Non-Cooperative Location Privacy

Non-Cooperative Location Privacy

Julien Freudiger[1], Mohammad Hossein Manshaei[2], Jean-Pierre Hubaux[1], and David C. Parkes[3]
[1] EPFL, Switzerland
[2] Isfahan University of Technology, Iran
[3] Harvard University, USA

***Abstract*—In mobile networks, authentication is a required primitive for most security protocols. Unfortunately, an adversary can monitor pseudonyms used for authentication to track the location of mobile nodes. A frequently proposed solution to protect *location privacy* suggests that mobile nodes collectively change their pseudonyms in regions called mix zones. This approach is costly. Self-interested mobile nodes might thus decide not to cooperate and jeopardize the achievable location privacy. In this paper, we analyze non-cooperative behavior of mobile nodes by using a game-theoretic model, where each player aims at maximizing its location privacy at a minimum cost. We obtain Nash equilibria in static n-player complete information games. As in practice mobile nodes do not know their opponents' payoffs, we then consider static incomplete information games. We establish that symmetric Bayesian-Nash equilibria exist with simple threshold strategies. By means of numerical results, we predict behavior of selfish mobile nodes. We then investigate dynamic games where players decide to change their pseudonym one after the other and show how this affects strategies at equilibrium. Finally, we design protocols - PseudoGame protocols - based on the results of our analysis and simulate their performance in vehicular network scenarios.**

***Index Terms*—Security and Privacy Protection, Mobile Computing, Network Protocols**

I. Introduction

The growing popularity of Bluetooth, WiFi in ad hoc mode [3] and other similar techniques is likely to fuel the adoption of peer-to-peer wireless communications. Corporations are developing wireless peer-to-peer technologies such as Nokia Instant Community [5] and Qualcomm FlashLinQ [29]. In addition to classic infrastructure-based communications, mobile devices can communicate directly with each other in an ad hoc wireless fashion. Such communications dramatically increase mobile devices' *awareness* of their environment, enabling a new breed of context-aware applications.

The integration of peer-to-peer wireless communications into mobile devices brings new security challenges, due to their mobile and ad hoc nature. Wireless communications are inherently dependent on geographic proximity: mobile devices detect each other's presence by periodically broadcasting beacon messages. These messages include *pseudonyms* such as public keys in order to identify communicating parties, route communications and secure communications. Much to the detriment of privacy, external parties can monitor pseudonyms in broadcasted messages in order to track the locations of mobile devices, thus jeopardizing *location privacy*.

There are multiple solutions to anonymously authenticate mobile devices. One of the most popular solutions is the *multiple pseudonym* approach [7] suggested in the context of Internet communications: it assigns a set of asymmetric key pairs to every node that are used alternatively.

A change to pseudonym by an isolated device in a wireless network can be trivially identified by an external party observing transmitted messages. Hence, a change of pseudonym should be spatially and temporally coordinated among mobile devices [4], i.e., a collective effort by neighboring devices. One solution [6] consists in changing pseudonyms periodically, at a pre-determined frequency. This works if at least two mobile nodes change their pseudonyms in proximity, a rarely met condition . Base stations can be used as coordinators to synchronize pseudonym changes [20], but this solution requires help from the infrastructure. The approach in [14] enables mobile nodes to change their pseudonyms 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 [4], [11], [12] coordinates pseudonym changes by forcing mobile nodes to change their pseudonyms within pre-determined regions called *mix zones*. This approach however lacks flexibility and is prone to attacks because a central authority fixes mix zone locations and must shared them with mobile nodes.

Several researchers advocate the use of a distributed approach [19], [20], [22], 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 infrastructure.

But pseudonym changes are costly, which can cause distributed approaches to fail. First, a pseudonym change causes considerable overhead, reducing networking performance, e.g., routing algorithms must update their routing tables [26]. Second, given the cost of pseudonym generation and management, pseudonyms can become a scarce resource if changed frequently. Third, mix zones impose limits on the services available to mobile users: in order to protect against spatial correlation of location traces, nodes in the mix zone are usually not allowed to communicate [19]. 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 [4], a selfish mobile node might decide to *not* change its pseudonym in settings offering low location privacy guarantees.

In this paper, we investigate strategic aspects of location privacy in mobile networks. In contrast with existing approaches, we consider *rational* mobile nodes that locally decide whether

to change their pseudonyms. Although selfish behavior can reduce the cost of location privacy, it can also jeopardize the welfare achieved with a location privacy scheme. We investigate whether the multiple pseudonym approach achieves location privacy in non-cooperative scenarios. We propose a *user-centric location privacy model* that captures the evolution of the location privacy level of mobile nodes over time and helps them determine when to change pseudonyms. We then define a game-theoretic model - the *pseudonym change game* - that models the decisions of mobile nodes in a mix zone.

We first analyze the *static* game with *complete information* (i.e., every node knows the user-centric location privacy level of other nodes) and obtain both pure and mixed Nash equilibria [23]. We show that nodes should either cooperate when there is a sufficient number of neighbors with low privacy, or defect. Then, because mobile nodes do not have good knowledge about payoffs of other nodes, we study, using a Bayesian approach [15], the *incomplete information* scenario. We evaluate the strategic behavior of mobile nodes and derive Bayesian Nash equilibria for a class of threshold strategies, where nodes decide whether to change their pseudonyms based on a comparison of their privacy level to a threshold value. We find a symmetric equilibrium where all nodes cooperate with the same probability. We then analyze a *dynamic* version of the game and show that it copes better with uncertainty. Finally, we design PseudoGame protocols that implement pseudonym change strategies, and evaluate them.

II. System and Threat Model

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

a) System Model: We study a network where mobile nodes are autonomous entities equipped with WiFi or Bluetooth-enabled devices and 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 [16], a delay tolerant network [10], or a network of directly communicating hand-held devices [29].

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 devices. In line with the multiple pseudonym approach, 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. 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 assume that mobile devices automatically exchange information (unbeknownst to their users, such as beacon messages in VANETs) as soon as they are in communication range of each other. Although our evaluation is independent from the communication protocol, we make 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 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 verifies the legitimacy of the sender by checking the certificate of the public key of the sender. After this, i verifies the signature of the beacon message. Subsequently, if confidentiality is required, a security association is established (e.g., with Diffie-Hellman).

b) 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 the worst case, a *global* adversary $\mathcal{A}$ obtains complete coverage and tracks nodes throughout the entire network, by placing eavesdropping devices in the network.

$\mathcal{A}$ collects identifying information (i.e., pseudonyms) from the 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, in preventing other parties from learning a node's past and current location [4]. Finally, we assume that the key-pair generation and distribution process cannot be altered or controlled by the adversary.

III. User-Centric Location Privacy

We evaluate the location privacy provided by multiple pseudonyms and propose a user-centric model of location privacy to capture achievable location privacy over time.

A. Location Privacy

There are several techniques to mitigate the tracking of mobile nodes. We consider the use of *multiple pseudonyms*: over time, mobile nodes change 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 pseudonyms, the old pseudonym expires and is removed from the node's memory. In other words, two nodes cannot use the same pseudonyms at the same time.

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/encrypted mix zones [11], [19], [22], (ii) a mobile proxy [25], or (iii) regions where the adversary has no coverage [6]. 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 change pseudonyms 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, one node among a group of $n(t)$ mobile nodes in proximity can initiate the pseudonym change using the one-round Swing protocol [22]: it 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.

