM*, 2007.

[47] M. Raya, M. H. Manshaei, M. Felegyhazi, and J.-P. Hubaux. Revocation Games in Ephemeral Networks. In *CCS*, 2008.

[48] D. M. Reeves and M.P. Wellman. Computing best-response strategies in infinite games of incomplete information. In *Uncertainty in artificial intelligence*, pages 470–478, 2004.

[49] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *ASIACRYPT*, 2001.

[50] K. Sampigethaya, M. Li L. Huang, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing location privacy for VANET. In *ESCAR*, 2005.

[51] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos. Impact of pseudonym changes on geographic routing in VANETs. In *ESAS*, 2006.

[52] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In *PET*, 2002.

[53] O. Ureten and N. Serinken. Wireless security through RF fingerprinting. *Canadian J. Elect. Comput. Eng.*, 32, 2007.

[54] H. Varian. Economic aspects of personal privacy. White paper, UC Berkeley, 1996.

[55] S. Vasudevan, J. Kurose, and D. Towsley. On neighbor discovery in wireless networks with directional antennas. In *Infocom*, 2005.

[56] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-to-vehicle safety messaging in DSRC. In *VANET*, 2004.

APPENDIX

A. PROOF OF THEOREM 1

PROOF. We first prove the existence of the pure-strategy NE. (C, C) is a NE since $1-\gamma > u_i^-$ for $i = 1, 2$. Similarly (D, D) is a NE because $u_i^- > u_i^- - \gamma$ for $i = 1, 2$. For the mixed strategy NE, let x_i denote the probability of cooperation of u_i. The average payoff of player 1 is:

$$\begin{aligned} u_1(x_1, x_2) &= x_1x_2(1-\gamma) + x_1(1-x_2)(u_1^- - \gamma) \\ &\quad +(1-x_1)x_2u_1^- + (1-x_1)(1-x_2)u_1^- \\ &= x_1x_2(1-u_1^-) - \gamma x_1 + u_1^- \end{aligned}$$

The payoff is maximized for:

$$\frac{\partial}{\partial x_1} u_1(x_1, x_2) = x_2(1-u_1^-) - \gamma = 0$$

which gives $x_2 = \frac{\gamma}{1-u_1^-}$ and by symmetry $x_1 = \frac{\gamma}{1-u_2^-}$. □

B. PROOF OF LEMMA 1

PROOF. All Defection is a NE, because if any player P_i unilaterally deviates from D and cooperates, then its payoff is equal to $u_i^- - \gamma$, which is always smaller than its payoff of defection u_i^-. □

C. PROOF OF LEMMA 2

PROOF. First, if any $P_i \in C^{k^*}$ unilaterally deviates from cooperation to defect, then its payoff u_i^- is smaller than $\log_2(|C^{k^*}|) - \gamma$. Now let D^{n-k^*} be the set of all nodes except those in C^{k^*}. As C^{k^*} is the largest group of nodes where $\log_2(|C^{k^*}|) - \gamma > u_i^-$, no mobile node in D^{n-k^*} can increase its payoff by joining the set of nodes in C^{k^*}. Hence, none of the nodes can unilaterally change its strategy to increase its payoff and $\underline{s}^*$ is a NE when $|C^{k^*}| > 1$. We show by contradiction that the equilibrium is unique. Consider $C^{k_1^*}$ and $C^{k_2^*}$ such that $\forall P_i \in C^{k_j^*}$, $\log_2(|C^{k_j^*}|) - \gamma > u_i^-$ for $j = 1, 2$. There always exists a $C^{k^*} = C^{k_1^*} \cup C^{k_2^*}$ such that $\forall P_i \in C^{k^*}$, $\log_2(|C^{k_1^*}| + |C^{k_2^*}|) - \gamma > u_i^-$ because $\log_2(|C^{k_1^*}| + |C^{k_2^*}|) > \log_2(|C^{k_j^*}|)$ for $j = 1, 2$ and users will merge to the larger group of C^{k^*}. Thus $\underline{s}^*$ is the unique NE. □

D. PROOF OF LEMMA 3

PROOF. Fix player 2's strategy to threshold $\tilde{\theta}_2^*$ and consider player 1 with type $\theta_1 < \tilde{\theta}_1^*$. We have $E[u_1(C, \underline{s}_2^*)|\tilde{\theta}_1^*] = E[u_1(D, \underline{s}_2^*)|\tilde{\theta}_1^*]$. Now, $E[u_1(D, \underline{s}_2^*)|\tilde{\theta}_1^*] - E[u_1(D, \underline{s}_2^*)|\theta_1] = \tilde{\theta}_1^* - \theta_1 \geq (1 - F(\tilde{\theta}_2^*))(\tilde{\theta}_1^* - \theta_1) \geq E[u_1(C, \underline{s}_2^*)|\tilde{\theta}_1^*] - E[u_1(C, \underline{s}_2^*)|\theta_1]$, where the first inequality follows because $F(\tilde{\theta}_2^*) \geq 0$. Therefore, the drop in payoff from D relative to with type $\tilde{\theta}_1^*$ is at least that from C and a best-response for the player is to play C. Now consider player 1 with type $\theta_1 > \tilde{\theta}_1^*$. By a similar argument, we have $E[u_1(D, \underline{s}_2^*)|\theta_1] - E[u_1(D, \underline{s}_2^*)|\tilde{\theta}_1^*] = \theta_1 - \tilde{\theta}_1^* \geq (1 - F(\tilde{\theta}_2^*))(\theta_1 - \tilde{\theta}_1^*) \geq E[u_1(C, \underline{s}_2^*)|\theta_1] - E[u_1(C, \underline{s}_2^*)|\tilde{\theta}_1^*]$, and the increase in payoff for D is greater than the increase in utility for C and the player's best response is to play D. □

