Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy

Mingyan Li*, Krishna Sampigethaya*, Leping Huang†, Radha Poovendran*
*Network Security Lab, EE Department, University of Washington, Seattle, WA 98195, USA
†Nokia Research Center & University of Tokyo, Tokyo, Japan
{myli,rkrishna,rp3}@u.washington.edu, Leping.Huang@nokia.com

ABSTRACT

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. On the other hand, since each user may need privacy at different locations and times, a *user-centric* approach is needed to enable the nodes to independently determine where/when to update their identifiers. However, mitigation of tracking with a user-centric approach is difficult due to the lack of synchronization between updating nodes. This paper addresses the challenges to providing location privacy by identifier updates due to the predictability of node locations and the asynchronous updates, and proposes a user-centric scheme called *Swing* that increases location privacy by enabling the nodes to loosely synchronize updates when changing their velocity. Further, since each identifier update inherently trades off network service for privacy, the paper also introduces an approach called *Swap*, which is an extension of Swing, that enables the nodes to exchange their identifiers to potentially maximize the location privacy provided by each update, hence reducing the number of updates needed to meet the desired privacy levels. The performance of the proposed schemes is evaluated under random and restricted pedestrian mobility.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; H.1.2 [**Models and Principles**]: User/Machine Systems—*Human factors*

General Terms

Algorithms, Design, Performance, Security

Keywords

Location Privacy, Tracking, User-centric, Wireless Network

WPES'06, October 30, 2006, Alexandria, VA, USA.

1. INTRODUCTION

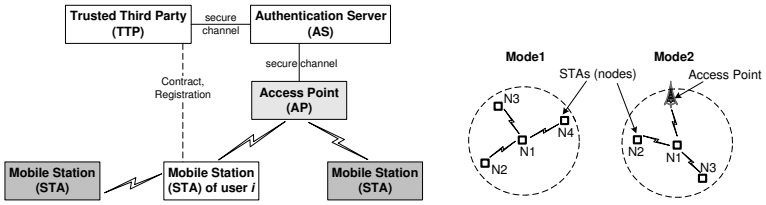
The significant benefits of ubiquitous network access have fueled the deployment of Radio Frequency (RF) based network connectivity, such as Wireless Local Area Network (WLAN), in user devices as well as in vehicles (nodes) [1, 13, 26]. However, the broadcast nature of the wireless medium allows an adversary to eavesdrop on the communications containing node identifiers, and to estimate the locations of the communicating nodes with an accuracy that is sufficient for tracking the nodes [2, 20, 29]. When correlated with public information such as geographic maps, location tracking of nodes leads to potential threats to the *location privacy* of their users by disclosing personal user preferences [11, 13].

However, since privacy is a context-specific property and is socially and/or culturally defined [18, 19], the location privacy needs of individual users may vary, and further each user may require location privacy protection at different times and locations. Hence, it is desirable that the protection of location privacy is *user-centric*, i.e. the independently mobile user nodes in the network are able to independently determine based on the accessible network information when/where to protect their user privacy. Additionally, a user-centric approach, essentially a distributed approach, has the advantage of not requiring a user node to rely on the external network infrastructure (e.g. base stations) that can potentially disclose user information to adversaries, for location privacy protection [14].

In this paper, we focus on the protection of location privacy by the mitigation of the tracking of nodes.[1] Existing tracking mitigation solutions in [4, 13, 16] enable nodes to update their identifiers to remove any correlation between locations based on identifiers (see Section 6). However, not all of these solutions are user-centric, since the approach in [13] enables the nodes to update their identifiers only at specific time instances (e.g. before associating with network base stations), while the approach in [4] enables the nodes to update only at pre-determined locations (MIX-Zones). Although the *random silent period* technique proposed in [16], in which the nodes do not transmit for a random period during update of identifiers, allows the nodes to independently update at random times/locations, it results in *asynchronous updates* that limit the location privacy provided by each update [16]. It is suggested in [16] that a base station be used as a coordinator to synchronize the updates of nodes. But, this is not a user-centric approach, since the base station would be determining when the user nodes can update.

Further, the location privacy provided by the solutions in [4, 13, 16] is limited by tracking methods that leverage the predictability of the movement of pedestrians and vehicles to correlate their locations before and after each identifier update [4, 16, 21, 23]. While an increase in the MIX-Zone size or the silent period (that in turn

[1]This paper assumes that mechanisms such as traffic monitoring cameras and physical pursuit are not used for location tracking.



(a) System Model **(b)** Mobile ad hoc network scenarios

Figure 1: (a) System model considered. *Dark grey* boxes are untrusted, *light grey* are semi-trusted and *white* boxes are trusted components for node of a user i. (b) Two modes of communication between nodes w/o AP.

increases the update period during which a node does not transmit) and/or an increase in the number of updates can potentially mitigate such tracking based on the predictability of node movement [4,16], the update period and the number of identifier updates are shown to be limited by the quality-of-service (QoS) [13,17] and network application requirements [23]. As one solution to balance this tradeoff, we propose *maximizing* the location privacy provided by each update.

Therefore, in this paper, we study the problem of designing a user-centric approach that can not only overcome the limitations to location privacy enhancement posed by the asynchronous identifier updates and tracking based on movement predictability, but can also increase the location privacy provided by each update towards a maximum value for the given node density and node mobility. The proposed user-centric approach builds on the random silent period technique of [16]. In particular, the paper makes the following contributions. (i) We address the asynchronous identifier updates and the predictability of node movement, and propose a user-centric approach called *Swing* that enables nodes to independently initiate and loosely synchronize updates at opportune locations/times to mitigate tracking. However, at such opportune locations/times, the location privacy provided by Swing does not account for the neighbors of the target that do not update their identifiers. (ii) We propose an extension of Swing, called *Swap*, where nodes cooperate to enable exchange of their identifiers. Swap can potentially increase the location privacy at each update towards the maximum by taking into account all the neighbors of the target. However, unlike Swing which can be applied to mobile networks, Swap is only conditionally applicable to mobile networks due to requirements such as a network base station to forward protocol messages and network identity management that allows for the exchange of identifiers between nodes, as seen later in Section 5.2.

The rest of the paper is as follows. Section 2 describes the system and adversary models and the problem addressed. Section 3 presents the proposed schemes and discusses the potential security attacks by an adversary. Section 4 evaluates the performance of the proposed schemes. Section 5 discusses applicability of the proposed schemes, while Section 6 compares them with related work. Section 7 presents our conclusions.

2. SYSTEM MODEL AND PROBLEM DESCRIPTION

Fig. 1(a) presents the system model considered including the following entities: mobile Stations (STA), Access Points (AP), the Authentication Server (AS), and the Trusted Third Party (TTP). Each STA belongs to a user entity that enters a contractual agreement with the TTP to obtain network service. Additionally, during a registration process with the TTP, each STA obtains a set of public/private key pairs, and a set of identifiers with each identifier having a maximum lifetime[2] after which the STA has to update its identifier for location privacy protection from eavesdroppers. It is assumed that the identifiers are used by the STAs as source addresses in the broadcasts to satisfy the requirements of the communication protocols. Further, each STA has GPS capability and can self-determine its locations when needed on pre-loaded digital geographic maps, and is also capable of predicting any change in its velocity (see Section 5), and channel monitoring to sense its *neighbors*, i.e. the STAs that are one-hop away in the network graph.