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 [4], [22]. 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 [27], the location privacy level of node i involved in a successful pseudonym change at time T is computed as the adversary's uncertainty:

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

The achievable location privacy depends on both the number of nodes $n(T)$ and the unpredictability $p_{d|b}$ of their whereabouts in the mix zone. 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 $log_2(n(T))$. 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.

The adversary could be physically present in mix zones to visually observe mobile nodes and/or prevent mix zone creation. We rule out this threat because of its high cost. The adversary could also strategically place sniffing devices. Previous work investigated this [21] and showed how mobile nodes could strategically retaliate. Finally, the adversary could physically follow mobile nodes across the network. Mix zones (as any other privacy-preserving mechanism) are useless against such a threat and we consider it out of scope.

B. User-Centric Model

The entropy measures the location privacy achieved in specific mix zones at some point in time. However, location privacy needs of individuals vary depending on time and location. It is thus desirable to protect location privacy in a user-centric manner, such that each user can decide when and where to protect its location privacy. We consider a *user-centric* model of location privacy, where each mobile node locally monitors its location privacy over time [17], [18], [22].

A network-wide metric could evaluate the average entropy in the network but might ignore that some nodes have a low location privacy level and are traceable for long distances. As a user-centric approach captures the evolution of location privacy of users over time, mobile nodes can evaluate the distance over which they are potentially tracked by an adversary (i.e., the *distance-to-confusion* [17]) and can act upon it by deciding whether and when to change its pseudonym.

With a user-centric model, mobile nodes can request a pseudonym change from other nodes in proximity if 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.

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:

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

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 location privacy is null). 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 next to change pseudonyms.[1] 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. With this modeling assumption, 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.

C. Pseudonym Cost

Pseudonyms are costly to manage and to acquire because they are a scarce resource and may require contacting a central authority for refill. Similarly, routing [26] becomes difficult as it requires frequent updates of routing tables. In addition, while traversing silent mix zones, mobile nodes cannot communicate and thus momentarily lose access to services. We take into account the various costs involved in changing pseudonym in parameter γ 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. The cost can be seen as the minimum privacy gain that

[1] In user-centric models, users are not involved: devices take decisions on their behalf.

compensates for the effort of a pseudonym change. Hence, we express the cost in privacy units (bits), causing a decrease in the achieved privacy.

IV. Pseudonym Change Games

We present the game-theoretic aspects of achieving location privacy with multiple pseudonyms in a rational environment. We refer to the game-theoretic model as the *pseudonym change game* G. The key aspect of the game-theoretic analysis is to consider costs and the potential location privacy gain when making a pseudonym change decision.

Considering the cost of pseudonym and the available location privacy gain (upperbounded by the density of nodes and their locations unpredictability), the user-centric location privacy level might encourage selfish mobile nodes to change pseudonym and obtain a satisfactory location privacy level, as long as other nodes are also changing.

Nodes may also delay their decision in order to try to find the better conditions that maximize the effectiveness of pseudonym changes. Therefore, we investigate whether location privacy can emerge in a non-cooperative system despite the cost of changing pseudonym, differentiated privacy levels, and the need for coordination to achieve a confusion point.

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 both as a *static* and *dynamic* game depending on the constraints on the pseudonym change protocol. The static version of the game captures protocols in which nodes are unable to sense their wider environment when deciding whether or not to change its pseudonym, e.g., 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 pseudonyms without knowing the decision of other nodes in proximity. The dynamic version of the game models protocols in which nodes do not start/stop transmitting at the same time, and may thus observe each others messages before making their decision.

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).

1) 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 can adopt a neighbor discovery protocol [28].

2) Strategy: Each player has two 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 $\mathcal{S} = \{S_i\}_{i=1}^{n(t)}$.

3) 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 continues to decrease 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:
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 $(s_i = C) \wedge (n_C(s_{-i}) = 0)$,

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

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

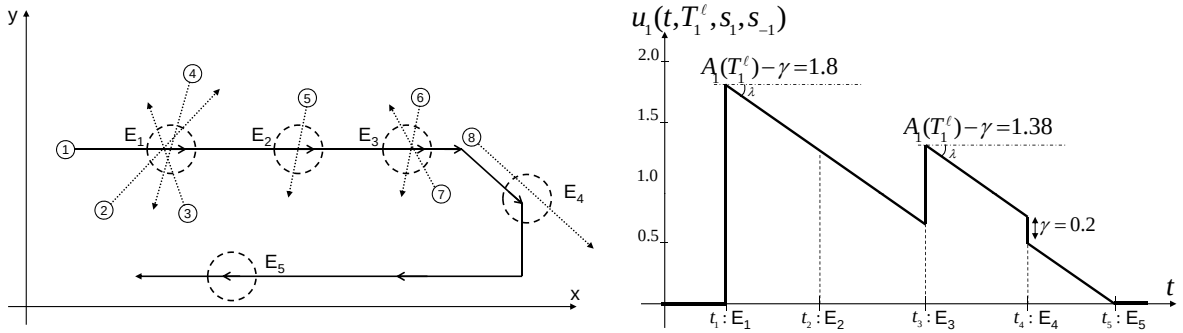
If $(s_i = D)$,

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

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, and $n_C(s_{-i})$ 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.)

Fig. 1 (a) shows seven users moving in a network and meeting in four mix zones. Fig. 1 (b) illustrates the evolution of user centric location privacy of node 1. The payoff of node 1 increases twice after a successful pseudonym change (in mix zones E_1 and E_3) and then decreases after a failed pseudonym change (in mix zone E_4) because of the penalty γ. Because we analyze only a single strategic interaction between players, we simplify notation and write in the following $n = n(t)$, $\beta_i = \beta_i(t, T_i^\ell)$, $\alpha_i = \alpha_i(t, T_i^\ell)$, and $u_i(s_i, s_{-i}) = u_i(t, T_i^\ell, s_i, s_{-i})$.

4) Type: In this paper we also deal with *incomplete information* games. For example, 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 [13] 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, $\theta_i = u_i^-$, 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.



(a) (b)

Fig. 1. 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 node 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).

5) Equilibrium Concepts: We introduce the game-theoretic concepts that model 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 [23].

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 [13], [15]. 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:

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

V. Analysis of the Game

We study several types of pseudonym change games with complete and incomplete information, and two type of strategies static or dynamic.

A. Static Game with Complete Information

We call the complete information game $\mathcal{C}$-game ($\mathcal{C}$ stands for complete information). We assume that there exists only one time step, i.e., players have only one move as a strategy. In game-theoretic terms, this is called a single-stage or static game. This is a realistic assumption because in mix zones, nodes are unable to sense their environment. Hence, each player with common knowledge about the type of all players chooses a strategy simultaneously. For simplicity, we assume that upon a pseudonym change, every node achieves the same privacy and thus we consider the upperbound $A_i = \log_2(k)$, where $k \leq n$ is the number of cooperating nodes. Using the upperbound is qualitatively similar to using other privacy metrics as all are sublinear in the anonymity set size.

1) 2-player $\mathcal{C}$-game: The strategic representation of the two player $\mathcal{C}$-game is shown in Table I. 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. Values in cells represent the payoff of each player.

TABLE I
2-PLAYER STRATEGIC FORM $\mathcal{C}$-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^-)

We assume 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 $\gamma < 1/2$ to bound the cost.