E. PROOF OF THEOREM 3

PROOF. To see that *All Defection* is a BNE with thresholds $\tilde{\theta}_1^* = \tilde{\theta}_2^* = 0$, simply note that $E[u_1(C, \underline{s}_2^*)|\tilde{\theta}_1^* = 0] = 0 = E[u_1(D, \underline{s}_2^*)|\tilde{\theta}_1^* = 0]$ and appeal to Lemma 3. Similarly, to see that *All Cooperation* is a BNE consider thresholds $\tilde{\theta}_1^* = \tilde{\theta}_2^* = 1 - \gamma$, for which $F(\tilde{\theta}_1^*) = F(\tilde{\theta}_2^*) = 1$ since $\theta_i \in [0, 1-\gamma]$. With this, we have $E[u_1(C, \underline{s}_2^*)|\tilde{\theta}_1^* = 1-\gamma] = 1 - \gamma = E[u_1(D, \underline{s}_2^*)|\tilde{\theta}_1^* = 1-\gamma]$.

Second, we prove by contradiction the symmetry of any threshold equilibrium. Assume without loss of generality that there exists an asymmetric equilibrium $\underline{s}_2^* = (\tilde{\theta}_1; \tilde{\theta}_2)$, such that $\tilde{\theta}_1 = \tilde{\theta}_2 + \epsilon$, where ϵ is a strictly positive number. Adopt short hand F for $F(\tilde{\theta}_2^*)$ and F_ϵ for $F(\tilde{\theta}_2^* + \epsilon)$. Then, for this to be a BNE we require by Eq. (19) that

$$F \cdot (1-\gamma) + (1-F)\max(0, \tilde{\theta}_2^* + \epsilon - \gamma) - \tilde{\theta}_2 - \epsilon = 0 \quad (20)$$

$$F_\epsilon \cdot (1-\gamma) + (1-F_\epsilon)\max(0, \tilde{\theta}_2^* - \gamma) - \tilde{\theta}_2^* = 0 \quad (21)$$

Three cases can be identified considering the values of $\tilde{\theta}_2$, ϵ, and γ.

(Case 1) $\tilde{\theta}_2^* \leq \gamma - \epsilon$. By equating Eq. (20) and (21) and simplification, we have

$$F(1-\gamma) - \epsilon = F_\epsilon \cdot (1-\gamma) \quad (22)$$

$$\Rightarrow \ \epsilon = F \cdot (1-\gamma) - F_\epsilon \cdot (1-\gamma) < 0, \quad (23)$$

since $F_\epsilon > F$ because the type distribution is continuous with $f(\theta_i) > 0$ everywhere. This is a contradiction.

(Case 2) $\gamma - \epsilon < \tilde{\theta}_2^* < \gamma$. By equating Eq. (20) and (21) and simplification, we have

$$F \cdot (1 - \tilde{\theta}_2^*) + \tilde{\theta}_2^* - \gamma - F\epsilon = F_\epsilon \cdot (1-\gamma) \quad (24)$$

$$\Rightarrow \epsilon = \frac{F \cdot (1 - \tilde{\theta}_2^*) - F_\epsilon \cdot (1-\gamma) - (\gamma - \tilde{\theta}_2^*)}{F} \quad (25)$$

Now, we have $F \cdot (1 - \tilde{\theta}_2^*) - F_\epsilon \cdot (1-\gamma) < F \cdot (1 - \tilde{\theta}_2^*) - F \cdot (1-\gamma) = F \cdot (\gamma - \tilde{\theta}_2^*) < \gamma - \tilde{\theta}_2^*$, where the first inequality follows because $F_\epsilon > F$ and the second inequality because $\tilde{\theta}_2^* < \gamma$, by assumption of this case. From this it follows that $\epsilon < 0$ since $F > 0$, and a contradiction.

(Case 3) $\gamma \leq \tilde{\theta}_2^*$. By equating Eq. (20) and (21) and simplification, we have

$$F \cdot (1 - \tilde{\theta}_2^*) - F\epsilon = F_\epsilon \cdot (1 - \tilde{\theta}_2^*) \quad (26)$$

$$\Rightarrow \ \epsilon = \frac{F \cdot (1 - \tilde{\theta}_2^*) - F_\epsilon \cdot (1 - \tilde{\theta}_2^*)}{F} < 0, \quad (27)$$

where the inequality holds because $F < F_\epsilon$. This is a contradiction. □