The AS controlled by the TTP, is connected to the APs for authenticating the STAs for network access and billing of the users, as well as for the identity management of the STAs [13]; the AS is a trusted entity accessible to all the STAs in the network. In order to update its identifier, a STA is able to de- and re-associate with an AP before and after update, respectively, and securely authenticate with the AS during re-association [13]. As illustrated in Fig. 1(b) we consider two modes: (*Mode1*) STAs directly communicate with each other without any AP; (*Mode2*) STAs can directly communicate with each other, but require an AP to facilitate these communications (see Section 5.2) and to communicate with the AS for authentication and identity management.

It is assumed that a user can trust its own STA, while other STAs in the network are untrusted, and that the APs are *semi-trusted*, i.e. operate as expected but can disclose information to an adversary.

2.1 Adversary Model Considered

The objective of the adversary is to track the STAs (nodes) in the network and breach the location privacy of their users. Such an adversary can be abstracted as (i) *Global Passive Adversary (GPA)* [16, 25] that can eavesdrop all communications of any node within a region of interest; and (ii) *Local Active Adversary (LAA)* [25] that can inject messages into a target's neighborhood. The LAA controls one or more neighboring nodes of the target that collude with the GPA to reveal information that can breach the target's location privacy; but these nodes do not reveal their secret cryptographic quantities to the adversary. However, we note that any location tracking by the LAA is equivalent to a physical pursuit of the mobile target, and hence is not addressed in this paper. But, we do address other attacks by the LAA such as node impersonation that can lead to privacy breaches. It is assumed that the adversary knowledge includes the node mobility model (e.g. random or restricted), and the tracking mitigation technique used by nodes.

2.2 Problem Description: Maximizing Location Privacy

In this paper, we study the problem of maximizing the location privacy of a user at each update in the presence of the GPA and the LAA, by utilizing a user-centric tracking mitigation approach for the system model considered.

The level of location privacy provided to a target by each identifier update can be measured using an *anonymity set* [8] denoted as S_A that includes the nodes with identifiers indistinguishable from that of the target T. We note here that the related *k-anonymity*

[2]Determining ID maximum lifetime is not the focus of the paper.

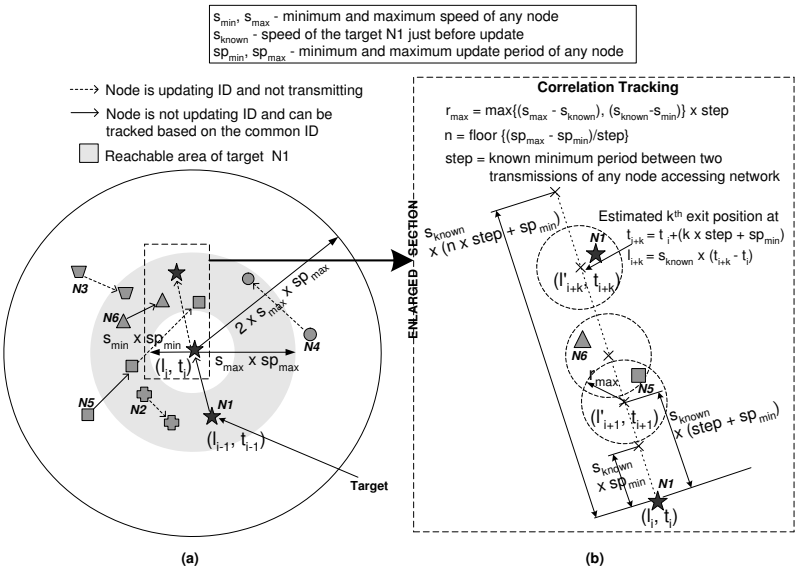


Figure 2: (a) Identifier update by target N1 to mitigate location tracking. Potential candidates for target anonymity set are in the circular region with radius $2s_{max}sp_{max}$. (b) Correlation tracking of target. Among N1-N5, only N1 and N5 have non-zero probabilities to be the target since each node appears after update near an estimated target exit position. N6 is not considered as a candidate as it does not update ID.

model [22] for privacy protection as used in [12] essentially refers to an anonymity set S_A with a minimum size k, where the target is guaranteed to be not distinguishable from at least $k-1$ nodes with respect to information related to the target (such as location information [12]). However, not all the nodes in the anonymity set may be equally likely to be the target since an adversary may be able to obtain additional knowledge on the nodes, such as the predictability of node movement as will be described below. In such scenarios, the *entropy* of the anonymity set distribution is considered to be a suitable measure of location privacy provided per update [4, 16, 24]. Let the probability that a node i of S_A is the target T be $p_i = Pr(T=i), \forall i \in S_A$, with $\sum_{i=1}^{|S_A|} p_i = 1$, then the entropy of the distribution of the anonymity set S_A of target T is given by $H(p) = -\sum_{i=1}^{|S_A|} p_i \log_2 p_i$. Using entropy as a measure of location privacy [4, 16, 24], we consider the problem of maximizing the location privacy of the target T as:

$$\max_p H(p) \qquad \text{s.t.} \qquad \sum_{i=1}^{|S_A|} p_i = 1, \;\; |S_A| \leq |S_A^*|,$$

where $|S_A^*|$ is the maximum anonymity set size that is dependent on the node density in the network, the node mobility model including the velocity range of nodes, the node tracking method employed by the adversary, and the tracking mitigation technique employed by the nodes. We make the following observations related to the maximization of the location privacy of the target T:

C1. For a given $|S_A|$, a uniform distribution for the anonymity set S_A is needed, i.e. $p_i = 1/|S_A|, \forall i \in S_A$ to maximize entropy, i.e. $\max_p H(p) = \log_2 |S_A| \leq \log_2 |S_A^*|$ [10].

C2. When $|S_A| = |S_A^*|$, $H(p)$ attains the possible maximum value of $\log_2 |S_A^*|$.

Consequently, the maximum location privacy for the target T in S_A is achieved when $|S_A| = |S_A^*|$ and all nodes in S_A are equally likely to be the target T.

Before presenting the challenges to satisfying the above two conditions, we first describe how the target anonymity set S_A is computed. Fig. 2 shows a target denoted N1, that is being tracked and is updating its identifier at location l_i and time t_i. We define the *reachable area* of the target to be the bounded region where it is expected to reappear after the identifier update. For example, as seen in Fig. 2(a), if the target enters a random silent period during the update, the reachable area is then determined by the allowable movement directions, the known achievable speed range $[s_{min}, s_{max}]$, and the update period which is between a minimum and maximum silent period value, sp_{min}, sp_{max}, respectively; the reachable area shown in Fig. 2(a) is for random node mobility, i.e. node direction is in $[0, 2\pi)$. The target anonymity set includes nodes that update their identifiers along with the target and appear in the reachable area of the target. As shown in Fig. 2 since out of nodes N2-N6, only N2-N5 update identifiers with the target N1 and appear in the reachable area after exiting a random silent period, the target anonymity set S_A={N1, N2, N3, N4, N5}.