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.

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.

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 $x_1 = \frac{\gamma}{1-u_2^-}$. ∎

We observe that the pseudonym change game is a *coordination game* [9], 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 consistent decisions. Coordination games have three NE, as obtained with Theorem 1. (C, C) is the Pareto-optimal strategy and thus the preferred equilibrium.

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., $x_1 \neq x_2$).

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. Lemma 1 identifies the existence of an All Defection NE.

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

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^-. ∎

Lemma 2 identifies a condition for the existence of NE with cooperation.

Lemma 2: There is at least one cooperative pure-strategy Nash equilibrium (i.e., at least two players cooperate) for the n-player pseudonym change $\mathcal{C}$-game if there exists a set of cooperating nodes C^{k^*} s.t. $\forall P_i \in C^{k^*}$, $\log_2(|C^{k^*}|) - \gamma > u_i^-$. The strategy profile is then $s^* = \{s_i^* | s_i^* = C \ if \ P_i \in C^{k^*}, s_i^* = D \ if \ P_i \in D^{n-k^*}\}$.

Proof: If any $P_i \in C^{k^*}$ unilaterally deviates from cooperation to defect, then its payoff $u_i = u_i^-$ 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 s^* is a NE when $|C^{k^*}| > 1$. ∎

Lemma 3: There are at most $\lfloor \frac{n}{2} \rfloor$ cooperative pure-strategy Nash equilibria for the n-player pseudonym change $\mathcal{C}$-game.

Proof: Assume that the minimal set of cooperating nodes is $C^{k_1^*}$ s.t. $\forall P_i \in C^{k_1^*}$, $\log_2(|C^{k_1^*}|) - \gamma > u_i^-$. This is the pure-strategy NE with the lowest number of cooperative players. We show by contradiction that if another set of cooperating nodes $C^{k_2^*}$ exists, then it must be a superset of $C^{k_1^*}$.

Consider $C^{k_1^*}$ and $C^{k_2^*}$ such that $C^{k_1^*} \cap C^{k_2^*} = \emptyset$ and $\forall P_i \in C^{k_j^*}$, $\log_2(|C^{k_j^*}|) - \gamma > u_i^-$ 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 into the larger group C^{k^*} and create a new cooperative equilibrium. Thus if $C^{k_2^*}$ exists, it must be a superset of $C^{k_1^*}$.

Another set of cooperating players $C^{k_2^*}$ exists if $C^{k_1^*} \subset C^{k_2^*}$ and $\forall P_i \in C^{k_2^*} \setminus C^{k_1^*}$, $\log_2(|C^{k_2^*}|) - \gamma > u_i^- \geq \log_2(|C^{k_1^*}|) - \gamma$. Indeed, with such condition, none of the players in $C^{k_2^*} \setminus C^{k_1^*}$ can deviate from cooperation to unilaterally improve its strategy. Thus, a superset of $C^{k_1^*}$ can make another NE.

Finally, we observe that $|C^{k_2^*}| - |C^{k_1^*}| \geq 2$ meaning that at least two players must change their strategy to obtain a new NE. Otherwise, one player could unilaterally deviate to improve its strategy. Hence, the *maximum* number of cooperative NE will depend on the number of pairs of players that can exist, i.e., $\lfloor \frac{n}{2} \rfloor$. ∎

Considering Lemma 1, 2 and 3, and as there are no 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 one and at most $\lfloor \frac{n}{2} \rfloor + 1$ 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 $\lfloor 3/2 \rfloor = 1$ cooperative NE as defined by Lemma 3. 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 only cooperative NE strategy profile is (C, C, D), corresponding to $|C^{k^*}| = 2$.

B. Static Game with Incomplete Information

We call games of incomplete information $\mathcal{I}$-games ($\mathcal{I}$ stands for incomplete information): players do not know the payoff type of their opponents. The incomplete information assumption better models the knowledge of mobile nodes.

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 $\theta_i = A_i - \beta_i - \gamma\alpha_i - \gamma$; this 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. 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 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.

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:

$$\begin{aligned} E[u_1(C, \underline{s}_2)|\theta_1] &= F(\tilde{\theta}_2)(1-\gamma) + (1 - F(\tilde{\theta}_2)) \cdot \\ &\quad \max(0, (\theta_1 - \gamma)) \qquad (14) \\ E[u_1(D, \underline{s}_2)|\theta_1] &= \theta_1, \qquad (15) \end{aligned}$$

and similarly for player 2. For a threshold equilibrium, when a player's type is its threshold type, it must be 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 solving for thresholds with this property defines a BNE for the 2-player $\mathcal{I}$-game.

Lemma 4: 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:

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

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. ■

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.

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 4. 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. (16) that

$$F \cdot (1 - \gamma) + (1 - F) \max(0, \tilde{\theta}_2^* + \epsilon - \gamma) - \tilde{\theta}_2^* - \epsilon = 0 \tag{17}$$

$$F_\epsilon \cdot (1 - \gamma) + (1 - F_\epsilon) \max(0, \tilde{\theta}_2^* - \gamma) - \tilde{\theta}_2^* = 0 \tag{18}$$

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

(Case 1) $\tilde{\theta}_2^* \leq \gamma - \epsilon$. By equating Eq. (17) and (18) and simplification, we have

$$F(1 - \gamma) - \epsilon = F_\epsilon \cdot (1 - \gamma) \tag{19}$$

$$\Rightarrow \epsilon = F \cdot (1 - \gamma) - F_\epsilon \cdot (1 - \gamma) < 0, \tag{20}$$

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. (17) and (18) and simplification, we have

$$F \cdot (1 - \tilde{\theta}_2^*) + \tilde{\theta}_2^* - \gamma - F\epsilon = F_\epsilon \cdot (1 - \gamma) \tag{21}$$

$$\Rightarrow \epsilon = \frac{F \cdot (1 - \tilde{\theta}_2^*) - F_\epsilon \cdot (1 - \gamma) - (\gamma - \tilde{\theta}_2^*)}{F} \tag{22}$$

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.

