Tracking Games in Mobile Networks

Mathias Humbert, Mohammad Hossein Manshaei,
Julien Freudiger, and Jean-Pierre Hubaux

LCA1, EPFL, Switzerland
{mathias.humbert, hossein.manshaei,
julien.freudiger, jean-pierre.hubaux}@epfl.ch

Abstract. Users of mobile networks can change their identifiers in regions called mix zones in order to defeat the attempt of third parties to track their location. Mix zones must be deployed carefully in the network to reduce the cost they induce on mobile users and to provide high location privacy. Unlike most previous works that assume a global adversary, we consider a local adversary equipped with multiple eavesdropping stations. We study the interaction between the local adversary deploying eavesdropping stations to track mobile users and mobile users deploying mix zones to protect their location privacy. We use a game-theoretic model to predict the strategies of both players. We derive the strategies at equilibrium in complete and incomplete information scenarios and propose an algorithm to compute the equilibrium in a large network. Finally, based on real road-traffic information, we numerically quantify the effect of complete and incomplete information on the strategy selection of mobile users and of the adversary. Our results enable system designers to predict the best response of mobile users with respect to a local adversary strategy, and thus to select the best deployment of countermeasures.

Key words: Location Privacy, Game Theory, Mobile Networks, Mix Zone.

1 Introduction

The advanced communication capabilities of mobile devices (e.g., WiFi or Bluetooth) enable the use of a new breed of mobile applications: mobile devices can directly communicate in a peer-to-peer wireless fashion and exchange *contextual* information, for example, about road-traffic conditions [16] or social presence [2, 25]. In such applications, mobile devices must unveil their identifiers (e.g., pseudonyms or cryptographic credentials) to authenticate and identify each other.

Yet, an adversary eavesdropping on such peer-to-peer wireless communications can, based on their identifiers, track mobile users. In order to protect their location privacy, mobile nodes can use multiple pseudonyms that they change over time. This approach has been adopted in cellular networks to achieve location privacy with respect to external eavesdroppers: cellular operators identify

their subscribers with a "Temporary Mobile Subscriber Identity" (TMSI). Every time a subscriber moves to a new geographical area, the cellular operator issues a new TMSI. The use of multiple pseudonyms has also been investigated to protect location privacy in mobile ad hoc networks [4,10,23]: in order to impede the linkability of old and new pseudonyms by using spatial and temporal correlation, pseudonym changes are coordinated in regions called *mix zones* [4]. In a mix zone, mobile users alter their spatial correlations by changing their pseudonyms, and their temporal correlations by: (i) remaining silent for a short period [17,23], (ii) encrypting their communications [9], or (iii) using a mobile proxy [30]. We call these regions *active* mix zones. Mix zones must be carefully deployed in the network to reduce the cost they induce on users and to provide high location privacy. Indeed, the placement of mix zones affects their performance [18] and traversing mix zones incurs a communication overhead [31].

In contrast with most previous works on location privacy [3, 8, 10, 13, 23], we do not restrict our model to a global adversary. The cost might be prohibitive for an adversary to build and maintain a global eavesdropping system and to sort and process all the received information. Instead, we consider a *local adversary* with a limited budget and that eavesdrops on communications in only certain regions of the network. In the worst case, a local adversary has an unlimited budget and becomes global. The local adversary has to strategically deploy its eavesdropping stations to gather information from the network. Mobile users can take advantage of the presence of a local adversary and change pseudonyms in regions where the adversary has no coverage [6]. We call these regions *passive* mix zones.

In this paper, we investigate the strategic behavior of mobile users deploying active and passive mix zones to protect their location privacy and the behavior of a local adversary deploying eavesdropping stations to track mobile users. To do so, we develop a game-theoretic framework to predict the strategies of the adversary and of mobile users. We refer to these games as *tracking games*. We first analyze the interaction between users and the adversary in a single road intersection with *complete information*: the adversary and mobile users know each others' strategies and payoffs. We obtain one pure-strategy Nash equilibrium and one mixed-strategy Nash equilibrium [26]. We generalize the results to a network of intersections using the notion of supergames [11]. Then, we relax the complete information assumption because mobile users may not know the position of eavesdropping stations, and we study the *incomplete information* scenario. We prove the existence of one pure-strategy Bayesian Nash equilibrium [15] in the single road intersection game and extend the result to a network of intersections. Finally, we test our model using real road traffic statistics from Lausanne, Switzerland, and obtain two important results. First, in complete information scenarios, mobile users and the adversary tend to adopt complementary strategies: users place mix zones where there is no eavesdropping station, and the adversary deploys eavesdropping stations where there is no mix zone. Second, in incomplete information scenarios, the location privacy level achieved

by mobile users depends on their level of uncertainty about the strategy of the adversary.

To the best of our knowledge, this paper is the first investigation of the strategic aspects of tracking games in mobile networks. Previous works aim at optimizing privacy-preserving mechanisms with respect to a worst case adversary [3,10,13]. In contrast, game theory allows us to further analyze the interactions between privacy-conscious nodes and the adversary in order to predict their strategies. In this direction, previous works investigate pursuit-evasion games (e.g., [20]) in which several users cooperate to locate one target user. Tracking games complement this existing work by considering a new type of game in which several users collaborate to protect their location privacy against a rational adversary equipped with local eavesdropping devices. Our results allow system designers to predict the strategies of a local adversary and mobile users with a limited budget. This paper is part of the trend of blending game theory with security to predict the strategies of the rational parties involved [1,5,7,8,12,14,21,29,33].

This paper is organized as follows. In Section 2, we present the system and threat models, and describe how mix zones provide location privacy. We introduce the game-theoretic framework in Section 3 and analyze it in Section 4. We provide the main numerical results based on real-traffic data in Section 5 and conclude in Section 6.

2 Preliminaries

In this section, we present the assumptions made throughout the paper. We also introduce mix zones and define a metric to measure location privacy.

2.1 Mobile Network Model

We study a system composed of mobile nodes moving in a road network of K intersections. Nodes are equipped with peer-to-peer wireless communication technologies (e.g., WiFi) and can communicate with other nodes in transmission range. Mobile devices identify each other using pseudonyms [27]. In order to prevent tracking by third parties, we assume that mobile nodes use multiple pseudonyms that they change over time. An offline Certification Authority (CA) run by an independent trusted third party provides mobile users, prior to entering the network, with a set of pseudonyms, such as public/private key pairs.

For each intersection, we assume the knowledge of accurate statistics: the parties know the number of vehicles per hour driving through any specific path, i.e., for each entering and exiting road pair. In practice, such information can be provided by city authorities in charge of road traffic optimization. Based on these statistics, we express the traffic intensity for each specific path in each intersection. The traffic intensity is defined in a normalized form as:

$$\lambda_i = \frac{n_i}{\mu_{\max}} \tag{1}$$

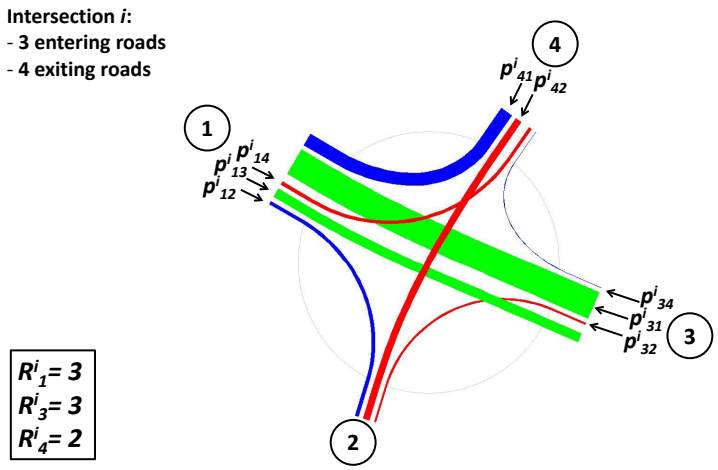


Fig. 1. Intersection i. Road 2 is one-way: no vehicle can enter the intersection from there. The width of each flow is proportional to the traffic intensity. Vehicles entering by roads 1 and 3 have 3 possible exits on each of them, whereas vehicles entering by road 4 have 2 possible exits.

where n_i is the number of nodes going through intersection or road i per unit of time and $\mu_{\max}$ is the maximum number of nodes driving through any intersection of the network per unit of time. Figure 1 shows an example of one particular intersection i.