In order to satisfy the condition C1, all the nodes in the target anonymity set must be equally probable to be the target. However, tracking based on the predictability of node movement can assign a non-uniform distribution to the target anonymity set and lower entropy [4, 16]. Fig. 2(b) illustrates one such tracking method, called *correlation tracking* [16], which assumes that the target does not change direction during update, and estimates "exit" positions on a trajectory where the target may appear after the update period. Only those nodes in the target anonymity set that appear close to the trajectory[3] are considered as candidates for the target. Note here that if the update period is fixed, i.e. $sp_{min} = sp_{max}$, then there is only one estimated exit position for the target. For example, in Fig. 2(b) the target N1 can be estimated to exit close to l'_{i+k} if the known update period is $(t_{i+k} - t_i)$, and the distribution of S_A is then {1,0,0,0,0} with entropy equal to zero. But, if the update period is random, i.e. when the target enters a random silent period, there are multiple estimated exit positions and correlation tracking will assign $p_i = \frac{l_i}{m}, i \in S_A$, if i is closest to l_i of m estimated target exit positions where nodes are observed, to relatively increase the entropy. For example, as seen in Fig. 2(b), since only N1 and N5 each appear with new ID close to an estimated exit position, we

[3]For each estimated target exit position, only those nodes that are within r_{max} (see Fig. 2(b)) are considered as "close", and among them only the node that appears closest to the position is selected.

have $m = 2$ and $p_{N1} = 1/2, p_{N5} = 1/2$; hence the distribution of the anonymity set S_A is $\{0.5,0,0,0,0.5\}$ and the entropy is one.

Nevertheless, as seen from the above illustration, correlation tracking limits the entropy from reaching the maximum value by assigning a non-uniform distribution to S_A. Moreover, a stronger adversary can utilize additional knowledge, such as by performing correlation tracking on multiple nodes (e.g. N1 and N5 in Fig. 2(a)), to further reduce the probability that one or more nodes (such as N5) in S_A is a target candidate, and thereby decrease the entropy towards zero. We note here that in the rest of the paper it is assumed that the GPA defined in Section 2.1 is capable of performing correlation tracking of the target as well as its updating neighbors. Therefore, under such an adversary model, in order to provide a uniformly distributed anonymity set, the predictability of the locations of nodes after identifier updates must be reduced.

Next, in order to satisfy the condition C2, the number of nodes updating and appearing in the reachable area of the target must be maximized. For example, from Fig. 2(a) it is seen that if the target N1 updates using a random silent period, then S_A can include at most the nodes within distance $2s_{max}sp_{max}$ from the location l_i where N1 enters a random silent period (see Section 4.1); nodes in this bounded region can possibly update and appear in the reachable area of the target. However, in a user-centric approach, since the target independently determines to update, other nodes in the reachable area (such as N6 in Fig. 2) may not update identifier with target, hence decreasing target's anonymity set size due to the resulting asynchronous updates. Therefore, to increase the anonymity set size the identifier updates need to be synchronized.

3. PROPOSED SCHEMES

This section presents user-centric approaches that address the tracking methods based on predictable node movement and the asynchronous updates, and increase the location privacy level towards the maximum value for a given node density and node mobility model.

3.1 Swing: Increasing Location Privacy

In order to prevent the GPA from utilizing the predictability of node movement to correlate node locations before and after update, we propose that the update of identifiers be performed by the nodes only when *changing velocity*, i.e. direction and speed. Assuming equal probability of a node choosing speed in $[s_{min}, s_{max}]$ and direction in $[0, 2\pi)$, the nodes appearing in the target reachable area during $[sp_{min}, sp_{max}]$ are equally likely to be the target, hence maximizing entropy of the anonymity set distribution and satisfying the condition C1. Therefore, the GPA can no longer use tracking methods based on predictable node movement, such as correlation tracking.

However, nodes may not be present in the target's neighborhood or the neighboring nodes may not be aware of the target update. To address the resulting asynchronous updates, we propose to increase the anonymity set size by enabling the target to perform the following before update: (i) monitor communication channels to ensure a neighborhood size of at least one; and (ii) broadcast to the nodes within distance $2s_{max}sp_{max}$ that it is entering update, to loosely synchronize as well as increase the probable updates. These observations lead to the Swing scheme described below.

The pseudocode for Swing protocol is in Appendix B. In the protocol, if a node i's current location privacy level is less than desired (set by the user of i) or the lifetime of the current identifier expires, then i enters an *update process* when it is changing velocity and neighbors are present. The update process is initiated by i broadcasting an *update message*, after which i updates identifier and remains silent for a random period sp.

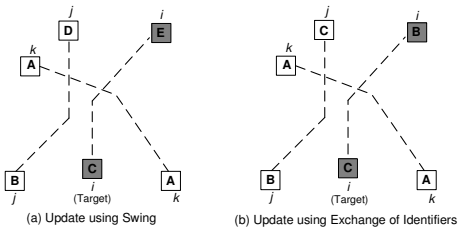


Figure 3: Illustration of an advantage of exchanging identifiers over updating to new identifiers. Boxes represent nodes with the letters inside being their associated identifiers. Dashed line indicates node is silent.

However, not all the nodes receiving the update message broadcast from i may update their identifiers since they may have already achieved the desired privacy levels, thereby restricting the anonymity set size of node i from reaching the maximum value for a given node density and node mobility, as described below.

3.2 Swap: Towards Maximizing Location Privacy

As seen in Fig. 3(a), if the target i has two neighbors j, k during identifier update in Swing with all three nodes changing their direction, and k does not update with i, then the anonymity set size is only two and the location privacy provided is at most $\log_2(2)$; since the GPA knows the mitigation technique used by i is Swing, it needs to only determine an association between target identifier C and an identifier in $\{$D, E$\}$. But, in order to provide the maximum location privacy level, i.e. $\log_2(3)$, all the three nodes need to be included in the anonymity set. Hence, as a solution towards maximizing the anonymity set size, i.e. satisfying condition C2, we propose that instead of updating to new identifiers (as in Swing), the node j and the target i *exchange* their identifiers during update with probability 0.5 and enter a random silent period. As illustrated in Fig. 3(b), even if k does not update identifier along with i, it can be included in the anonymity set if it only changes direction and enters a random silent period k; since the GPA does not know which node among j and k that i exchanged identifiers with, and if i exchanged identifier at all, the GPA must determine an association between C and an identifier in $\{$A, B, C$\}$. This illustrates the idea behind the proposed *Swap* scheme.