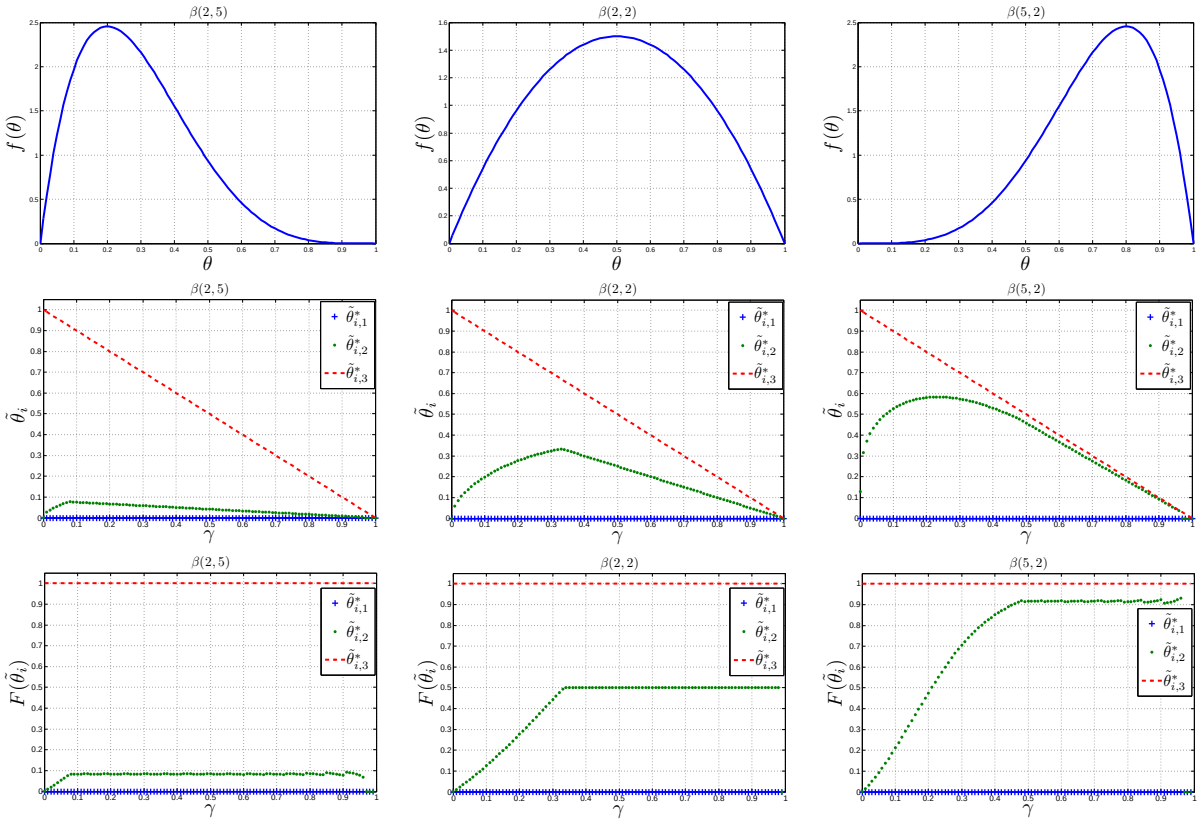


Fig. 2. Probability distribution of user types $f(\theta)$, threshold $\tilde{\theta}_i^*$, and probability of cooperation $F(\tilde{\theta}_i^*)$ at the equilibrium as a function of γ for different distributions of type: $\beta(2,5)$, $\beta(2,2)$, and $\beta(5,2)$. For each type distribution, there 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 $\tilde{\theta}_1^*$, i.e., the probability of cooperation increases.

(Case 3) $\gamma \leq \tilde{\theta}_2^*$. By equating Eq. (17) and (18) and simplification, we have

$$F \cdot (1 - \tilde{\theta}_2^*) - F\epsilon = F_\epsilon \cdot (1 - \tilde{\theta}_2^*) \tag{23}$$

$$\Rightarrow \quad \epsilon = \frac{F \cdot (1 - \tilde{\theta}_2^*) - F_\epsilon \cdot (1 - \tilde{\theta}_2^*)}{F} < 0, \tag{24}$$

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

With numerical evaluations, we find an intermediate, symmetric threshold equilibrium in almost all cases, where players don't simply always cooperate or always defect.[2]

To illustrate 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 $F(\theta_i) = \theta_i/(1-\gamma)$. 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:

$$\tilde{\theta}_i^* \triangleq 1 - \frac{\gamma}{F(\tilde{\theta}_{-i}^*)}, i = 1, 2 \tag{25}$$

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 solutions:

$$\tilde{\theta}_i^* \in \{\gamma, 1-\gamma\} \tag{26}$$

[2]Previous works [8], [24] 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. We consider this distribution for illustration purposes as in practice $F(\theta)$ would be obtained from real measurements. The beta distribution is easily configurable and thus allows for testing different scenarios corresponding to various network conditions. If $\theta \sim \mathcal{B}(2, 5)$, nodes have a small θ with a high probability, whereas with $\theta \sim \mathcal{B}(5, 2)$, nodes have a large θ with a high probability. If $\theta \sim \mathcal{B}(2, 2)$, θ is symmetric and centralized around 0.5. Fig. 2 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

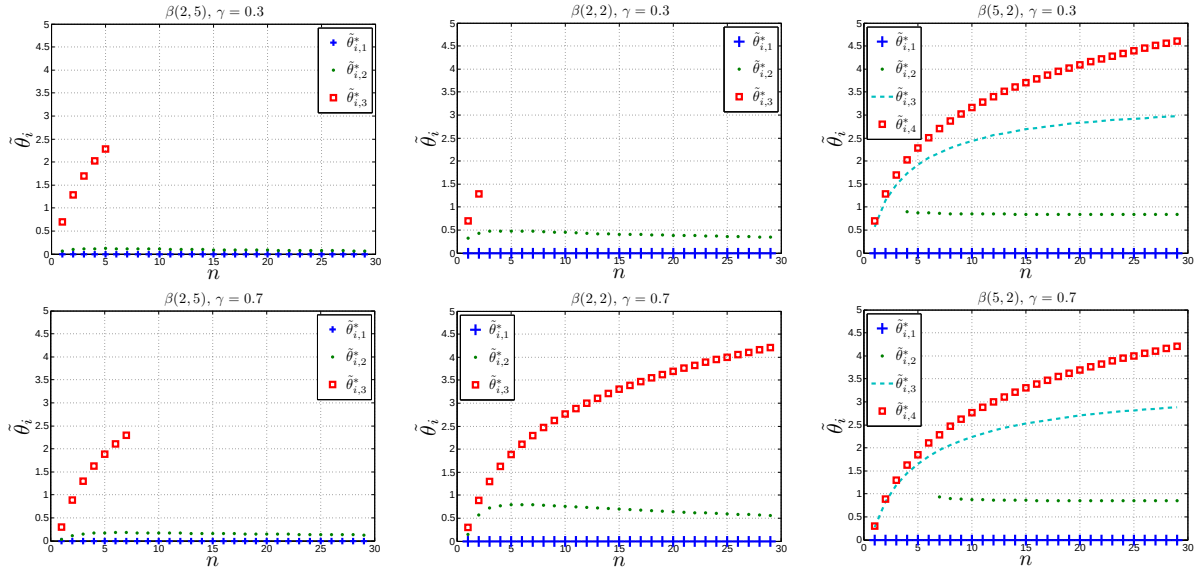


Fig. 3. Threshold $\tilde{\theta}^*_i$ at the equilibrium as a function of n for different values of γ and distributions of type: $\beta(2,5)$, $\beta(2,2)$, and $\beta(5,2)$. For each type distribution, the number of BNE changes depending on the cost γ.

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, 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.

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:

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

By a similar argument to that for the 2-player $\mathcal{I}$-game (Lemma 4), a BNE $\underline{s}^* = (\tilde{\theta}^*_1; \cdots; \tilde{\theta}^*_n)$ can be obtained as the solution to the following system of n non-linear equations for the n variables $\tilde{\theta}_i$:

$$\sum_{k=0}^{n-1} Pr(K = k) u_i(C, \underline{s}_{-i}) = u_i^-, \quad i = 1, 2, \cdots, n \qquad (27)$$

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 $Pr(K = 0) = 1$. Thus, the All Defection equilibrium exists.
- If $q \to 1$, then $\tilde{\theta}^*_i = 1$, $Pr(K < n-1) = 0$ and $Pr(K = n-1) = 1$. Thus, 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. (27) with Matlab (Fig. 3). For $\gamma = 0.3$, we observe that with a higher density of nodes n, $\tilde{\theta}^*_{i,2}$ decreases, which means that players cooperate with a lower probability. Similarly, $\tilde{\theta}^*_{i,3}$ disappears for large values of n, which means 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 reason 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, the All Cooperation equilibrium survives longer when γ increases.