2.2 Threat Model

We consider a *local* adversary $\mathcal{A}$ that aims at tracking nodes: $\mathcal{A}$ has a limited number of eavesdropping stations to deploy in the network. As road intersections are strategic points of the network (through which all mobile nodes pass), we assume that the local adversary deploys its eavesdropping stations only at these places. Eavesdropping stations have a coverage area large enough to detect mobile nodes entering and exiting the intersection.

We assume a *passive* adversary: $\mathcal{A}$ cannot inject or modify messages [7]. $\mathcal{A}$ collects pseudonyms sniffed at every intersection where it has an eavesdropping station. Based on the collected information, it attempts to track the location of mobile nodes. Hence, the adversary threatens the location privacy of nodes [4].

2.3 Location Privacy Model

In order to defeat the tracking by an adversary, nodes can use multiple pseudonyms that they change over time. Nodes must coordinate pseudonym changes in regions called mix zones in order to prevent the spatial and temporal correlation of their location. We can distinguish between two types of mix zones: first, those

that, besides the pseudonym change, request user action, such as turning their transceivers off [17, 23] or using a mobile proxy [30]; second, mix zones where the nodes merely take advantage of the adversary's lack of coverage to change pseudonyms without any other action [6]. In this paper, we refer to the former as *active mix zones* and the latter as *passive mix zones*. In the following, we consider active mix zones created using silent periods.

We now quantify the location privacy provided by active mix zones in the presence of an attacker that eavesdrops on communications. As proposed in a previous work [3], we measure the uncertainty of $\mathcal{A}$ in matching mobile nodes that enter and exit an active mix zone. The uncertainty of the adversary is measured with an information-theoretic metric, the entropy [32]. To generalize this measure to an entire intersection, we compute the normalized entropy for each incoming road k and sum over all possible incoming roads with a weighted factor based on traffic intensity λ_k. We then divide the result by λ_i to get a normalized entropy H_i at intersection i:

$$H_i = \frac{1}{\lambda_i} \sum_{\forall k} \lambda_k \frac{-\sum_{\forall j} p_{kj}^i \log_2 p_{kj}^i}{\log_2 R_k^i} \tag{2}$$

where R_k^i is the total number of possible outgoing roads when entering at road k in intersection i, and p_{kj}^i is the probability that a node coming in intersection i via road k leaves via road j. The normalized entropy H_i captures the uncertainty of the adversary about the direction of nodes exiting an intersection.

Assuming that the monitoring and correlation processes become more difficult for the adversary with a higher number of nodes within the intersection, the uncertainty increases with the number of nodes entering the mix zone. Thus, we assume that the mixing effectiveness at intersection i is $m_i = \lambda_i H_i$, where λ_i is the total traffic intensity at intersection i.

In passive mix zones, mobile nodes can change pseudonyms in regions where the adversary has no coverage while continuing to communicate. However, if nodes change pseudonyms in a region where the adversary eavesdrops, the mixing effectiveness becomes equal to zero because the adversary can easily link nodes before and after a pseudonym change. If there is no eavesdropping station, we have $m_i = 1$. Note that we assume that at least two nodes traverse a passive mix zone and change pseudonyms.

3 A Game-Theoretic Approach to Location Privacy

In order to model the interaction between a local adversary and mobile nodes wanting to protect their location privacy, we define a static game G=($\mathcal{P}$, $\mathcal{S}$, $\mathcal{U}$). $\mathcal{P} = \{\mathcal{N}, \mathcal{A}\}$ is the players' set, where $\mathcal{N}$ corresponds to the aggregation of mobile nodes and $\mathcal{A}$ represents the adversary. $\mathcal{S}$ is the strategies' set. At any given intersection i, nodes can either *abstain* (A), deploy an *active mix zone* (M) or a *passive mix zone* (P), whereas the adversary can either *abstain* (A) or *eavesdrop* (E) on wireless communications. Thus, we get $\mathcal{S} = \{\mathcal{S}_{\mathcal{N}}^i, \mathcal{S}_{\mathcal{A}}^i\}_{i=1}^K$ with

Table 1. Normal form of game G at intersection i

$\mathcal{N}\backslash\mathcal{A}$	**Eavesdrop (E)**	**Abstain (A)**
Active mix zone (M)	$(\lambda_i m_i - c_p^i - c_q^i, \lambda_i(1-m_i) - c_s)$	$(\lambda_i - c_p^i - c_q^i, 0)$
Passive mix zone (P)	$(-c_p^i, \lambda_i - c_s)$	$(\lambda_i - c_p^i, 0)$
Abstain (A)	$(0, \lambda_i - c_s)$	$(0, 0)$

$\mathcal{S}_{\mathcal{N}}^i = \{M, P, A\}$ and $\mathcal{S}_{\mathcal{A}}^i = \{E, A\}$. Finally, $\mathcal{U}$ is the payoffs' set, where utility u for each player is equal to benefit b minus cost c.

When a player *abstains*, it has neither benefits nor costs, its payoff being zero (Table 1). An eavesdropping station is worth c_s for the adversary, regardless of the intersection i. On the nodes' side, a passive mix zone (P) and an active mix zone (M) cost $c_p^i = \alpha\lambda_i$ and $c_m^i = c_p^i + c_q^i = (\alpha + \beta)\lambda_i$, respectively. Value c_p^i encompasses the cost of acquiring new pseudonyms, whereas c_q^i is the cost of remaining silent for a certain period. When the adversary plays E and the nodes play M, the benefit of nodes is proportional to the mixing effectiveness m_i and the traffic intensity at intersection i (i.e., $\lambda_i m_i$) whereas the attacker's benefit is proportional to $(1 - m_i)$ and the traffic intensity (i.e., $\lambda_i(1 - m_i)$). If the adversary plays A, m_i is equal to 1 because the nodes are not tracked. Thus, the nodes' benefit is λ_i and the adversary's benefit is zero. If the nodes play P or A while the adversary plays E, nodes lose all their privacy benefits and the attacker earns a maximal benefit (i.e., λ_i). Note finally that all players' costs (c_m^i and c_s) and benefits (λ_i and m_i) are normalized between zero and one.

In real life, nodes may not know the total amount of investment $\Gamma \cdot c_s$ (Γ being the number of eavesdropping stations that the attacker can afford) made by the adversary to eavesdrop on the communications, and thus its stations' number and position around the network. Nodes have *incomplete information* about the attacker's strategy and payoff. To solve this problem, Harsanyi [15] proposes to introduce a new player called *Nature* that turns an incomplete information game into an *imperfect information* game. To do so, Nature assigns a type θ to the adversary's power according to a *probability density function* $f(\theta)$ known to the nodes. We assume here that the adversary is aware of the nodes' costs c_p^i and c_q^i. We thus have an asymmetric information game, meaning that the information sets of the players differ in ways relevant to their behavior. The adversary has useful private information: an information partition that is different and not worse than that of the nodes [28]. Table 2 summarizes the notation used throughout the paper.