Fig. 4 shows the Swap protocol on a time line; the protocol pseudocode is in Appendix C. When the node i needs to enhance privacy and is changing velocity while neighbors are present, i initiates an *exchange process*:

(1) i broadcasts an *exchange request* containing one of i's public keys.

(2) All nodes receiving the exchange request, respond by encrypting an *exchange response* with i's public key; the exchange response from a neighbor o includes its approval or disapproval to exchange identifier and o's public key, signed and timestamped for authenticity.

(3) i randomly selects one of the received exchange responses, say from j, and broadcasts an *exchange acknowledgment* including (i) a *response* to j encrypted with j's public key, to indicate if i will exchange identifier or not, and (ii) a verifiable exchange outcome containing a signed response of j and a timestamped response of i, encrypted with a key shared between i and AS.

(4) The AP forwards an exchange acknowledgment from i to the trusted AS.

(5) The AS sends an acknowledgment to i and j encrypted with the corresponding keys shared with the AS.

(6) Finally, i, j enter a random silent period and re-associate with AP by authenticating with AS after silent period.

In Swap, neighbors of the target contribute to its anonymity set despite not updating identifiers, as long as they change their velocity and broadcast only during a specific interval in the exchange process as shown in Fig. 4. As an incentive, these cooperating nodes are provided with location privacy enhancement without the need for any update of identifiers, hence conserving the number of identifiers used by them for privacy enhancement. It should be noted here that in Swap, while the node initiating exchange becomes indistinguishable from all the cooperating nodes, each cooperating node is only indistinguishable from the node initiating exchange, and not from other cooperating nodes. In order to further improve the privacy of the cooperating nodes, Swap can be extended to allow "shuffling" of multiple identifiers, i.e. each cooperating node can also exchange identifier with another cooperating node. However, such an extension will incur overhead in terms of multiple executions of the Swap protocol.

3.3 Comparison between Swing and Swap

Unlike Swing, Swap accounts for all the neighbors of the target within its transmission range that change direction, enter a random silent period, and appear in the target reachable area, hence potentially maximizing the target anonymity set size. However, the number of neighbors of the target that change direction is determined by the node mobility model. We evaluate the location privacy provided by Swing and Swap under the Random Way Point (RWP) model [28] later in Section 4.

Apart from providing a potentially larger, uniformly distributed anonymity set, and consequently a higher level of location privacy at each update, Swap inherently conserves node identifiers compared to Swing. However, these advantages are achieved at the cost of the protocol overhead. Further, since for identity management an AP is required to forward the Swap protocol messages to the AS, Swap applies only to Mode2 of the system model described in Section 2. On the other hand, Swing which is independent of the AP, applies to both Mode1 and Mode2.

3.4 Mitigating Security Attacks and Traffic Analysis by LAA and GPA

In Swap, one potential attack is for the LAA to impersonate nodes using their observed identifiers during the exchange process for network access. However, such an attack can be prevented by Steps 2-5 of the Swap protocol that ensure an identifier exchange is valid by requiring node i to send to the AS the signed approval/disapproval from a randomly chosen node j, and requiring the AS to verify and acknowledge the identifier exchange. Further, the LAA cannot initiate the exchange process and select the target to exchange identifiers, since it does not have the secret cryptographic quantities of the compromised nodes. The authenticity of the communication between i and the AS (as well as between the AS and j) is ensured by the use of encryption with a shared symmetric key and timestamps. We note here that since any exchange of identifiers is verified by the AS, the exchanging nodes can reauthenticate themselves to the AS when needed after the exchange.

Further, in order to track a target, the GPA can eavesdrop on the communications in Swing and Swap protocols. The Swing protocol only indicates to the GPA that a target will be updating, and the GPA cannot obtain any additional information by analyzing the protocol messages. In Swap protocol, while the GPA knows when a target i initiates exchange process (in Step 1), in order to mitigate tracking the GPA must not be able to *(a)* identify the node j selected by i, and *(b)* ascertain if i exchanged identifiers. To prevent the GPA from identifying j: *(1)* j is randomly chosen by i and public keys are used to encrypt the messages between i and j (in Steps 2-3); *(2)* all the neighbors are required to reply to i; and *(3)* the exchange acknowledgment from i (in Step 3) does not reveal the identifier of j. Further, to prevent the GPA from ascertaining the exchange of identifiers by i, the forwarding of the exchange acknowledgment and the reply from AS (in Steps 4-5) is performed irrespective of whether i ultimately chooses to exchange identifier with j or not. We also note that to prevent the GPA from identifying a broadcast of the target i after Swap based on the public key used by i in Step 1 of Swap, i must update the public/private key after Swap. Overall, upon initiation of Swing or Swap by a target, based on the knowledge that the target enters update, the GPA can at best construct an uniformly distributed anonymity set as described in Section 2.2. The location privacy level provided by the constructed anonymity set is analyzed in Sections 4.1, 4.3.

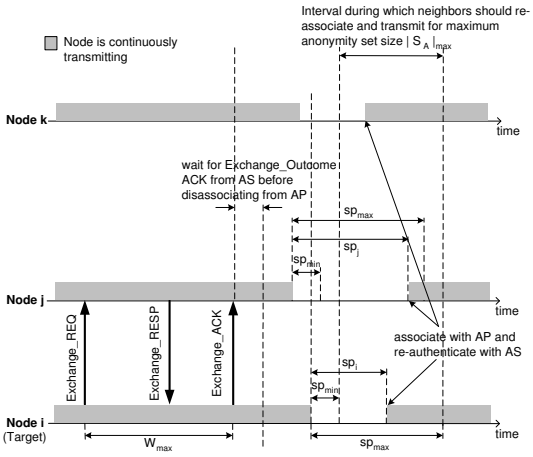


Figure 4: Illustration of Swap protocol on a time line, involving i, j, k (for clarity, AP and AS are omitted from the figure).

However, the LAA can potentially use the following attacks to lower the location privacy level of the constructed anonymity set: (Attack1) Impersonate multiple nodes to mislead a target into Swing or Swap; (Attack2) Reveal the Swap protocol outcome observed by the compromised nodes to the GPA. While mitigation of Attack1 is difficult (see Section 5.1), the Attack2 on Swap is mitigated by the random selection of j by i from the received exchange responses.

4. PERFORMANCE ANALYSIS

In this section, we analyze the location privacy provided by the proposed schemes under location tracking by the GPA, and also under different compromised node densities by the LAA.