We observe that the game admits several equilibria $\tilde{\theta}^*_{i,\_}$, and thus different players may choose to play different equilibria. Some equilibria can be ruled out: All Defect does not provide privacy and All Cooperate incurs large cost. Intermediate equilibria can exist. If only one intermediate equilibrium exists, then NE selection is trivial. If multiple intermediate equilibria exist ($\tilde{\theta}^*_{i,2}$ and $\tilde{\theta}^*_{i,3}$ with $\beta(5,2)$ and $\gamma = 0.7$), then players pick the equilibrium with best outcome. As the game is symmetric, the same intermediate equilibrium is best for all.

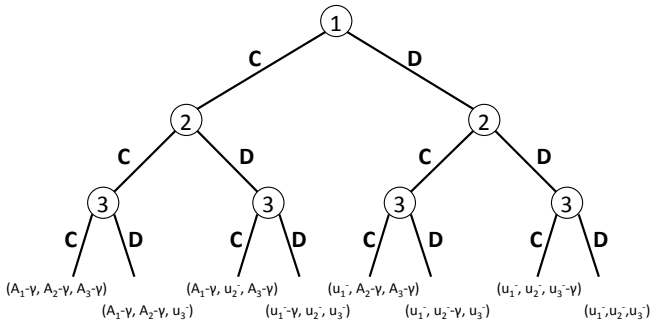


Fig. 4. Extensive form of the Pseudonym Change Game. The game is represented by a tree and node 1 plays the first action. The game has three stages corresponding to the moves of the three players. The actions (cooperate C and defect D) are represented on each branch of the tree. The leaves of the tree represent the payoff of the game for all players.

C. Dynamic Game with Complete Information

Until now, we assumed that the players make their moves simultaneously in mix zones without knowing what the other players do. This is a reasonable assumption because in mix zones, nodes are unable to sense their environment. Yet, nodes could exchange messages in mix zones to advertise their decision. In this case, players have several moves as a strategy and can have sequential interactions: the move of one player can be conditioned by the move of other players (i.e., the second player knows the move of the first player before making his decision). These games are called dynamic games, and we refer to dynamic pseudonym change games with complete information as *dynamic $\mathcal{C}$-games*. We can represent dynamic games by their extensive form (Fig. 4), similar to a tree where branches represent the strategies for a given player. Each level of the tree represents a stage of the game.

For such dynamic scenarios to exist, nodes must be able to observe the action of other nodes. There are several ways to achieve this. A simple solution is that players broadcast their decision to cooperate in a sequential manner [22]. Nonetheless, this increases the communication overhead. Another solution is that players observe the messages of other nodes exiting a mix zone. For example, if a node decides to defect, then it continues broadcasting messages that can be observed by other nodes in the mix zone. In other words, nodes participating in a mix zone can use defection as a signal to avoid the cost of being silent. Any of these solutions can be used, but we consider the latter because it requires less network resources.

1) Backward Induction: In dynamic game, we use the concept of subgame-perfect equilibrium. The strategy profile s is a subgame-perfect equilibrium of a finite extensive-form game G if it is a Nash equilibrium of any subgame G' of the original game G [13]. We will check for the existence of subgame-perfect equilibria by backward induction [13]. Backward induction works by eliminating sub-optimal actions, beginning at the leaves of the extensive-form tree. The obtained path (sequence of actions) in the game tree defines the backward induction solution and any strategy profile that realizes this solution is a subgame-perfect equilibrium. Note that the above game belongs to a class of finite game, because it should be played in a short amount of time.

2) n-player Dynamic $\mathcal{C}$-Game: For any order of players, the subgame-perfect Nash equilibrium can be derived by all nodes with the following theorem.

Theorem 4: 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 exist such a C^{k^*}, then in the n-player dynamic pseudonym change $\mathcal{C}$-game, there is a strategy that results in a single subgame-perfect equilibrium:

$$s_i^* = \begin{cases} C & \text{if } P_i \in C^{k^*} \\ D & \text{else} \end{cases} \tag{28}$$

If there does not exist such a C^{k^*}, then the subgame perfect equilibrium is all defection.

Proof: Similar to the proof of Lemma 2, no player $P_i \in C^{k^*}$ has an incentive to unilaterally deviate from cooperation to defection as its payoff u_i^- would be smaller than $\log_2(|C^{k^*}|) - \gamma$. The same is true for players that defect, i.e., that are not in C^{k^*}. Hence, none of the nodes can unilaterally change its strategy to increase its payoff and s^* is an subgame-perfect equilibrium when $|C^{k^*}| > 1$. If C^{k^*} is empty, then the subgame-perfect equilibrium corresponds to an All Defection. Because the actions of the players are dynamic, a single subgame-perfect equilibrium will be selected. ■

We observe that the All Defection equilibrium does not always exist as there is only one subgame-perfect equilibrium. An advantage of the dynamic game is that the All Defection equilibrium is often an incredible threat. Similarly, among possible cooperative equilibria, the equilibrium with the largest number of cooperating devices is selected. In other words, coordination is simpler in dynamic games than in static games.

D. Dynamic Game with Incomplete Information

We call dynamic games of incomplete information dynamic $\mathcal{I}$-games. The concept of subgame-perfect Nash equilibrium introduced in the previous section cannot be used to solve games of incomplete information. Even if players observe one another's actions, the problem is that players do not know the others' types and cannot predict each others' strategy.

Dynamic games of incomplete information can be solved using the concept of *perfect Bayesian equilibrium* (PBE). This solution concept results from the idea of combining subgame perfection, Bayesian equilibrium and Bayesian inference. Strategies are required to yield a Bayesian equilibrium in every subgame given the a posteriori beliefs of the players about each others' types. To do so, players update their beliefs about their opponents' types based on others' actions using Bayes' rule. The resulting game is called a dynamic Bayesian game where "dynamic" means that the game is sequential and "Bayesian" refers to the probabilistic nature of the game. For further details, we refer the interested reader to [13].

1) n-player Dynamic $\mathcal{I}$-Game: Consider that a pseudonym change game starts at time t_0. Every player can decide to cooperate or defect at each stage of the game. Hence, players can delay their decision and enter the game at any time $t \geq t_0$. The actions of players at time t is denoted $a^t = (a_1^t, ..., a_n^t)$ and is cooperate C or defect D. The history of actions of the game is $h^t = (a^0, ..., a^{t-1})$. The following theorem provides a strategy that leads to a perfect Bayesian equilibrium.

Theorem 5: In the n-player dynamic pseudonym change $\mathcal{I}$-game, the following strategy results in a unique perfect Bayesian equilibrium:

$$\underline{s}_i^* = \begin{cases} C & \text{if } (n_D(t) = 0) \wedge (u_i^- < \log_2(n_r)) \\ D & \text{else} \end{cases} \quad (29)$$

where $n_r < n$ is the number of nodes remaining in the game (i.e., that did not defect) and $n_D(t)$ is the number of nodes that defect at time t.