4 Game Results

In this section, we first analyze the complete information game, at one and then at K intersections ($\mathcal{C}_1$-game and $\mathcal{C}_K$-game). Then, we extend the analysis to the incomplete information $\mathcal{I}_1$-game and $\mathcal{I}_K$-game.

Table 2. List of symbols.

Symbol	Definition
K	Number of intersections in the network
$\mathcal{N}$	Mobile nodes
$\mathcal{A}$	Adversary
λ_i	Normalized traffic intensity at intersection i
m_i	Mixing effectiveness of an active mix zone at intersection i
c_p^i	Nodes' cost of changing pseudonyms at intersection i
α	Cost of changing pseudonym per node
c_q^i	Nodes' cost of remaining silent at intersection i
β	Cost of being silent per node
c_m^i	Active mix zone cost: $c_p^i + c_q^i$
c_s	Adversary's cost of installing an eavesdropping station
θ	Nodes' belief in the type of the adversary
$f(\theta)$	Probability density function of the nodes' belief
$F(\theta)$	Cumulative distribution function of the nodes' belief
Γ	Total number of eavesdropping stations
$z_{\mathcal{A}}^i$	Nodes' belief in the presence of an eavesdropping station at intersection i
$u_{\mathcal{N}}^i$	Nodes' payoff function at intersection i
$u_{\mathcal{A}}^i$	Adversary's payoff function at intersection i
$s_{\mathcal{N},i}$	Nodes' strategy at intersection i
$s_{\mathcal{A},i}$	Adversary's strategy at intersection i
$s_{\mathcal{N},i}^*$	Nodes' best response at intersection i
$s_{\mathcal{A},i}^*$	Adversary's best response at intersection i
$u_{tot}^{\mathcal{N}}$	Nodes' global payoff function
$u_{tot}^{\mathcal{A}}$	Adversary's global payoff function

4.1 Complete Information Game

We begin the analysis with $\mathcal{C}_1$-game. The following theorem identifies all Nash equilibria (NE) of the game at one intersection with complete information.[1]

Theorem 1. *The $\mathcal{C}_1$-game has either a single pure-strategy Nash equilibrium:*

$$(s_{\mathcal{N},i}^*, s_{\mathcal{A},i}^*) = \begin{cases} (M,E) & \text{if} \quad (c_s < \lambda_i(1-m_i)) \wedge (c_m^i < \lambda_i m_i) \\ (P,A) & \text{if} \quad (c_s > \lambda_i) \wedge (c_p^i < \lambda_i) \\ (A,E) & \text{if} \quad (c_s < \lambda_i) \wedge (c_m^i > \lambda_i m_i) \\ (A,A) & \text{if} \quad (c_s > \lambda_i) \wedge (c_p^i > \lambda_i) \end{cases}$$

or a single mixed-strategy NE:

$$(s_{\mathcal{N},i}^*, s_{\mathcal{A},i}^*) = (x_{\mathcal{N}}^i, x_{\mathcal{A}}^i) \quad \text{if} \quad (\lambda_i(1-m_i) < c_s < \lambda_i) \wedge (c_m^i < \lambda_i m_i)$$

where $x_{\mathcal{N}}^i = \frac{\lambda_i - c_s}{\lambda_i m_i}$ is the probability of using an active mix zone at intersection i and $x_{\mathcal{A}}^i = \min(\frac{c_q^i}{\lambda_i m_i}, 1)$ is the probability of eavesdropping at intersection i. Moreover, $P(s_{\mathcal{N},i}^* = P) = 1 - x_{\mathcal{N}}^i$ and $P(s_{\mathcal{N},i}^* = A) = 0$.

[1] For convenience's sake, we focus in this paper on strict inequalities between benefits and costs.

Proof. We first distinguish five different cases that encompass all possible scenarios. For four of them, we get pure-strategy Nash equilibria, computed by finding both players' best responses in Table 1. In the last case, if

$$\begin{cases} \lambda_i(1-m_i) < c_s < \lambda_i \\ c_m^i < \lambda_i m_i \end{cases}$$

there is no pure-strategy Nash equilibrium. However, we can derive a mixed-strategy Nash equilibrium. As nodes' strategy A is dominated by strategy M, it will never be used by the nodes. Then, we can find the mixed-strategy Nash equilibrium by simply finding the mixed-strategy Nash equilibrium of the 2-by-2 game shown in Table 3.

Table 3. Reduced $\mathcal{C}_1$-game for mixed-strategy Nash equilibrium

$\mathcal{N}\backslash\mathcal{A}$	**Eavesdrop (E)**	**Abstain (A)**
Active mix zone (M)	$(\lambda_i m_i - c_p^i - c_q^i, \lambda_i(1-m_i) - c_s)$	$(\lambda_i - c_p^i - c_q^i, 0)$
Passive mix zone (P)	$(-c_p^i, \lambda_i - c_s)$	$(\lambda_i - c_p^i, 0)$

Assuming that

$$\begin{cases} Pr(s_{\mathcal{N},i} = M) = x_{\mathcal{N}}^i \\ Pr(s_{\mathcal{A},i} = E) = x_{\mathcal{A}}^i \end{cases},$$

we can solve

$$\begin{cases} x_{\mathcal{A}}^i(\lambda_i m_i - c_p^i - c_q^i) + (1-x_{\mathcal{A}}^i)(\lambda_i - c_p^i - c_q^i) = -x_{\mathcal{A}}^i c_p^i + (1-x_{\mathcal{A}}^i)(\lambda_i - c_p^i) \\ x_{\mathcal{N}}^i(\lambda_i(1-m_i) - c_s) + (1-x_{\mathcal{N}}^i)(\lambda_i - c_s^i) = 0 \end{cases},$$

and obtain the following mixed-strategy Nash equilibrium:

$$\begin{cases} P\{s_{\mathcal{N}}^i = M\} = \frac{\lambda_i - c_s}{\lambda_i m_i} \\ P\{s_{\mathcal{N}}^i = P\} = 1 - \frac{\lambda_i - c_s}{\lambda_i m_i} \\ P\{s_{\mathcal{A}}^i = E\} = \min(\frac{c_q^i}{\lambda_i m_i}, 1) \\ P\{s_{\mathcal{A}}^i = A\} = \max(1 - \frac{c_q^i}{\lambda_i m_i}, 0) \end{cases}$$

□

Theorem 1 shows that participants' strategies at NE are highly dependent on the traffic profiles at each specific intersection. The adversary plays E at NE either if the eavesdropping cost is low ($c_s < \lambda_i(1-m_i)$), or if it is not too high ($c_s < \lambda_i$) and the nodes do not use an active mix zone at the same place. The nodes play M if c_m^i is small enough for given traffic intensity and mixing effectiveness ($c_m^i < \lambda_i m_i$). If the adversary abstains and the cost of changing pseudonym is not prohibitive ($c_p^i < \lambda_i$), they play P. Nodes abstain if the adversary is eavesdropping and c_m^i is not small enough to be beneficial for them. For a high pseudonym cost ($c_p^i > \lambda_i$), nodes abstain as well, regardless

of the adversary's strategy. Finally, if c_s is neither too high nor too low and c_m^i small, players' best responses do not converge to a pure-strategy NE, leading to a mixed-strategy NE as defined in the theorem.

