ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Preserving Location Privacy of Mobile Network

P. Sakthi Priyanka[1] and B. Raja Rajeswari, Tamilnadu, India[2]

M.E (CSE), Muthayammal Engineering College, Rasipuram, Tamilnadu, India[1, 2]

ABSTRACT: Mobile network consists of number of mobile nodes moving in the network randomly, 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. To 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. To 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—Pseudo Game protocols—based on the results of our analysis and simulate their performance in vehicular network scenarios, The pseudonyms key changes mainly used in many areas such as peer to peer communication and wireless network, because this network only each time change the location .Public and private key is used for transferring the information, number of routing algorithm is used for route the information.

KEYWORDS—Security and privacy protection, mobile computing, network protocols

I. INTRODUCTION

The mobile nodes are frequently changing their location, while change the location privacy of the mobile node is very important. The growing popularity of Bluetooth, WiFi in ad hoc mode, and other similar techniques is likely to fuel the adoption of peer-to-peer wireless communications. Corporations are developing wireless peer-to-peer technologies. 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. A change of 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 , i.e., a collective effort. One solution consists in changing pseudonyms periodically, at a predetermined 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 but this solution requires help from the infrastructure.

The approach in 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 coordinates pseudonym changes by forcing mobile nodes to change their pseudonyms within predetermined regions called mix zones. This approach lacks flexibility and is prone to attacks because a central authority fixes mix zone locations and must share them with mobile nodes.

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.

II. RELATED WORK

2.1 Mix Zones: User Privacy in Location-aware Services

Privacy of personal location information is becoming an increasingly important issue. This paper a method, called the mix zone, developed to enhance user privacy in location-based services. We improve the mathematical model, examine and minimize computational complexity and develop a method of providing feedback to users. Traditionally, privacy of personal location information has not been a critical issue but, with the development of location tracking systems capable of following user movement twenty-four hours a day and seven days a week, location privacy becomes important: records of everything from the shelves you visit in the library to the clinics you visit in a hospital can represent a very intrusive catalogue of data. Location privacy is an important new issue and several strategies have been suggested to protect personal location information. The access Geographic Location/Privacy (Geopriv) Working Group has outlined architecture to allow users to control delivery and accuracy of location information through rule-based policies. Hengartner and Steenkiste describe a method of using digital certificates combined with rule-based policies to protect location information. The attacker can observe the times, coordinates and pseudonyms of all these ingress and egress events. His ideal goal is to reconstruct the correct mapping between all the ingress events and the egress events. This is equivalent to discovering the mapping between new and old pseudonyms. During the period of observation, assume there are n ingress events and n egress events.4 the attacker observes n old pseudonyms going in, and n new pseudonyms coming out, most likely with some interleaving. Each permutation of the set of n new pseudonyms gives a new mapping.

2.2 On Neighbor Discovery in Wireless Networks with Directional Antennas

Several probabilistic algorithms in which nodes perform random, independent transmissions to discover their one-hop neighbors. Our neighbor discovery algorithms are classified into two groups, viz. *Direct- Discovery Algorithms* in which nodes discover their neighbors only upon receiving a transmission from their neighbors and *Gossip-Based Algorithms* in which nodes gossip about their neighbors' location information to enable faster discovery. consider the operation of these algorithms in a slotted, synchronous system and mathematically derive their optimal parameter settings. We show how to extend these algorithms for an asynchronous system and describe their optimal design. Analysis and simulation of the algorithms show that nodes discover their neighbors much faster using gossip-based algorithms than using direct-discovery algorithms. Furthermore, the performance of gossip-based algorithms is insensitive to an increase in node density. The efficiency of a neighbor discovery algorithm also depends on the choice of antenna bandwidth. Direct discovery algorithm is used for determining neighbor only hear the when they hear transmission from neighbors.Gossip based algorithm are insensitive. *Discovery Algorithms* in which nodes gossip about each others' location information to speed up discovery. Some of the important contributions of our work are:

1. A simple mathematical model to derive the optimal parameter settings for synchronous direct-discovery and gossip-based algorithms.