4.1 Analytical Results for Swing and Swap

As a performance measure to evaluate the level of location privacy provided by the proposed schemes, we use *entropy* of the anonymity set distribution of a target, defined in Section 2.2. We first establish the upper bound on the entropy that can be achieved by the random silent period technique for a given node density. From Fig. 2 it is seen that the target anonymity set can at most include all the nodes that are within $2s_{max}sp_{max}$ from the location where the target enters a random silent period. Assuming that nodes are uniformly distributed with density ρ in the deployment region, the bounds for the average anonymity set size due to each update is as follows (derived in Appendix A):

$$1 \leq \mathbb{E}\{|S_A|\} \leq \frac{\rho\pi(2s_{max}sp_{max})^2}{1 - e^{-\rho\pi(2s_{max}sp_{max})^2}}, \quad (1)$$

Table 1: Random and Restricted Mobility Simulation Setup. RWP - Random Way Point; p_x - prob. of changing direction by x

Parameter	*Value*
Mobility model	RWP (pausetime=0); Manhattan ($p_0 = 1/3$, $p_{\pi/2} = 1/3$, $p_{-\pi/2} = 1/3$)
Region	100m $\times$ 100m (RWP), 9 $\times$ 9 uniform street grid, street length 300 m, separation 30 m (Manhattan)
Simulation step	0.1 secs
Traffic model	Continuous broadcasting, no packet collisions, Minimum period between two broadcasts is 0.1 secs
Node Speed	[1, 3] m/sec
Node Acceleration	0 m/sec^2 (RWP), 0.2 m/sec^2 (Manhattan)
Node Density	[0.01, 0.1] /m^2 (RWP); [0.05, 0.5] /m, traffic volume=600/hr/street (Manhattan)
Silent period	[0, 5] secs
Tracking	Construction of anonymity set, correlation tracking
Metrics	Entropy of anonymity set distribution

and the bounds for entropy of anonymity set distribution due to each update is:

$$0 \leq H(p) \leq \log_2 \frac{\rho\pi(2s_{max}sp_{max})^2}{1 - e^{-\rho\pi(2s_{max}sp_{max})^2}}. \quad (2)$$

These upper bounds are achieved only when all the nodes within $2s_{max}sp_{max}$ from the target will fully cooperate and move such that they appear in the target's reachable area. However, we note that such an approach, which assumes control over the movement of the otherwise independently mobile neighbors for location privacy of the target, is not user-centric. Moreover, under tracking based on movement predictability, only the nodes that change velocity will contribute to target anonymity set. Hence, the anonymity set size and entropy in Eqs. (1), (2), are additionally limited by the node mobility model considered. We evaluate the entropy provided by each update using Swing and Swap under the Random Way Point model (RWP), a widely used mobility model in mobile ad hoc network simulation [28]. In a RWP, a node chooses a destination (or a way point) and moves toward the destination with a constant velocity, and then pauses before starting the next trip to a newly chosen way point. To account for the inherent problem of average speed decay in RWP [28], the pause time is set to zero.

We denote the reachable region of a target by R_R, and its broadcast region by R_B with $R_B \geq R_R$. The nodes that contribute to the anonymity set of the target are those (i) updating their identifiers and their silent period overlapping with the target's (*temporally close*), and (ii) reappearing in R_R (*spatially close*). To count the number of nodes that are spatially close to the target, we assume that the number of nodes going from $R_B - R_R$ to R_R during the silent period of the target is equal to that from R_R to $R_B - R_R$.[4] The average number of nodes that appear in R_R after silent period, given at least one node (the target) in R_R, is $\frac{\rho A(R_R)}{1-e^{-\rho A(R_R)}}$, where $A(R_R)$ denotes the area of region R_R and

$$A(R_R) = \pi * ((sp_{max} * s_{max})^2 - (sp_{min} * s_{min})^2) \quad (3)$$

Let p_u denote the probability that a node enters a random silent period and updates its identifier at each direction change after reaching a waypoint. Given that the target updates at time t_0, nodes emerging with new identifiers during $[t_0 + sp_{min}, t_0 + sp_{max}]$ will be temporally indistinguishable from the target to the adversary. The probability of a node changing direction and reappearing during $[t_0 + sp_{min}, t_0 + sp_{max}]$ in the RWP model is $\frac{(sp_{max} - sp_{min})}{avgT_m}$ (derived in Appendix D), where $avgT_m$ is the average time of a node spending in each segment before choosing a new destination.

[4]This reasonable assumption for random mobility models is corroborated by close match between analytical and simulation results.

Given that the average length of a segment is $0.5214 * L$ for a square area with edge length L [6], $avgT_m$ is computed as:

$$avgT_m = \frac{\text{average length of a segment}}{\text{average speed}} = \frac{0.5214 * L}{(s_{max} + s_{min})/2}$$

for a square area with edge length L.

Therefore, for Scheme I (Swing) where a node broadcasts for its update before entering silent period, the average size of the anonymity set of the target during one update is:

$$\mathbb{E}\{|S_A|\} = \text{(avg. num. of nodes in } R_R \text{, excluding target)} * p_u * \text{(prob. of reappearing in } [t_0 + sp_{min}, t_0 + sp_{max}]) + 1$$
$$= \left(\frac{\rho * A(R_R)}{1 - e^{-\rho A(R_R)}} - 1\right) * p_u * \left(\frac{(sp_{max} - sp_{min})}{\frac{0.5214*L}{(s_{max}+s_{min})/2}}\right) + 1, \quad (4)$$

where $A(R_R)$ is given in Eq. (3). As GPA has no additional knowledge on node mobility to eliminate any candidate in the anonymity set but assigns equal probability to all the candidates, the probability that the target can be uniquely identified at each update is $p_{track} = 1/\mathbb{E}\{|S_A|\}$. The entropy of the anonymity set distribution of the target at each update in Scheme I is $E_I = \log_2 \mathbb{E}\{|S_A|\}$. In Scheme II (Swap), all the nodes in R_R will contribute to target anonymity set, regardless of whether they update their identifier or not. Hence, the entropy at each update in Scheme II is $E_{II} = \log_2(\frac{\mathbb{E}\{|S_A|\}}{p_u}) \geq E_I$.

Now, we consider the case that the probability of a node being an adversary (i.e. the LAA) $p_a > 0$. Under this scenario, the entropy achieved by Scheme I at each update is $E_{I,a} = \log_2((1 - p_a) * \mathbb{E}\{|S_A|\})$. For Scheme II, if the target randomly chooses a exchange response among all the responses received, the entropy achieved at each update is $E_{II,a} = \log_2((1-p_a) * \frac{\mathbb{E}\{|S_A|\}}{p_u})$. Note that $E_{II} \geq E_I \geq E_{II,a} \geq E_{I,a}$, and first, third equal signs hold when $p_u = 1$, and second equal sign holds when $p_a = 0$.