We will now extend the $\mathcal{C}_1$-game to the $\mathcal{C}_K$-game for K intersections. The $\mathcal{C}_K$-game can be viewed as a *supergame* with K simultaneous moves as defined in [24]. Because the strategy profiles are independent at different intersections and the set of strategies is not restricted by any constraints, both players can determine their best responses with $\mathcal{C}_1$-games at K intersections and aggregate them to get their $\mathcal{C}_K$-game best responses. This *supergame* NE can be defined by the union of the K NE of $\mathcal{C}_1$-games as follows:

$$(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}}) = \bigcup_{i=1}^{K} (s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i}) \tag{3}$$

and the *supergame* payoff is the sum of payoffs provided by each $\mathcal{C}_1$-game:

$$\begin{cases} u^{\mathcal{N}}_{\text{tot}}(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}}) = \sum_{i=1}^{K} u^i_{\mathcal{N}}(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i}), \text{ for the nodes} \\ u^{\mathcal{A}}_{\text{tot}}(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}}) = \sum_{i=1}^{K} u^i_{\mathcal{A}}(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i}), \text{ for the adversary} \end{cases} \tag{4}$$

However, a local adversary cannot afford an unlimited number of eavesdropping stations. The total number of eavesdropping stations is thus assumed to be capped by an upper bound Γ. Consequently, the NE strategy profile $(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}})$ of the $\mathcal{C}^{\Gamma}_K$-game can be defined as:

$$\boldsymbol{s}^*_{\mathcal{N}} \in \arg\max_{\boldsymbol{s}_{\mathcal{N}}} u^{\mathcal{N}}_{tot}(\boldsymbol{s}_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}}) \tag{5}$$

$$\begin{cases} \boldsymbol{s}^*_{\mathcal{A}} \in \arg\max_{\boldsymbol{s}_{\mathcal{A}}} u^{\mathcal{A}}_{tot}(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}_{\mathcal{A}}) \\ \text{subject to } \sum_{i=1}^{K} \mathbf{1}_{s_{\mathcal{A},i}=E} \leq \Gamma \end{cases} \tag{6}$$

where the i^{th} row of vectors $\boldsymbol{s}_{\mathcal{N}}$ and $\boldsymbol{s}_{\mathcal{A}}$ is $s_{\mathcal{N},i}$ and $s_{\mathcal{A},i}$, respectively.

Algorithm BoundedAdvCoverage copes with the new constraint on adversary's eavesdropping stations in the $\mathcal{C}^{\Gamma}_K$-game. This algorithm enables us to find the equilibrium of the game under the adversary's constraint for the whole network.

In BoundedAdvCoverage, we assume that $m_1 < m_2 < ... < m_K$, i.e. the first intersection has the lowest mixing effectiveness. Using Theorem 1, the algorithm first computes independently the Nash equilibria at each intersection (line 1). Then, if the total number of eavesdropping stations among the K intersections is larger than Γ, the adversary has to remove some of them.

First, the adversary changes strategy from $x^i_{\mathcal{A}}$ to A at the intersections where it has mixed strategies (lines 2 to 6). As the expected payoff of the adversary at mixed-strategy NE is equal to zero, it will not lose anything with this change. Note that the adversary starts with the intersection that has a mixed-strategy NE with smallest i (line 2), as this removes a mixed strategy with the highest probability of eavesdropping. If the first move is not sufficient, it considers the next intersection with a mixed-strategy NE. This continues until either the

Algorithm 1 BoundedAdvCoverage.

1: compute the Nash equilibria at each intersection $\Rightarrow (\boldsymbol{s}^*_{\mathcal{N}}; \boldsymbol{s}^*_{\mathcal{A}})$
2: $i = 1$
3: **while** $(\sum_{i=1}^{K} \mathbf{1}_{s^*_{\mathcal{A},i}=E} > \Gamma) \wedge ((s^*_{\mathcal{N},i}; s^*_{\mathcal{A},i}) = (x^i_{\mathcal{N}}, x^i_{\mathcal{A}}))$ **do**
4: $\quad (s^*_{\mathcal{N},i}; s^*_{\mathcal{A},i}) = (P; A)$
5: $\quad i = i + 1$
6: **end while**
7: **while** $(\sum_{i=1}^{K} \mathbf{1}^*_{s_{A,i}=E} > \Gamma)$ **do**
8: $\quad j = \underset{i, u^i_{\mathcal{A}} \neq 0}{\arg\min}\ u^i_{\mathcal{A}}(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i})$
9: $\quad$ **if** $(c^j_p < \lambda_j)$ **then**
10: $\quad\quad (s^*_{\mathcal{N},j}, s^*_{\mathcal{A},j}) = (P, A)$
11: $\quad$ **else**
12: $\quad\quad (s^*_{\mathcal{N},j}, s^*_{\mathcal{A},j}) = (A, A)$
13: $\quad$ **end if**
14: **end while**

number of eavesdropping stations is smaller than Γ, or there are no more intersections with mixed-strategy NE. In the latter case, the adversary then moves to the second step of the algorithm (line 7) and removes its eavesdropping stations at intersections with pure-strategy NE, starting with the intersection where its payoff is the smallest (line 8). In this case, each time the adversary changes strategy, it reduces its number of eavesdropping stations by one. The adversary obviously stops this removal process when the constraint Γ is satisfied.

As nodes do not have any constraints on cost, they just concentrate on their best responses with respect to the new strategy of the adversary. The nodes' best response if the adversary does not have any eavesdropping station is to deploy a passive mix zone if and only if $c^i_p < \lambda_i$ (line 9). In this case, a new local equilibrium appears: $(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i}) = (P, A)$ (line 10). Whereas, if $c^i_p > \lambda_i$, the new NE is $(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i}) = (A, A)$ (line 12).

Theorem 2. *The $\mathcal{C}^{\Gamma}_K$-game has a single Nash equilibrium, provided by the K $\mathcal{C}_1$-games equilibria and the* BoundedAdvCoverage *algorithm.*

Proof. The BoundedAdvCoverage algorithm removes the eavesdropping stations in order to maximize the payoff of the adversary with the available eavesdropping stations, i.e. Γ. This algorithm also derives the nodes' best response with respect to the new adversary's strategy. Hence, the strategy profile $(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}})$ is an equilibrium because no player is interested in unilaterally changing strategy. □

4.2 Incomplete Information Game

We extend the analysis to $\mathcal{I}$-games, where the mobile nodes have incomplete information about the adversary's payoff and strategy. Nodes must predict the attacker's best strategy based on the probability distribution $f(\theta)$ representing

the nodes' belief in the adversary's type. For the purpose of analysis, we suppose that the nodes know Γ but do not know c_s that will be modeled by θ. Indeed, if c_s increases, the adversary will need more money if it wants to deploy the same number of eavesdropping stations. The power of the adversary is always relative to the cost of eavesdropping.[2]

Definition 1. *The strategy profile $(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i})$ is a pure-strategy Bayesian Nash equilibrium (BNE) of the $\mathcal{I}_1$-game at intersection i if and only if*

$$\begin{cases} s^*_{\mathcal{N},i} \in \underset{s_{\mathcal{N},i} \in \mathcal{S}^i_{\mathcal{N}}}{\arg\max}\ E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i}, s^*_{\mathcal{A},i}(\theta))] \\ s^*_{\mathcal{A},i} \in \underset{s_{\mathcal{A},i} \in \mathcal{S}^i_{\mathcal{A}}}{\arg\max}\ u^i_{\mathcal{A}}(s^*_{\mathcal{N},i}, s_{\mathcal{A},i}) \end{cases} \tag{7}$$

Let $z^i_{\mathcal{A}} = Pr\{s^*_{\mathcal{A},i} = E\}$ be the probability that the adversary installs an eavesdropping station at intersection i, in a given equilibrium. The following lemma provides the computation of $z^i_{\mathcal{A}}$ by the nodes, for any given distribution of adversary's type.