Proof: The strategy of players depends on their belief about other players' types. We define $\mu_i\left(\theta_j|h^t\right)$ as the belief of a player i about the type of another player j given a history of actions h^t. In order to obtain a perfect Bayesian equilibrium, Bayes' rule is used to update beliefs from $\mu_i\left(\theta_j|h^t\right)$ to $\mu_i\left(\theta_j|h^{t+1}\right)$. Formally, for all i, j, h^t and a_j, we have:

$$\mu_i\left(\theta_j|\left(h^t, a^t\right)\right) = \frac{\mu_i\left(\theta_j|h^t\right)\sigma_j\left(a_j^t|h^t, \theta_j\right)}{\sum_{\tilde{\theta}_j}\mu_i\left(\tilde{\theta}_j|h^t\right)\sigma_j\left(a_j^t|h^t, \tilde{\theta}_j\right)} \quad (30)$$

where σ_j is the probability that a user j plays a certain action a_j. Assume that the number of remaining nodes in the game is n_r (i.e., the number of nodes that did not defect) and that the initial belief function is: $\mu_i(\theta_j) = f(\theta_j)$. If at time $t_1 > t$ player j defects, it indicates that the type of player j is above the current threshold $\tilde{\theta} = \log_2(n_r)$. Hence, the behavior strategy $\sigma_j(a_j^{t_1}|h^{t_1}, \theta_j)$ returns 0 if $\theta_j \leq \tilde{\theta}$ and 1 otherwise. The denominator computes the belief about all possible types of player j and thus normalizes $\mu_i(\theta_j|h^{t_1})$ according the current threshold $\tilde{\theta}$. Other players that observe the action of player j can thus update their belief about the type of player j and obtain: $\mu_i(\theta_j > \tilde{\theta}|h^{t_1}, a^{t_1}) = 1$, i.e., they know that player j had a type above the current threshold. If at some time $t_2 > t_1$ no nodes defect ($n_D(t_2) = 0$), it indicates that with probability one all remaining players have types below the current threshold: $\mu_i(\theta_j \leq \tilde{\theta}|h^{t_2}, a^{t_2}) = 1$. Hence, all these players will cooperate and $\tilde{\theta}^* = \log_2(n_r)$. ■

Compared to the static game, the threshold computation is simpler as it only depends on the number of nodes remaining in the game.

We numerically evaluate the perfect Bayesian equilibrium using Matlab (Fig. 5). We compute the average number of nodes that cooperate in dynamic games of incomplete information given distributions of type and cost.

We observe that when the cost of cooperation γ increases, the number of nodes that cooperate decreases. The reason is that, in dynamic games, nodes have more information to optimize their decision and will thus avoid cooperating unless there is a large number of nodes in a game. The distribution of types also affects the number of cooperating nodes. We observe that a large population of nodes with high privacy (e.g., $\beta(5, 2)$) cooperate less than nodes with low privacy (e.g., $\beta(2, 5)$): nodes cooperate only if the privacy gain is large. We also observe that a larger number of nodes in a game, increases the probability of cooperation. In summary, the dynamic version of the game copes well with uncertainty by relying on the action of defecting nodes to improve the estimation of the potential privacy gain.

VI. Protocols

We formally describe location privacy protocols, including PseudoGame protocols and evaluate them using simulations. Pseudonym change protocols can be usually modeled with two parts: 1) an initiation phase, in which nodes request pseudonym changes, and 2) a decision phase, in which nodes decide upon receiving a request whether to change pseudonyms or not. Pseudonym change games model the latter.

A. Initiation Protocols

The initiation phase aims at finding appropriate contexts to request pseudonym changes from nearby nodes. A context provides high location privacy if there is high node density and mobility unpredictability.

1) NaiveInitiation Protocol: A simple solution consists in issuing a pseudonym change request at every time step t when there is at least another node nearby. The sender can choose a silent period in the range $[sp_{min}, sp_{max}]$ that it attaches to the initiation message. We call this protocol the NaiveInitiation protocol (Protocol 1).

Protocol 1 NaiveInitiation.

1: **if** (At least one neighbor) and (not in silent period) **then**
2: Broadcast initiation message to change pseudonym.

2) GainInitiation Protocol: In the GainInitiation protocol (Protocol 2), any node can initiate a pseudonym change by broadcasting an update message if a node has at least one neighbor and if its current location privacy is lower than the potential privacy gain. The sender can choose a silent period in the range $[sp_{min}, sp_{max}]$ that it attaches to the initiation message. This is a protocol similar to that in [22].

Protocol 2 GainInitiation.

1: maxGain = $\log_2$(number of neighbors)
2: **if** (At least one neighbor) and (current location privacy < maxGain) and (not in silent period) **then**
3: Broadcast initiation message to change pseudonym.

B. Decision Protocols

Mobile nodes receiving the initiation message must decide whether to stop communicating for a silent period, as defined in the initiation message, and change pseudonyms. The decision phase aims at making the best pseudonym change decision to maximize the level of privacy at a minimum cost. Below we describe several decision protocols, including protocols proposed in previous work and protocols resulting from the aforementioned game-theoretic analysis.

1) Swing Protocol: In the Swing protocol (Protocol 3) [22], the decision of mobile nodes to cooperate (or not) exclusively depends on their user-centric level of location privacy compared to a *fixed* threshold $\tilde{\theta}$. The cost of changing pseudonyms and the probability of cooperation of the neighbors are not considered in the computation of the threshold. Hence, this is a reactive model: users change pseudonyms only if their user-centric level of location privacy goes below the threshold.

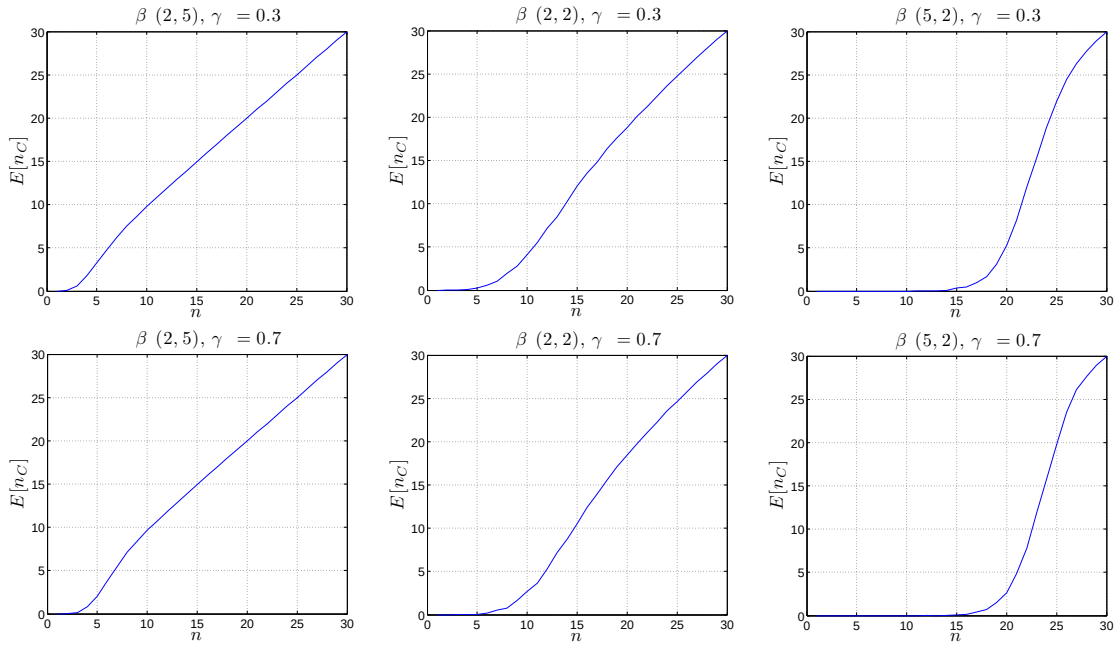


Fig. 5. Average number of nodes that cooperate in a game with respect to the number of nodes participating in the game for different values of γ and distributions of types: $\beta\,(2,5)\,,\beta\,(2,2)\,,\beta\,(5,2)$.