4.2 Simulation Setup

Table 1 summarizes the simulation settings for random and restricted node mobility. Random WayPoint (RWP) model [28] is utilized for random mobility, while the Manhattan model [3] is used for restricted mobility. In order to address the average speed decay in the RWP model, the pause time of nodes is set to 0, the minimum node speed is set to 1 m/sec, and the results are accounted only after a warm-up period of 1000 seconds [28]. Unlike the RWP model where nodes can randomly choose direction and speed from a range of values, the Manhattan model limits the velocity of nodes along fixed paths with associated speeds, and periodically uses the current/past spatial parameters of nodes to update their spatial parameters. Overall, the mobility of nodes is restricted to three directions,

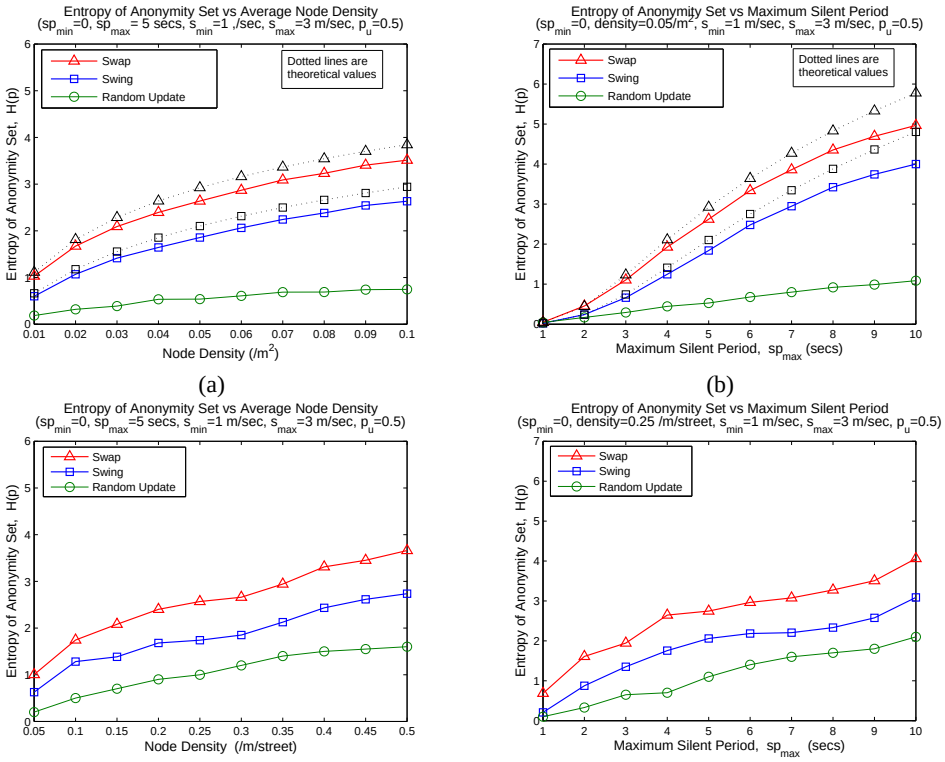


Figure 5: Performance of Swing and Swap compared to Random Update. (a),(b) Random mobility. (c),(d) Restricted mobility.

i.e. $\{-\frac{\pi}{2}, 0, \frac{\pi}{2}\}$, assuming that the nodes do not change their direction by π. Each data point in the simulation plots is averaged over more than 100 iterations. The border effect of the bounded simulation region in the Manhattan model is accounted for by making nodes randomly reappear in the region [3].

4.3 Simulation Results for Swing and Swap

Fig. 5 compares the entropy provided at each update by a *Random Update*, i.e. update of the identifier at a random location and time using random silent period, with that of the proposed Swing and Swap, under random and restricted mobility, respectively. As seen, both Swing and Swap perform relatively well and Swap providing the largest level of location privacy, under both mobility models. In fact, the location privacy level of Random Update is optimistically determined assuming that the GPA only performs correlation tracking of the target, while in the case of Swing and Swap the GPA tracks multiple nodes. Fig. 5(a), 5(c) also show that under restricted mobility, since the target can move in a lesser number of directions than under random mobility (it is assumed in the Manhattan model that a node does not change its direction by π), the GPA can eliminate nodes from the anonymity set provided under random mobility. Consequently, the entropy provided by Swing and Swap under restricted mobility is relatively lower than random mobility for a given density.

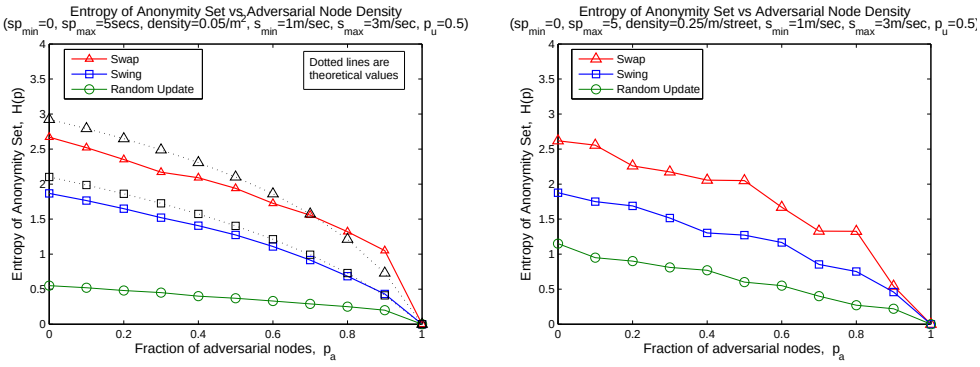
Fig. 6 shows the effect of the LAA on Swing, Swap, and Random Update, and expectedly performance degrades with increasing adversarial node density, since an increasing number of updating target neighbors are compromised (hence not contributing to the target anonymity), and also the mitigation of Attack2 (in Section 3.4) on Swap by random selection of an updating neighbor for identifier exchange becomes less effective. Further, Fig. 5(a), 5(b), 6(a) show that the theoretical (dotted lines) and simulated results closely match.

5. DISCUSSION AND OPEN PROBLEMS

5.1 Entropy Computation and Velocity Change Estimation

One requirement of a user-centric approach is to enable the nodes to estimate the level of privacy achieved by each identifier update. In both Swing and Swap, under random mobility, the channel monitoring can be leveraged to estimate the node density before update, and hence enable the computation of an upper bound on the entropy using Eq. (2). Further, the number of update messages/exchange responses received from neighbors can be used to compute the anonymity set size and entropy due to update. However, as the LAA can impersonate multiple nodes in Attack1 in Section 3.4, the target can be misled to compute an optimistic upper bound for entropy before update in Swing and Swap. A possible solution to mitigate such an attack is to impose the need for authenticated messages from nodes during the estimation of node density by channel monitoring. Similarly, the impact of multiple node impersonation on the entropy computation after update can be mitigated by enabling the target to authenticate the update messages from the neighbors. But, the entropy computation can still be affected if the adversary is able to compromise multiple nodes in the network without being detected and obtain their cryptographic keys. Hence, ensuring the robustness of entropy computation before and after update under such a strong adversary model remains a challenging open problem.

Further, as seen in Section 4.3, under restricted mobility, the entropy of the anonymity set distribution determined by the above method can be reduced, since the GPA can eliminate nodes at unlikely target locations from the anonymity set. Hence, we propose including node velocity in the update messages/exchange responses, to enable the computation of entropy based on the relative velocity of nodes. For example, in the Manhattan model a target



(a) (b)

Figure 6: Performance of Swing and Swap in the presence of LAA. (a) Random mobility (b) Restricted Mobility.

can determine that if a neighbor's velocity indicates it is moving in a direction opposite to that of the target, it has zero probability of being the target, since the target is restricted from changing direction by π. The construction of such a computational method is an open problem. We note that one approach is to estimate the entropy using an empirically determined *movement matrix* [4] for the target's reachable area.