2. A simulation-based performance comparison of the gossip-based and the direct-discovery algorithms, demonstrating that nodes discover their neighbors significantly faster using the gossip-based algorithm than using the direct-discovery algorithm. Interestingly, we also see that while the performance of direct-discovery algorithm degrades as node density increases, the gossip-based algorithm remains insensitive to an increase in node density

2.3 FlashLinQ: A Synchronous Distributed Scheduler for Peer-to-Peer Ad Hoc Networks

Channel allocation: By leveraging the fine-grained parallel channel access of OFDM, FlashLinQ develops an analog energy-level based signaling scheme that enables SIR (Signal to Interference Ratio) based distributed scheduling. This new signaling mechanism and the corresponding allocation algorithms permit efficient channel-aware spatial resource allocation, leading to significant gains over a CSMA/CA system with RTS/CTS. FlashLinQ is a complete system architecture including (i) timing and frequency synchronization derived from cellular spectrum, (ii) peer discovery, (iii) link management, and (iv) channel aware distributed power, data-rate and link scheduling. implement FlashLinQ over licensed spectrum on a DSP/FPGA platform. To collect the data, the modem reports its current link scheduling status to the Linux based host every second

We prove the existence of one pure-strategy Bayesian Nash equilibrium in the single road intersection game and extend the result to a network of intersections. Finally, we test our model using real road 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 In wireless networks, the location tracking of devices and vehicles (nodes) based on their identifiable and locatable broadcasts, presents potential threats to the location privacy of their users. While the tracking of nodes can be mitigated to an extent by updating their identifiers to decorrelate their traversed locations, such an approach is still vulnerable to tracking methods that utilize the predictability of node movement to limit the location privacy provided by the identifier updates.

III. EXISTING SYSTEM

The promise of vehicular communications is to make road traffic safer and more efficient. However, besides the expected benefits, vehicular communications also introduce some privacy risk by making it easier to track the physical location of vehicles. One approach to solve this problem is that the vehicles use pseudonyms that they change with some frequency. In this paper, we study the effectiveness of this approach. We define a model based on the concept of the *mix zone*, characterize the tracking strategy of the adversary in this model, and introduce a metric to quantify the level of privacy enjoyed by the vehicles. We also report on the results of an extensive simulation where we used our model to determine the level of privacy achieved in realistic scenarios.

In particular, in our simulation, we used a rather complex road map, generated traffic with realistic parameters, and varied the strength of the adversary by varying the number of her monitoring points. Our simulation results provide detailed information about the relationship between the strength of the adversary and the level of privacy achieved by changing pseudonyms. In particular, many envisioned safety related applications require that the vehicles continuously broadcast their current position and speed in so called *heart beat* messages .

We consider a continuous part of a road network, such as a whole city or a district of a city. We assume that the adversary installed some radio receivers at certain points of the road network with which she can eavesdrop the communications of the vehicles, including their heart beat messages, in a limited range. On the other hand, outside the range of her radio receivers, the adversary cannot hear the communications of the vehicles .Thus, we divide the road network into two distinct regions: the observed zone and the unobserved zone. Physically, these zones may be scattered, possibly consisting of many observing *spots* and a large unobserved area, but logically, the scattered observing spots can be considered together as a single observed zone.

We derive the delay distribution and the average total delay of a vehicle within a density zone. Given the delay information, an adversary may still be available to track the target vehicle by a selection rule. We investigate the effectiveness of DLP based on extensive simulation study. all to both the traffic arrival rate and the variance of vehicles' speed. Our proposed DLP scheme also has a better performance than both Mix-Zone scheme and AMOEBA with random silent period. We propose the vehicle density-based location privacy(DLP) scheme, which can mitigate the location tracking of vehicles by changing pseudonyms based on a threshold in neighboring vehicle count within a density zone.2)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

We derive the delay distribution and the expected total delay of a vehicle within the density zone. Given the delay information, an adversary may still be available to track the target vehicle based on a selection rule. 3) Simulation results show that the probability of successful location tracking by an adversary is inversely proportional to the intensity of the traffic and the variance of the vehicles' speed. Our proposed DLP scheme outperforms both AMOEBA (with random silent period) and Mix-Zone Schemes in reducing the probability of successful tracking by an adversary. The effectiveness of changing pseudonyms to provide location privacy in VANETs.

IV. PROPOSED SYSTEM

Protecting the location the location of mobile nodes from preventing third parties learning mobile node past and present location.To avoid the attack the pseudonym changes delete from present and past memory.The user centric model is proposed for enhance the privacy for particular threshold value.Each node in the network decide to take the decision about to change their position or not.During the silent period the node cannot take the position about the psedunoym Changes.psedunoym game protocol is proposed for take descision about position changes in mix zone.This protocol is based on the coordinate the pseudonym changes. 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. Different type of equation is used for psedunoym changes. Dynamic games of incomplete information can be solved using the concept of perfect Bayesian equilibrium (PBE).In the network each player connected in the network.Each node know the tree of all other nodes in the network.In user centric model node give the request to the other nodes in their proximity.user centric model update the changes of mobile node location.