Protocol 3 Swing.

Require: The current location privacy of node i is u_i^-
1: **if** (Receive Initiation message) or (Initiated change) **then**
2: **if** $u_i^- < \tilde{\theta}_i$ **then**
3: Change pseudonym and comply with silent period sp_{max}
4: **else**
5: Quit
6: **else**
7: Keep pseudonym

Protocol 4 Static PseudoGame.

Require: Node i knows the probability distribution $f(\theta)$
Require: The current location privacy of node i is u_i^-
1: **if** (Receive Initiation message) or (Initiated change) **then**
2: $n \Leftarrow estimate(n)$ //Number of neighbors
3: 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 $q \Leftarrow \int_0^{\tilde{\theta}_i} f(\theta_i) d\theta_i$
4: **if** $u_i^- \leq \tilde{\theta}_i^*$ **then**
5: Play C
6: Comply with silent period sp_{max}
7: **else**
8: Play D
9: **else**
10: Keep pseudonym

2) Static PseudoGame Protocol: Our game-theoretic evaluation allows us to design PseudoGame protocols that extend the Swing protocol to consider equilibrium strategies in a non-cooperative environment. The static PseudoGame protocol is based on our results for static n-player $\mathcal{I}$-games.

All nodes receiving the initiation message use the PseudoGame protocol to decide whether to change pseudonyms based on the number of neighbors and the probability of their cooperation (related to the distribution of user types $f(\theta_i)$). As described in Protocol 4 for any node i, the PseudoGame protocol assists mobile nodes in selecting the smallest intermediary BNE strategy (Please see Fig.3). Hence, 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 in a rational environment to determine when to change pseudonym.

3) Dynamic PseudoGame Protocol: The dynamic version of the PseudoGame protocol (Protocol 5) uses the action of other nodes as a signal to improve its decision making strategy.

After receiving the initiation message, each player estimates the number of players in the game. At each time step t, players check whether their current utility u_i^- is superior to the potential benefit $\log_2(n)$ and if so, defect. Players then observe the number of remaining players (that did not defect). If in a round t no nodes defected, it means that all remaining nodes are interested in changing pseudonym and thus cooperate.

4) All Cooperation Protocol: The AllCooperation protocol (Protocol 6) is a straightforward method in which players always cooperate when asked to change pseudonyms.

5) Random Decision Protocol: The Random protocol (Protocol 7) is a straightforward method in which players decide randomly whether to cooperate or not.

6) Evaluation: To evaluate the ability of these protocols to mix pseudonyms, we simulate them in a mobile network. We consider the following setup: mobility traces are generated with Sumo [1] over a cropped map [2] of Manhattan of 9 km^2 and include a total of 900 nodes injected in the map with average speed of $6,63$ m/s and average distance of 12.5 km. Each simulation lasts 5000 seconds; nodes have on average 116 encounters and the average nodes in encounter is 2.93.

Protocol 5 Dynamic PseudoGame.

Require: Node i knows the probability distribution $f(\theta)$
Require: The current location privacy of node i is u_i^-
if (Receive Initiation message) or (Initiated change) **then**
  $n \Leftarrow estimate(n)$ //Number of neighbors
  lastN $= n$
  for $t = 0$ to sp_{max} **do**
    if $u_i^- \geq \log_2(n)$ **then**
      Play D
      Quit
    $n =$ number of remaining nodes
    if $n = lastN$ **then**
      Play C
      Comply with silent period sp_{max}
    lastN $= n$
else
  Keep pseudonym

Protocol 6 AllCooperation.

if (Receive Initiation message) or (Initiated change) **then**
  Change pseudonym and comply with silent period sp_{max}
else
  Keep pseudonym

Protocol 7 Random.

if (Receive Initiation message) or (Initiated change) **then**
  Throw a coin
  if Heads **then**
    Change pseudonym and comply with silent period sp_{max}
else
  Keep pseudonym

For the game model, we consider an initial distribution of user types $\beta(2, 5)$, $\lambda = 0.0005$ and a cost of pseudonym change $\gamma = 0.3$. The results are averaged across 5 simulations.

A numerical analysis is required to derive the BNE in Protocol 4. In our experiments, we find the solution to the system of equations using the Brent-Dekker algorithm and systematically in a negligible time.

Fig. 6 shows the total number of games initiated by each initiation protocol. We observe that the NaiveInitiation protocol generates a larger number of games than the GainInitiation protocol. A large number of games will induce networking costs because of all the initiation messages, but will also provide more opportunities to change pseudonyms. Yet, the quality of the contexts of the initiated games may be lower.

Fig. 7 shows the average utility obtained with the different initiation and decision protocols. We observe that the initiation protocols do not affect the achievable utility of PseudoGame protocols, intuitively because PseudoGame protocols avoid inefficient pseudonym changes. In contrast, the NaiveInitiation protocol decreases the achievable utility of the AllCooperation, Swing and Random protocols because it increases the number of inefficient pseudonym changes.

In Fig. 7, we also observe the achievable privacy (utility) of different decision protocols. The dynamic PseudoGame achieves the highest utility among all protocols, showing that even with rational behavior high coordination is possible. In the case of the Swing protocol, with a large threshold, nodes participate in many inefficient mix zones, whereas with a small threshold, nodes have to wait long before changing pseudonyms again. In this regard, $\tilde{\theta} = 3$ appears as an efficient static threshold. Finally, the static PseudoGame performs slightly worse than the Swing protocol, showing that rational behavior negatively affects the achievable privacy in this case. This can be notably observed in Fig. 8 that shows the average cost associated with the different protocols. The cost is in general larger with the NaiveInitiation protocol.

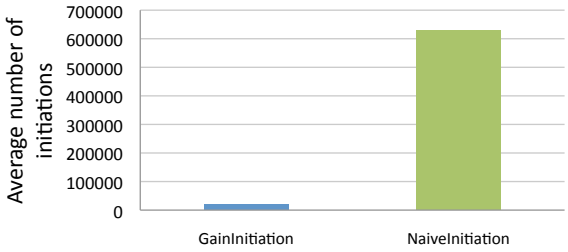


Fig. 6. Average number of pseudonym change initiations for each initiation protocols using the dynamic PseudoGame.

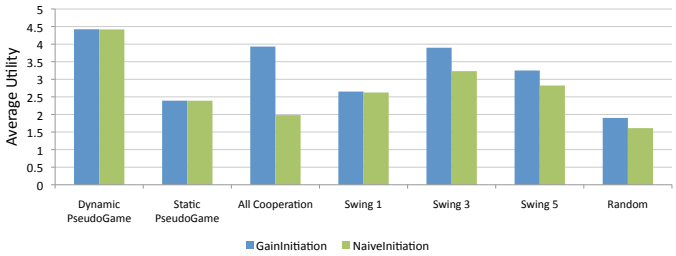


Fig. 7. Average utility with each decision and initiation protocols. Swing 3 means the Swing protocol with a threshold $\tilde{\theta} = 3$.