Additionally, in both Swing and Swap, it is assumed that each user node is capable of estimating the time and location where a change in its velocity can occur. One potential enabling mechanism can be based on the GPS capability of nodes combined with pre-loaded digital geographic maps, and assume that any user destination is known to only that user's node (e.g. by user input), hence allowing each node to predict changes in its direction and speed.

5.2 Applicability of Swing and Swap

Swing can be used in the Independent Basic Service Set (IBSS) mode as well as the Infrastructure Basic Service Set (BSS) mode in WLAN. However, since Swap requires an AP to provide access to the AS for identity management, in its current form it is only applicable to the BSS mode where an AP is present. But, since in the BSS mode a node cannot broadcast on its own, in order to enable both Swing and Swap, one approach is for nodes to broadcast via the AP. It then becomes necessary to quantify the latency incurred in the communication via the AP. A second approach is to integrate the two WLAN modes with the AP coordinating the switch for a node and its neighbors from the BSS to the IBSS mode [9] only for Swing/Swap. A third potential solution is to utilize direct links between STAs, as in 802.11e where a link managed by the AP is provided between two STAs in BSS [27]. We note that since we assume the AP is semi-trusted and not malicious, it would operate as expected in all the above methods.

Another potential application of Swing is in Vehicular Ad hoc Networks (VANET), where correlation tracking of vehicles has been shown to be possible due to the short intervals between node broadcasts [23]. However, the applicability of Swap in VANET, although more beneficial due to potential maximum location privacy provided per update as well as the scalability in terms of number of identifiers needed for privacy protection, is challenging due to the liability requirement for vehicles. Each vehicle identifier has an associated public/private key pair for the authenticity of broadcasts to ensure liability at any given time (e.g. in the event of an accident) [21, 23]. Hence, the exchange of identifiers without violating liability in VANET is an open problem.

5.3 Open Challenges of User-Centric Location Privacy Enhancement

All the user nodes involved in Swing or Swap are provided with the same level of privacy from an identifier update. However, each user may require a different level of privacy, and hence one user node may need to update identifier more frequently than others nearby to meet its desired privacy level. If a neighboring node has already reached its desired privacy level, it does not have any incentive to cooperate with another user node by switching off radio and/or updating identifier. As a result, users with higher privacy requirement may not get enough privacy in our system. Hence, satisfying the different privacy requirements of users in a user-centric approach is an open problem.

Further, there can be scenarios where no user node cooperates with a target to enter Swing or Swap, thereby not allowing the target to protect its location privacy. In such non-cooperative environments, one approach is for an AP to enforce the neighbors of the target to update their identifiers. However, such an approach is not user-centric. Therefore, the design of a user-centric approach that can protect the location privacy of the target in the presence of non-cooperative (but not compromised) neighbors is an open problem.

6. RELATED WORK

To protect users from location privacy threats, there are several research studies in mobile networks. In [4, 5], Beresford and Stajano propose an innovative scheme based on the idea of Chaum's MIX [7], that enables the nodes to update at pre-determined locations called *MIX-Zones*. A MIX-Zone for a group of nodes is a geographical region where the nodes do not access the network and can update their identifiers. Because the locations of nodes in a MIX-Zone cannot be estimated, the updating nodes can potentially *mix* their identifiers and constitute an anonymity set. However, the spatial and temporal relation between the locations of a mobile node can enable its entry and exit locations and times from a MIX-Zone to be correlated [4], hence lowering entropy.

For protecting the user location privacy in WLAN, in [13] Gruteser and Grunwald propose updating identifiers at specific time instances i.e. before associating with an AP for network access as a tradeoff solution between network disruption and privacy. Further, in [12] they also present an approach based on the k-anonymity privacy protection model, where a centralized trusted server adjusts the resolution of the location of nodes along spatial and temporal dimensions for mitigating their tracking [12]. Additionally, in [15] Hoh and Gruteser address the problem of maximizing privacy with QoS requirements as a constraint. However, in [12, 15] it is assumed that the tracking is due to the location information provided by the nodes accessing LBS applications, hence not applicable to mitigate tracking due to location estimation based on radio signal properties.

Unlike the above approaches, in [16], Huang et al. propose the random silent period technique to allow the nodes to update at ran-

dom locations and times. Noting that such updates are not able to mitigate correlation tracking, they suggest utilizing the AP as a coordinator to synchronize the updates as well as enforce the neighboring nodes to update with the target, thereby increasing the resulting entropy of the anonymity set distribution. However, by enforcing nodes to update the approach is not user-centric. Moreover, the user location privacy can be compromised when the semi-trusted AP reveals information to the adversary, hence making an AP-coordinated approach unsuitable. In contrast, Swing does not require an AP for location privacy protection, and the AP involved in Swap has no knowledge of the node exchanging identifier with the target and whether the identifier exchange occured.

7. CONCLUSIONS

In this paper, we studied the problem of maximizing location privacy at each identifier update by wireless users, in the presence of asynchronous identifier updates and predictability of movements of user nodes. As a solution, two user-centric location tracking mitigation schemes called *Swing* and *Swap* were proposed that enable the nodes to update when changing their direction and speed, before entering a random silent period. Swap apart from conserving identifiers, enables the inclusion of the non-updating neighboring nodes in the anonymity set and hence, potentially increases the location privacy at each update, towards a maximum value for a given node density and node mobility. An analytical as well as simulation based evaluation of Swing and Swap showed that they expectedly perform well compared to a scheme that updates identifier at random times/places. A future research direction is to address the application of Swap to vehicular adhoc networks. While the liability requirement in these networks does not allow for exchange of identifiers, the maximum update period and the number of identifier updates is limited by the safety application requirements, hence requiring each update to provide the maximum privacy possible.

8. ACKNOWLEDGEMENTS

The authors are grateful for the feedback of the anonymous reviewers. This work was supported in part by the following grants: NSF grant ANI-0093187-002, and by ARO PECASE grant W911NF-05-1-0491. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors, and should not be interpreted as the views of the National Science Foundation, or the U.S. Army Research Office, or the U.S. Government.

9. REFERENCES

[1] 5.9GHz DSRC. http://grouper.ieee.org/groups/scc32/dsrc/.

[2] P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *Proc. of INFOCOM*, pages 775–784, 2000.

[3] F. Bai, N. Sadagopan, and A. Helmy. IMPORTANT: A framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks. In *Proc. of IEEE INFOCOM*, pages 825–835, 2003.

[4] A. R. Beresford. *Location Privacy in Ubiquitous Computing*. PhD thesis, University of Cambridge, 2004.

[5] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[6] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. *IEEE Trans. on Mobile Computing*, 2(3):257–269, 2003.

[7] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[8] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1:65–75, 1988.