Lemma 1. *Supposing that $F(\theta)$ is the cumulative distribution function of the type of the eavesdropping station's cost, the nodes will assume that the adversary will play E at intersection i with probability*

$$z^i_{\mathcal{A}} = \begin{cases} F(\lambda_i(1-m_i)) + \min(\frac{c^i_q}{\lambda_i m_i}, 1)(F(\lambda_i) - F(\lambda_i(1-m_i))) & \text{if } c^i_m < \lambda_i m_i \\ F(\lambda_i) & \text{if } c^i_m > \lambda_i m_i \end{cases} \tag{8}$$

Proof. Nodes would like to express the probability that the adversary places an eavesdropping station based on the distribution probability $f(\theta)$ of the cost's type of such an eavesdropping station. First, let us define the cumulative distribution function of the cost's type:

$$F(\theta) = P(\Theta < \theta) = \int_0^\theta f(u)du$$

Moreover,

$$P(a < \Theta < b) = \int_a^b f(u)du = F(b) - F(a)$$

Assuming that nodes know the probability density function (and thus the cumulative distribution function), they can evaluate $z^i_{\mathcal{A}} = P(s^*_{\mathcal{A},i} = E)$ using the law of total probability:

$$\begin{aligned} P(s^*_{\mathcal{A},i} = E) &= P(s^*_{\mathcal{A},i} = E | \Theta < \lambda_i(1-m_i))P(\Theta < \lambda_i(1-m_i)) \\ &+ P(s^*_{\mathcal{A},i} = E | \lambda_i(1-m_i) < \Theta < \lambda_i)P(\lambda_i(1-m_i) < \Theta < \lambda_i) \\ &+ P(s^*_{\mathcal{A},i} = E | \Theta > \lambda_i)P(\Theta > \lambda_i) \end{aligned}$$

[2] It is similar to the purchasing power of consumers, which is relative to the level of goods/services' prices.

As $P(s^*_{\mathcal{A},i} = E|\Theta > \lambda_i) = 0$ and $P(s^*_{\mathcal{A},i} = E|\Theta < \lambda_i(1-m_i)) = 1$, we get

$$\begin{aligned} P(s^*_{\mathcal{A},i} = E) &= P(\Theta < \lambda_i(1-m_i)) \\ &\quad + P(s^*_{\mathcal{A},i} = E|\lambda_i(1-m_i) < \Theta < \lambda_i) P(\lambda_i(1-m_i) < \Theta < \lambda_i) \\ &= F(\lambda_i(1-m_i)) \\ &\quad + P(s^*_{\mathcal{A},i} = E|\lambda_i(1-m_i) < \Theta < \lambda_i)(F(\lambda_i) - F(\lambda_i(1-m_i))) \end{aligned}$$

There remains to express $P(s^*_{\mathcal{A},i} = E|\lambda_i(1-m_i) < \Theta < \lambda_i)$. Nodes can evaluate this probability using results of Theorem 1:

$$P(s^*_{\mathcal{A},i} = E|\lambda_i(1-m_i) < \Theta < \lambda_i) = \begin{cases} 1 & \text{if } c^i_m > \lambda_i m_i \\ \min(\frac{c^i_q}{\lambda_i m_i}, 1) & \text{if } c^i_m < \lambda_i m_i \end{cases}$$

□

Using Lemma 1, the nodes can then find their best response that maximizes their payoff. This is shown with the following lemma.

Lemma 2. *The nodes' best response in $\mathcal{I}_1$-game is:*

$$s^*_{\mathcal{N},i} = \begin{cases} M & \text{if} \quad (c^i_q < z^i_{\mathcal{A}} \lambda_i m_i) \wedge (c^i_m < \lambda_i(1 - z^i_{\mathcal{A}}(1-m_i))) \\ P & \text{if} \quad (c^i_q > z^i_{\mathcal{A}} \lambda_i m_i) \wedge (c^i_p < (\lambda_i(1 - z^i_{\mathcal{A}})) \\ A & \text{if} \quad (c^i_m > \lambda_i(1 - z^i_{\mathcal{A}}(1-m_i))) \wedge (c^i_p > \lambda_i(1 - z^i_{\mathcal{A}})) \end{cases} \tag{9}$$

Proof. First, let us explicitly write the expected payoff:

$$E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i}, s^*_{\mathcal{A},i}(\theta))] = z^i_{\mathcal{A}} u^i_{\mathcal{N}}(s_{\mathcal{N},i}, s^*_{\mathcal{A},i} = E) + (1 - z^i_{\mathcal{A}}) u^i_{\mathcal{N}}(s_{\mathcal{N},i}, s^*_{\mathcal{A},i} = A)$$

In order to get $s^*_{\mathcal{N},i} = M$, we must verify both conditions below:

$$\begin{cases} E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = M, s^*_{\mathcal{A},i}(\theta))] > E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = P, s^*_{\mathcal{A},i}(\theta))] \\ E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = M, s^*_{\mathcal{A},i}(\theta))] > E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = A, s^*_{\mathcal{A},i}(\theta))] \end{cases}$$

or, explicitly:

$$\begin{cases} z^i_{\mathcal{A}}(\lambda_i m_i - c^i_p - c^i_q) + (1 - z^i_{\mathcal{A}})(\lambda_i - c^i_p - c^i_q) > -z^i_{\mathcal{A}} c^i_p + (1 - z^i_{\mathcal{A}})(\lambda_i - c^i_p) \\ z^i_{\mathcal{A}}(\lambda_i m_i - c^i_p - c^i_q) + (1 - z^i_{\mathcal{A}})(\lambda_i - c^i_p - c^i_q) > 0 \end{cases}$$

or, by simplifying:

$$\begin{cases} c^i_q < z^i_{\mathcal{A}} \lambda_i m_i \\ c^i_p + c^i_q = c^i_m < \lambda_i(1 - z^i_{\mathcal{A}}(1-m_i)) \end{cases}$$

We can prove in the same way both other best responses. For $s^*_{\mathcal{N},i} = P$,

$$\begin{cases} E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = P, s^*_{\mathcal{A},i}(\theta))] > E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = M, s^*_{\mathcal{A},i}(\theta))] \\ E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = P, s^*_{\mathcal{A},i}(\theta))] > E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = A, s^*_{\mathcal{A},i}(\theta))] \end{cases}$$

must be verified, and

$$\begin{cases} E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = A, s^*_{\mathcal{A},i}(\theta))] > E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = M, s^*_{\mathcal{A},i}(\theta))] \\ E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = A, s^*_{\mathcal{A},i}(\theta))] > E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i} = P, s^*_{\mathcal{A},i}(\theta))] \end{cases}$$

for $s^*_{\mathcal{N},i} = A$. □

Note that the adversary has complete information, and consequently can obtain its best response using the calculated payoffs in Table 1. This is shown by the following lemma.

Lemma 3. *The adversary's best response of the $\mathcal{I}_1$-game is*

$$s^*_{\mathcal{A},i} = \begin{cases} E & \text{if} \quad (c_s < \lambda_i(1-m_i)) \vee ((\lambda_i(1-m_i) < c_s < \lambda_i) \wedge (s^*_{\mathcal{N},i} \neq M)) \\ A & \text{if} \quad (c_s > \lambda_i) \vee ((\lambda_i(1-m_i) < c_s < \lambda_i) \wedge (s^*_{\mathcal{N},i} = M)) \end{cases} \tag{10}$$

Considering Lemmas 1, 2 and 3, we immediately have the following theorem.