Comparing decision protocols, we observe that the dynamic PseudoGame protocol dramatically reduces the cost compared to other protocols. For the Swing protocol, the cost increases with the threshold. The dynamic PseudoGame protocol provides the best trade-off between privacy and cost: it efficiently deals with the uncertainty of incomplete information. In contrast, the static PseudoGame protocol performs poorly: rationality does not always reduce cost.

VII. Conclusion

We have considered the problem of rationality 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 and evaluated the strategic behavior of mobile nodes with a game-theoretic model, the *pseudonym change game*. We analyzed the n-player scenario with complete and incomplete information and derived the equilibrium strategies for each node for both static and dynamic games. The obtained equilibria allow us to predict the strategy of rational mobile nodes seeking to achieve location privacy in a non-cooperative environment. This analysis results in the design of new protocols, the PseudoGame protocols, that coordinate pseudonym changes.

An intriguing result is that when uncertainty about others' strategies is high (i.e., static games), rational nodes care

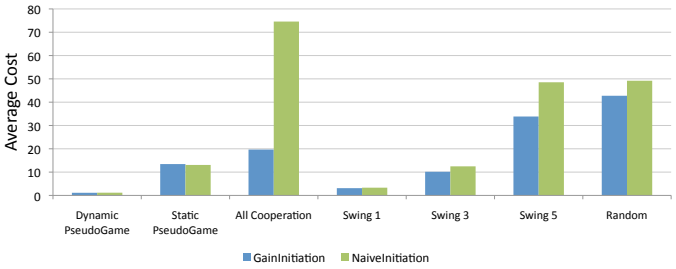


Fig. 8. Average Cost with each decision and initiation protocols.

more about the successful unfolding of the game if the cost of pseudonyms is also high. This result indicates that cost, usually a negative parameter, can positively affect the game by increasing the success of pseudonym change coordination. By means of simulations, we showed that dynamic games dramatically increase the coordination success of pseudonym changes. The dynamic PseudoGame protocol coordinates pseudonym changes better than other protocols and leads to an efficient trade-off between privacy and cost.

In future work, novel game models may be considered to include other strategic aspects, such as the evolution of user strategies across several games. It would also be interesting to consider how obtaining the distribution $f(\theta)$ in a distributed and noisy fashion may affect results.

REFERENCES

[1] SUMO (Simulation of Urban MObility): An open-source traffic simulator http://sumo.sourceforge.net
[2] TIGER maps. http://www.census.gov/geo/www/tiger
[3] WiFi Alliance. Wi-Fi CERTIFIED Wi-Fi Direct: Personal, portable Wi-Fi that goes with you anywhere, any time, 2010. http://www.wi-fi.org/Wi-Fi_Direct.php
[4] A. R. Beresford and F. Stajano. Mix zones: user privacy in location-aware services. In *Pervasive Computing and Communications Workshops*, pages 127–131, 2004
[5] Official Nokia Blog. Nokia Instant Community gets you social, 2010 http://conversations.nokia.com/2010/05/25/nokia-instant-community-gets-you-social
[6] L. Buttyan, T. Holczer, and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *ESAS*, 2007
[7] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–90, February 1981
[8] 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
[9] R. Cooper. Coordination Games. Cambridge Univ. Press, 1998
[10] K. Fall. A delay-tolerant network architecture for challenged internets. SIGCOMM, 2003
[11] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P. Hubaux. Mix Zones for Location Privacy in Vehicular Networks. In *WiN-ITS*, 2007
[12] J. Freudiger, R. Shokri, and J.-P. Hubaux. On the Optimal Placement of Mix Zones. PETS, 2009
[13] D. Fudenberg and J. Tirole. Game Theory. MIT Press, 1991
[14] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. Mob. Netw. Appl., 2005
[15] J. Harsanyi. Games with Incomplete Information played by Bayesian players. Management Science, 1967
[16] H. Hartenstein and K. Laberteaux. A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine, 46(6), 2008
[17] 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. MobiSys, pages = 15–28, 2008
[18] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady. Preserving privacy in GPS traces via path cloaking. CCS, 2007
[19] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing Wireless Location Privacy using Silent Period. In *ECNC*, 2005
[20] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, Towards modeling wireless location privacy. PET, 2005
[21] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux. Tracking Games in Mobile Networks. Conference on Decision and Game Theory for Security, 2010
[22] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran. Swing & Swap: user-centric approaches towards maximizing location privacy. In *WPES*, 2006
[23] J. Nash. Non-Cooperative Games. Annals of Mathematics, 1951
[24] D. M. Reeves and M.P. Wellman. Computing best-response strategies in infinite games of incomplete information. Uncertainty in artificial intelligence, pages 470–478, 2004
[25] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing Location Privacy for VANET. In *Proceedings of Embedded Security in Cars (ESCAR)*, 2005
[26] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos. Impact of Pseudonym Changes on Geographic Routing in VANETs. ESAS, 2006
[27] A. Serjantov and G. Danezis. Towards an Information Theoretic Metric for Anonymity. PET, 2002
[28] S. Vasudevan, J. Kurose, and D. Towsley. On neighbor discovery in wireless networks with directional antennas. Infocom, 2005
[29] X. Wu, S. Tavildar, S. Shakkottai, T. Richardson, J. Li, R. Laroia and A. Jovicic, FlashLinQ: A synchronous distributed scheduler for peer-to-peer ad hoc networks. In *Communication, Control, and Computing*, pages 514–521. IEEE, 2010

Julien Freudiger received the M.Eng. degree in Communication Systems from EPFL in 2006 and graduated with a Ph.D. in Computer and Communication Systems from EPFL in 2011. His research interests include security systems design and privacy protection. His thesis was on location privacy protection for wireless network applications.

Mohammad Hossein Manshaei is an assistant professor at the Isfahan University of Technology, Iran. He earned his B.S. degree in electrical engineering and his M.S. degree in communication engineering from the Isfahan University of Technology in 1997 and 2000. He earned another M.S. degree in computer science and his Ph.D. in computer science and distributed systems from the University of Nice Sophia-Antipolis, France, in 2002 and 2005. From 2006 to 2011, he was a senior researcher and lecturer at EPFL. His research interests include wireless networking, wireless security, cognitive radios, and game theory.

Jean-Pierre Hubaux is a professor at EPFL (which he joined in 1990) and a Fellow of both ACM and IEEE. His current research activity is focused on privacy preservation mechanisms, notably in pervasive communication systems. In 2008, he completed a graduate textbook entitled "Security and Cooperation in Wireless Networks", with Levente Buttyan. He held visiting positions at the IBM T.J. Watson Research Center and at UC Berkeley.

David Parkes received the M.Eng. (first class) degree in Engineering and Computing Science from Oxford University in 1995 and a Ph.D. in Computer and Information Science from the University of Pennsylvania in 2001. Parkes is Gordon McKay Professor of Computer Science at Harvard, and serves as Chair of the ACM SIGecom. His research interests include market design, electronic commerce and multi-agent systems.