PROPOSED SYSTEM ARCHITECTURE

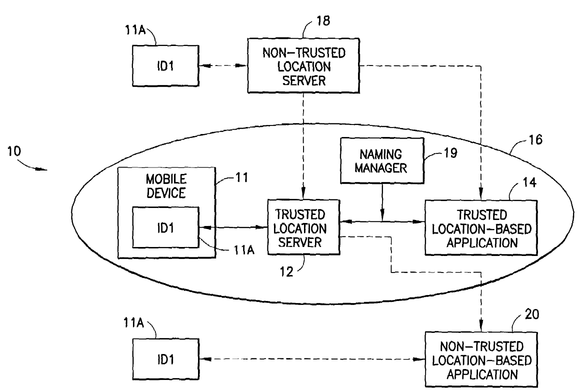


Fig 1: proposed system architecture

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 pseudonyms an the available location privacy gain (upperbounded by the density of nodes and their locations unpredictability.

.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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

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. Game theory allows for modeling situations of conflict and for predicting the behavior of participants deciding whether or not to change their pseudonym, e.g., during the sile period, nodes cannot observe each other messages.

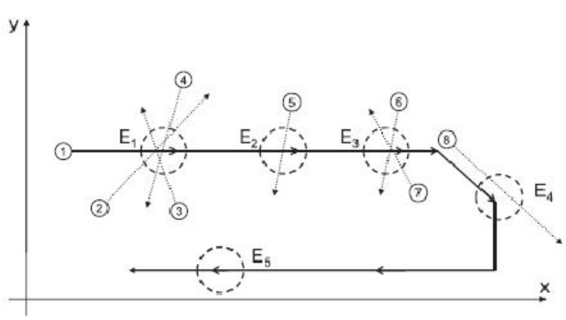
TABLE 1
2-Player Strategic Form $\mathcal{C}$-Game

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

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)

4.1 Players

The set of players corresponds to the set of mobile nodes in transmission range of each other at time t. For a valid game we require no > 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



4.2 Payoff Function

We model the payoff function of every node level of location privacy of node i at time t, whereas the cost 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. If a node is alone in changing its pseudonym, then it still pays the cost 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 $(s_i = C) \wedge (n_C(s_{-i}) > 0)$,

$$T_i^\ell := t$$

$$\alpha_i(t, T_i^\ell) := 0$$

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

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

$$u_i(t, T_i^\ell, C, s_i) := \max(0, u_i^- - \gamma)$$

$$\alpha_i(t, T_i^\ell) := \alpha_i(t, T_i^\ell) + 1.$$

If $(s_i = D)$,

$$u_i(t, T_i^\ell, D, s_i) := \max(0, u_i^-),$$

4.3 Register with public key

Wireless communications are inherently dependent on geographic proximity: mobile devices detect each other's presence by periodically broadcasting beacon messages .A aims to track the location of mobile nodes. We consider that A can have the same credentials as mobile nodes and is equipped to eaves drop communications. In the worst case, a global adversary A obtains complete coverage and tracks nodes throughout the entire network, by placing. 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.

V. CONCLUSION

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 equilibriums 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 Pseudo Game protocols, which coordinate pseudonym changes. An intriguing result is that when uncertainty about others' strategies is high (i.e., static games), rational nodes care more about the successful unfolding of the game if the cost of pseudonyms is also high. 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.

REFERNCES

1.G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 56–64, Mar. 2003.

2. M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys)*, San Francisco, CA, May 2003.

3.E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, Impact of pseudonym changes on geographic routing in VANETs," *Lecture Notes in Computer Science (LNCS)*, vol. 4357, pp. 43–57, Mar. 2007.

4. E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of anonymity in VANETs - Putting pseudonymity into practice," in *Proc. Of IEEE WCNC*, Hong Kong, China, Mar. 2007.

5.. M. Lei, X. Hong, and S. V. Vrbsky, "Protecting location privacy with dynamic MAC address exchanging in wireless networks," in *Proc. Of IEEE Globecom*, Washington, DC, Nov. 2007.

6. M. Garlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," in *Proc. of IEEE VTC-Spring*, Dublin, Ireland.