Theorem 3. *The $\mathcal{I}_1$-game has at least one pure-strategy Bayesian Nash equilibrium.*

Proof. As the Bayesian NE is defined by the players' mutual best responses (Definition 1), the result follows from Lemmas 1, 2, and 3. □

Note that, comparing to the $\mathcal{C}_1$-game, (M, A) and (P, E) can also be pure-strategy BNE for the $\mathcal{I}_1$-game. For example, (M, A) is a BNE if the nodes believe that the cost of an eavesdropping station is small, whereas in reality the actual cost of an eavesdropping station is high (typically greater than λ_i). If the mobile nodes had perfect knowledge about the adversary's payoff, they would have deployed a passive mix zone instead of an active mix zone. Similarly, the nodes deploy passive mix zone at (P, E) BNE due to incomplete information about the adversary, which degrades their location privacy.

We now generalize our $\mathcal{I}_1$-game to the $\mathcal{I}^{\Gamma}_K$-game by aggregating all the equilibria at each intersection and sum the payoffs of all intersections to obtain the *supergame* payoffs for both participants. Similarly, the BNE strategy profile $(\boldsymbol{s}^*_{\mathcal{N}}, \boldsymbol{s}^*_{\mathcal{A}})$ can be expressed as:

$$\boldsymbol{s}^*_{\mathcal{N}} \in \arg\max_{\boldsymbol{s}_{\mathcal{N}}} \sum_{i=1}^{K} E_\theta[u^i_{\mathcal{N}}(s_{\mathcal{N},i}, s^*_{\mathcal{A},i}(\theta))] \tag{11}$$

$$\begin{cases} \boldsymbol{s}^*_{\mathcal{A}} \in \arg\max_{\boldsymbol{s}_{\mathcal{A}}} \sum_{i=1}^{K} u^i_{\mathcal{A}}(s^*_{\mathcal{N},i}, s_{\mathcal{A},i}) \\ \text{subject to } \sum_{i=1}^{K} \mathbf{1}_{s_{\mathcal{A},i}=E} \leq \Gamma \end{cases} \tag{12}$$

BayesianBoundedAdvCoverage algorithm enables the players to find the BNE of the $\mathcal{I}^{\Gamma}_K$-game.

The algorithm first computes the BNE at each intersection independently, using Theorem 3. Then, the adversary removes eavesdropping stations at intersections where they provide the smallest payoffs (lines 3 and 4), until its total

Algorithm 2 BayesianBoundedAdvCoverage.

1: compute the Bayesian Nash equilibria at each intersection $\Rightarrow (\boldsymbol{s}^*_{\mathcal{N}}; \boldsymbol{s}^*_{\mathcal{A}})$
2: **while** $(\sum_{i=1}^{K} \mathbf{1}^*_{s_{\mathcal{A},i}=E} > \Gamma)$ **do**
3: $\quad j = \underset{i, u^i_{\mathcal{A}} \neq 0}{\arg\min}\ u^i_{\mathcal{A}}(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i})$
4: $\quad s^*_{\mathcal{A},j} = A$
5: **end while**
6: **for** $i = 1 : K - \Gamma$ **do**
7: $\quad j = \underset{i \neq k, \forall k < i}{\arg\min}\ E[u^i_{\mathcal{A}}(s^*_{\mathcal{N},i}, s^*_{\mathcal{A},i} = E)]$
8: $\quad$ **if** $(c^j_p < \lambda_j)$ **then**
9: $\quad\quad s^*_{\mathcal{N},j} = P$
10: $\quad$ **else**
11: $\quad\quad s^*_{\mathcal{N},j} = A$
12: $\quad$ **end if**
13: **end for**

Table 4. Number of NE (among all intersections)

scenario\NE	$(\mathbf{M}, \mathbf{E})$	$(\mathbf{A}, \mathbf{E})$	$(\mathbf{P}, \mathbf{A})$	**mixed**
$\mathbf{c_s = 0.1, \Gamma = 23}$	17	6	0	0
$\mathbf{c_s = 0.1, \Gamma = 5}$	2	3	18	0
$\mathbf{c_s = 0.5, \Gamma = 23}$	2	3	5	13
$\mathbf{c_s = 0.5, \Gamma = 5}$	2	3	18	0

number of eavesdropping stations satisfies the upper bound Γ. The mobile nodes find the $K - \Gamma$ intersections where the expected payoff of the adversary playing E is the smallest (line 7). Indeed, these intersections are those where there is the highest probability that the adversary removes its eavesdropping stations. The nodes then play P at these intersections if $c^j_p < \lambda_j$ or play A if c^j_p is prohibitive.

5 Numerical Results

In this section, we evaluate our game-theoretic model by means of numerical results based on traffic data[3] from Lausanne [22]. For convenience, we concentrate on the $K = 23$ main intersections of Lausanne and use Matlab to numerically evaluate the results. We test both the $\mathcal{C}^{\Gamma}_K$-game and the $\mathcal{I}^{\Gamma}_K$-game, with different costs. Benefits depend on the traffic parameters λ_i and m_i.

5.1 Complete Information Game

Table 4 summarizes the results with different players' costs in the complete information scenario. In all of the four cases, nodes' costs are fixed: $c^i_p = \alpha\lambda_i = 0.1\lambda_i$ and $c^i_q = \beta\lambda_i = 0.1\lambda_i$. We sum the different NE at each intersection and

[3] The data are publicly available on http://icapeople.epfl.ch/mhumbert/tracking.

Table 5. Number of Bayesian Nash equilibria (BNE) among all intersections.

scenario\BNE	(M, E)	(P, E)	(A, E)	(M, A)	(P, A)	(A, A)
$\theta \sim \mathbf{U(0,1)}, \mathbf{c_s = 0.2}, \mathbf{\Gamma = 23}$	10	13	0	0	0	0
$\theta \sim \mathbf{U(0,1)}, \mathbf{c_s = 0.2}, \mathbf{\Gamma = 5}$	1	4	0	0	18	0
$\theta \sim \beta(\mathbf{2,5}), \mathbf{c_s = 0.2}, \mathbf{\Gamma = 23}$	16	3	4	0	0	0
$\theta \sim \beta(\mathbf{2,5}), \mathbf{c_s = 0.2}, \mathbf{\Gamma = 5}$	1	0	4	0	18	0
$\theta \sim \beta(\mathbf{2,5}), \mathbf{c_s = 0.5}, \mathbf{\Gamma = 23}$	2	0	2	14	3	2
$\theta \sim \beta(\mathbf{2,5}), \mathbf{c_s = 0.5}, \mathbf{\Gamma = 5}$	1	1	2	0	17	2

provide the results for two values of c_s (0.1 and 0.5). For each case, we solve the game with an unlimited and a limited number of stations ($\Gamma = 23$ and $\Gamma = 5$).

In the first scenario, as c_s is very low, the adversary plays E at each intersection. On the contrary, the nodes decide to abstain at six intersections, where m_i is too low to get a significant benefit, despite the relatively low price of an active mix zone (Figure 2(a)). In the second scenario, the adversary keeps eavesdropping stations at two intersections where there are active mix zones, instead of placing them at intersections free of mix zones (Figure 2(b)). This is due to the fact that, at those two intersections, the number of vehicles per hour is quite high, with a mixing effectiveness that does not confuse the adversary too much ($m_i < 0.5$). Finally, we notice that the nodes take advantage of their complete knowledge of the adversary's payoff to use passive mix zones wherever the attacker ceases eavesdropping.

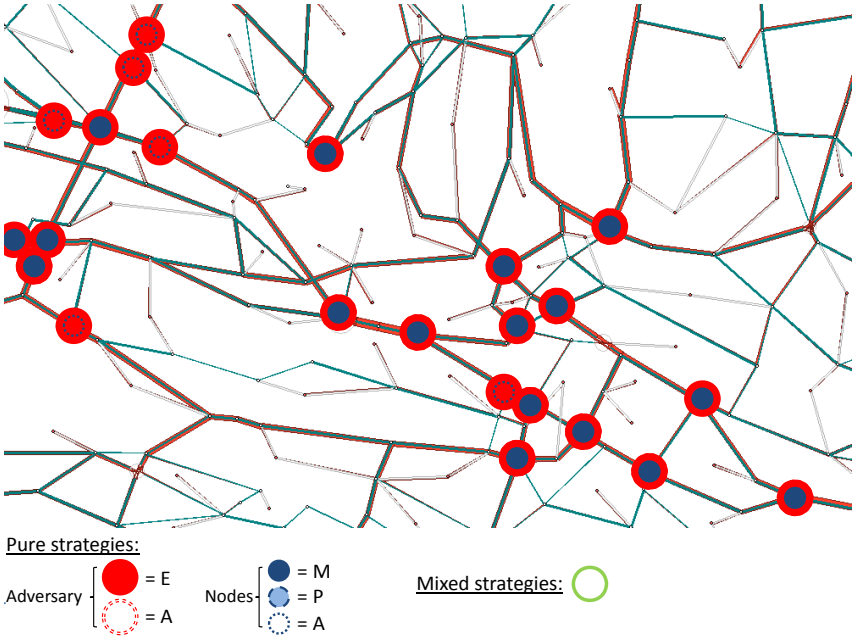
If c_s increases to 0.5 (third and fourth scenarios), the adversary deploys fewer eavesdropping stations, five in total without any limit on the stations' number (Figure 3). The eavesdropping stations tend to be placed at intersections with the lowest mixing effectiveness. Most surprising here is that the nodes' best responses change as well, showing that they are not independent of the adversary's strategies. Except for two intersections, the nodes and the adversary adopt complementary strategies. If the adversary places an eavesdropping station, the nodes abstain, whereas, if the adversary abstains, the nodes place a (passive) mix zone. If we limit the number of stations to five, we get the same resulting equilibrium as in Figure 2(a) and reach the same conclusions.

5.2 Incomplete Information Game

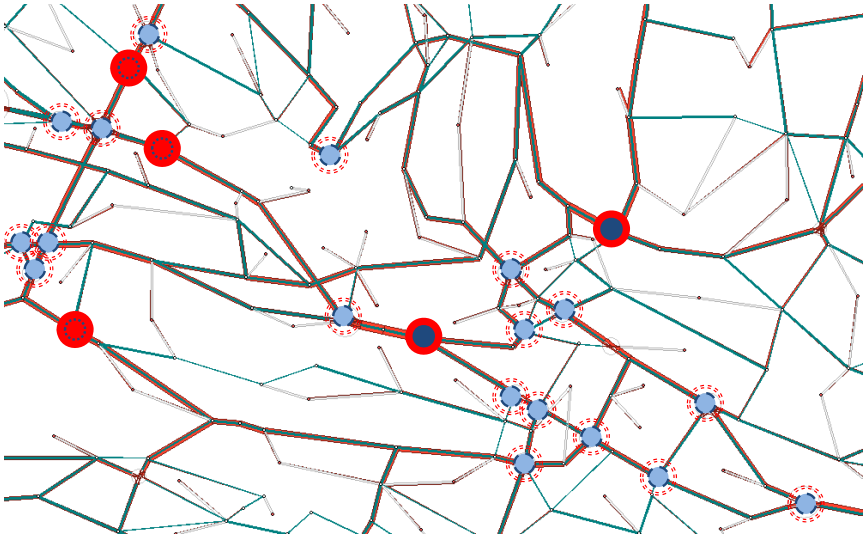
We model the imperfect nodes' knowledge of c_s by using two different probability distributions. First, the uniform distribution $U(0,1)$ represents the case when mobile nodes have no idea about c_s. Second, the beta distribution $\beta(2,5)$[4] models the case when the nodes' belief in c_s is more accurate. Table 5 summarizes the results of the $\mathcal{I}_K^\Gamma$-game.

In the first scenario, we notice that there are 13 intersections where the nodes deploy passive mix zones while the adversary is eavesdropping at the same places.

[4] The beta distribution is a family of continuous probability distributions defined on the interval $[0,1]$. $\beta(2,5)$ is maximal in 0.2 and its mean is equal to $2/7$.



(a)



(b)

Fig. 2. Maps of Lausanne downtown and strategies chosen (at the main 23 intersections) with $\alpha = 0.1$, $\beta = 0.1$ and $c_s = 0.1$. (a) Equilibrium with an unlimited number of eavesdropping stations, (b) Equilibrium with a limited number of eavesdropping stations (equal to five).

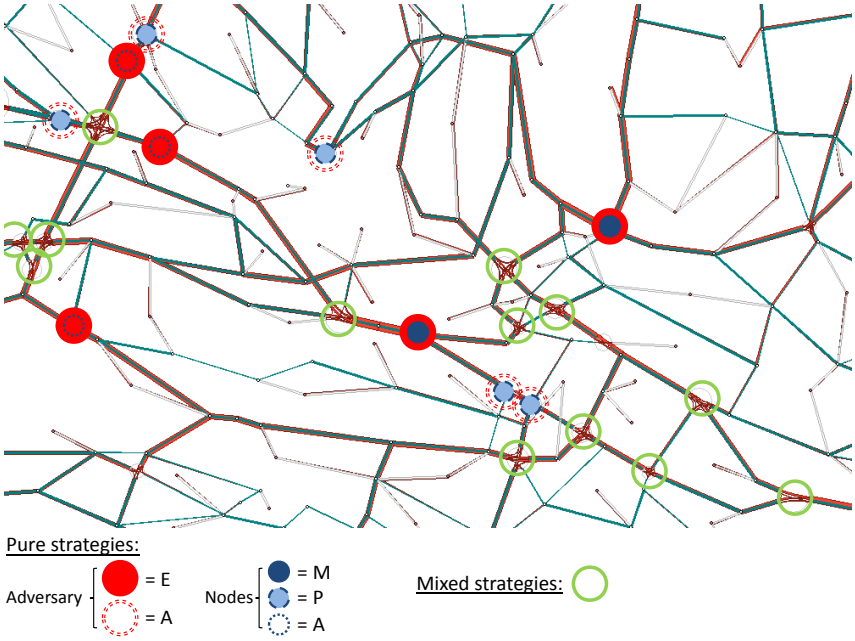


Fig. 3. Map of downtown Lausanne with $\alpha = 0.1$, $\beta = 0.1$ and $c_s = 0.5$. Equilibrium with an unlimited number of eavesdropping stations.

Nodes lose all their location privacy and pay the cost of changing pseudonyms, which leads to a negative payoff. The nodes have no clue about c_s, and thus must lay a bet on the adversary's payoff. Nodes believe that c_s is close to $E[\Theta] = 0.5$, whereas $c_s = 0.2$. Thus, the nodes think that the adversary will not play E everywhere, whereas it will, because of low actual c_s. We also notice that the nodes privilege passive mix zones at intersections with low m_i and active mix zones where m_i is higher. This is surprising because nodes should expect that the adversary places eavesdropping stations where the m_i is low, and thus deploy active mix zones at these intersections, instead of passive ones. In the second scenario, the nodes take advantage of the limited number of eavesdropping stations to deploy more passive mix zones. However, the nodes still have passive mix zones at four intersections out of five where the adversary keeps eavesdropping. Hence, in this case either, the BNE is not optimal for the nodes.

In the third and fourth scenarios, we observe that if nodes' knowledge about c_s becomes more accurate, the nodes' strategy at equilibrium leads to a higher payoff. There are three and no (P, E) in the third and fourth cases, respectively. The nodes know that $E[\Theta] = 2/7 \approx 0.29$, which is quite close to $c_s = 0.2$, leading to a much better strategy than with the uniform distribution.

The last two cases depict a nodes' wrong belief in c_s. Their belief is the same as in cases 3 and 4, but the real c_s is higher. This inaccuracy leads to a decrease on the nodes' payoff at BNE but not as significant as with a uniform

distribution. We can observe this especially in the fifth scenario. In this case, there are 14 (M, A) at BNE, whereas with a good knowledge on c_s, the nodes would have played P instead of M. Thus, nodes adopt non-optimal strategies, leading to a decrease in payoff equal to c_q^i (for intersection i). We also notice in the last case a single (P, E) and a single (M, E). The difference between these two intersections is in the value of m_i (both values of λ_i are high). In the former intersection, $m_i = 0.42$, whereas in the latter $m_i = 0.35$. Thus, nodes probably believe that the adversary ceases eavesdropping at the intersection with highest m_i, whereas it does not.

6 Conclusion

We have considered the problem of deploying mix zones in the presence of a passive adversary equipped with a limited number of eavesdropping stations. We have proposed a game-theoretic model to evaluate the strategic behaviors of both players in such *tracking games*. First, we analyze the complete information game and derive an algorithm to obtain NE strategy profiles for a large network. Second, we evaluate the incomplete information game where mobile nodes are uncertain about the placement of eavesdropping stations. We obtain a single pure-strategy Bayesian NE at one intersection. We also describe an algorithm to obtain the equilibrium in a large network. Finally, we evaluate using real road traffic statistics both the complete information and incomplete information games. Among other results, the numerical evaluations show that the adversary and mobile nodes often adopt complementary strategies when they have complete information: nodes place (passive) mix zones at locations where there are no eavesdropping stations, whereas the adversary deploys eavesdropping stations at places where there are no (active) mix zones. In the incomplete information case, we notice that mobile nodes' strategy (and thus payoff) highly depends on their belief about the type of adversary. Our results quantify how the lack of information by mobile nodes about the attacker's strategy leads to a significant decrease in the achievable location privacy level at BNE. In summary, our results enable system designers to predict the strategy of a local adversary and mobile nodes with limited capabilities in tracking games.

For future work, we intend to test our results by using traffic data from other cities and more precisely measure the mixing effectiveness using the sojourn times and the evolution of traffic over time. Moreover, we would like to extend our results to other kinds of mobile networks, such as pedestrian ones. We would also like to enrich our analysis by developing a scenario where the attacker leverages on the geographical positions and the interdependence of the intersections to improve his tracking power. This approach would require more complex strategies and utility functions, and the games at different intersections would no longer be independent [19]. Another extension of this work is the evaluation of the interactions between the attacker and the defenders by using repeated games.

Acknowledgements

We would like to thank Tansu Alpcan, Igor Bilogrevic, Joseph Y. Halpern and Georgios Theodorakopoulos for their insights and discussions about the game-theoretic analysis. We also thank Nevena Vratonjic and the anonymous reviewers for their helpful feedback. We are very grateful to Jean-Pierre Leyvraz for providing us with the traffic data of Lausanne.

References

1. Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity. In: Financial Cryptography (2003)
2. Aka-aki: http://www.aka-aki.com
3. Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing 2, 46–55 (2003)
4. Beresford, A.R., Stajano, F.: Mix zones: User privacy in location-aware services. In: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (2004)
5. Buchegger, S., Alpcan, T.: Security games for vehicular networks. In: 46th Annual Allerton Conference on Communication, Control, and Computing (2008)
6. Buttyán, L., Holczer, T., Vajda, I.: On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In: Security and Privacy in Ad-hoc and Sensor Networks (2007)
7. Buttyán, L., Hubaux, J.P.: Security and Cooperation in Wireless Networks. Cambridge University Press (2008)
8. Freudiger, J., Manshaei, M.H., Hubaux, J.P., Parkes, D.C.: On non-cooperative location privacy: a game-theoretic analysis. In: Proceedings of the 16th ACM conference on Computer and communications security (2009)
9. Freudiger, J., Raya, M., Felegyhazi, M., Papadimitratos, P., Hubaux, J.P.: Mix zones for location privacy in vehicular networks. In: Proc. 1st Intl. Wksp. Wireless Networking for Intelligent Transportation Systems (Win-ITS) (2007)
10. Freudiger, J., Shokri, R., Hubaux, J.P.: On the optimal placement of mix zones. In: Privacy Enhancing Technologies (2009)
11. Friedman, J.W.: A non-cooperative equilibrium for supergames. The Review of Economic Studies 38, 1–12 (1971)
12. Grossklags, J., Johnson, B., Christin, N.: The price of uncertainty in security games. In: Proceedings (online) of the Eighth Workshop on the Economics of Information Security (WEIS), London, UK (2009)
13. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on Mobile systems, applications and services (2003)
14. Halpern, J.Y., Teague, V.: Rational secret sharing and multiparty computation: extended abstract. In: Proceedings of the thirty-sixth annual ACM symposium on Theory of computing. pp. 623 – 632 (2004)
15. Harsanyi, J.: Games with incomplete information played by Bayesian players. Management Science 14, 159–182 (1967)
16. Hartenstein, H., Laberteaux, K.: A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine 46(6), 164–171 (2008)

17. Huang, L., Matsuura, K., Yamane, H., Sezaki, K.: Enhancing wireless location privacy using silent period. In: IEEE Wireless Communications and Networking Conference (2005)
18. Huang, L., Matsuura, K., Yamane, H., Sezaki, K.: Towards modeling wireless location privacy. In: Privacy Enhancing Technologies (2005)
19. Humbert, M.: Location Privacy amidst local Eavesdroppers. Master's thesis, EPFL (2009)
20. Isaacs, R.: Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization. Dover Publications (1999)
21. Katz, J.: Bridging game theory and cryptography: recent results and future directions. In: Theory of Cryptography (2008)
22. Leyvraz, J.P., Mattenberger, P., Robert-Grandpierre, A.: Mise à jour majeure de la modélisation EMME2 de l´agglomération Lausanne-Morges. Tech. Rep. TRANSP-OR 061208, EPFL (2006)
23. Li, M., Sampigethay, K., Huang, L., Poovendra, R.: Swing & swap: User centric approaches towards maximizing location privacy. In: Proceedings of the 5th ACM workshop on Privacy in electronic society (2006)
24. Luce, R.D., Raiffa, H.: Games and Decisions. Wiley (1957)
25. MIT Media Lab: Reality Mining. http://reality.media.mit.edu/serendipity.php
26. Nash, J.: Non-cooperative games. Annals of Mathematics 54 (1951)
27. Pfitzmann, A., Köhntopp, M.: Anonymity, unobservability, and pseudonymity - a proposal for terminology. In: Designing Privacy Enhancing Technologies (2001)
28. Rasmusen, E.: Games and information. Blackwell (1989)
29. Raya, M., Manshaei, M.H., Felegyhazi, M., Hubaux, J.P.: Revocation games in ephemeral networks. In: Proceedings of the 16th ACM conference on Computer and communications security (2008)
30. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: CARAVAN: providing location privacy for VANET. In: Proceedings of Embedded Security in Cars (ESCAR) (2005)
31. Schoch, E., Kargl, F., Leinmüller, T., Schlott, S., Papadimitratos, P.: Impact of pseudonym changes on geographic routing in VANETs. In: Security and Privacy in Ad-Hoc and Sensor Networks (2006)
32. Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In: Privacy Enhancing Technologies (2002)
33. Varian, H.R.: Economic aspects of personal privacy. In: Internet Policy and Economics (2009)