[9] J. Chen, S. Chan, and S. Liew. Mixed-mode WLAN: the integration of ad hoc mode with wireless LAN infrastructure. In *Proc. of IEEE Globecom*, pages 231–235, 2003.

[10] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.

[11] F. Dötzer. Privacy issues in vehicular ad hoc networks. In *Proc. of PET*, pages 197–209, 2005.

[12] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of ACM MobiSys*, pages 31–42, 2003.

[13] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. In *Proc. of ACM WMASH*, pages 46–55, 2003.

[14] Q. He, D. Wu, and P. Khosla. The quest for personal control over mobile location privacy. *IEEE Communications Magazine*, 42(5):130–136, 2004.

[15] B. Hoh and M. Gruteser. Location privacy through path confusion. In *Proc. of IEEE SecureComm*, 2005.

[16] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Towards modeling wireless location privacy. In *Proc. of Privacy Enhancing Technologies (PET)*, pages 59–77, 2005.

[17] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Silent cascade: Enhancing location privacy without communication qos degradation. In *Proc. of Security in Pervasive Computing (SPC)*, pages 165–180, 2006.

[18] R. Leenes and B.-J. Koops. 'Code' and privacy - or how technology is slowly eroding privacy. In *Essays on the normative role of information technology*. T.M.C. Asser Press, The Hague, Netherlands, 2005.

[19] H. Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 17:101–139, 2004.

[20] T. S. Rappaport, J. H. Reed, and B. D. Woerner. Position location using wireless communications on highways of the future. *IEEE Communications Magazine*, 10(1):33–41, 1996.

[21] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc neworks. *Proc. of ACM SASN*, pages 11–21, 2005.

[22] P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. In *Tech. Report SRI-CSL-98-04, CS Lab, SRI International*, 1998.

[23] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing location privacy for VANET. In *Proc. of Embedded Security in Cars (ESCAR)*, 2005.

[24] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In *Proc. of Privacy Enhancing Technologies (PET)*, pages 41–53, 2002.

[25] A. Serjantov, R. Dingledine, and P. Syverson. From a trickle to a flood: Active attacks on several mix types. In *Proc. of Information Hiding Workshop*, pages 36–52, 2002.

[26] IEEE 802.11 WG. http://grouper.ieee.org/groups/802/11/.

[27] X. Yang. IEEE 802.11e: Qos provisioning at the MAC layer. *IEEE Wireless Communications*, 11(3):72–79, 2004.

[28] J. Yoon, M. Liu, and B. Noble. Random waypoint considered

harmful. In *Proc. of IEEE INFOCOM*, pages 1312–1321, 2003.

[29] Y. Zhao. Mobile phone location determination and its impact on intelligent transportation systems. *IEEE Trans. on Intelligent Transportation Systems*, 1(1):55–64, 2000.

Appendix A

Given nodes are uniformly distributed, the number of nodes in area A, denoted by $\nu(A)$, distributes according to spatial Poisson process as: $Pr\{\nu(A) = i\} = \frac{(\rho A)^i}{i!}e^{-\rho A}$, with average as ρA. If S_A denotes target anonymity set, then its expected size is: $\mathbb{E}\{|S_A|\}$

$$= \mathbb{E}\{\nu(A)|\nu(A) \geq 1\} = \frac{\mathbb{E}\{\nu(A)\}}{1 - Pr\{\nu(A) = 0\}} = \frac{\rho A}{1 - e^{-\rho A}}.$$

As seen from Fig. 2, the target anonymity set at least includes the target itself, and can at most include nodes within the circular area, $A \leq \pi(2s_{max}sp_{max})^2$, where s_{max} is the maximum node speed and sp_{max} is the maximum silent period. Consequently:

$$1 \leq \mathbb{E}\{|S_A|\} \leq \frac{\rho\pi(2s_{max}sp_{max})^2}{1 - e^{-\rho\pi(2s_{max}sp_{max})^2}}.$$

Therefore, the maximum value for entropy is:

$$\begin{aligned} H(p) &\leq -\sum_{i=1}^{\mathbb{E}\{|S_A|\}} \frac{1}{\mathbb{E}\{|S_A|\}} \log_2 \frac{1}{\mathbb{E}\{|S_A|\}} \\ &\leq \log_2\left(\frac{\rho\pi(2s_{max}sp_{max})^2}{1 - e^{-\rho\pi(2s_{max}sp_{max})^2}}\right). \end{aligned}$$

Appendix B

The Swing protocol for enabling a target i is as follows.

Swing Protocol

---

if (($current\_loc\_priv < desired\_loc\_priv$) OR (*identifier lifetime expired*)
if ((*neighbor density > 0*) and (*changing* $velocity$)) OR
((*received* UPD_MSG_j) and (*changing* $velocity$ *within* sp_{max})
if (*not in silent period*)
i: randomly choose $sp_{min} \leq silent\_period \leq sp_{max}$
$i \rightarrow$: $UPD\_MSG_i = PID_{i,l-1}||$"updating"
i: remain silent for $silent\_period$
i: update $PID_{i,l-1}$ to $PID_{i,l}$
endif
endif
endif

Appendix C

Denote the set of nodes receiving broadcast of a target as G_i. The Swap protocol for enabling a target i with current identifier $PID_{i,l}$ and current public key $K_{i,m}$ to exchange identifiers with one its neighbors before entering random silent period, is as follows.

Swap Protocol

---

if (($current\_loc\_priv < desired\_loc\_priv$) OR (*identifier lifetime expired*)
if ((*neighbor density > 0*) and (*changing* $velocity$)) OR
((*received* $Exch\_REQ_o$) and (*changing* $velocity$ *with* sp_{max}))
if (*not in silent period*)
$i \rightarrow$: $Exch\_REQ_i = PID_{i,l}||$"exchanging?"$||K_{i,m}$
while (*time <= W*$_{max}$)
i: receive $Exch\_RES_o = PID_{i,l}||PID_{o,h}||$
$E_{K_{i,m}}(rep||sign_o(rep, tstamp_o)||K_{o,n})$, $o \in G_i$
/** rep=YES/NO **/
/** o is a neighbor of i **/
/** $K_{o,n}$, $PID_{o,h}$ is current public key and ID of o **/
endwhile
$i \rightarrow$: $Exch\_ACK = PID_{i,l}||exch\_ack||E_{K_j}(resp)||$
$E_{k_{i-AS}}(resp||sign_j(reply, tstamp_j)||K_j||tstamp_i)$, $j \in G_i$
/** j is randomly selected by i from responses from G_i **/
/** k_{i-AS} is symmetric key known to i and AS **/
/** resp=exchange/no exchange with j **/
/** exch_ack used to enable AP to forward to AS **/
$AP \rightarrow AS$: forward $Exch\_ACK_i$
$AS \rightarrow i$: $E_{k_{i-AS}}$(*exch_outcome_ack*$||tstamp_{AS}$)
$AS \rightarrow j$: $E_{k_{j-AS}}$(*exch_outcome_ack*$||tstamp_{AS}$)
/** ACK is needed from AS to prevent impersonation **/
/** exch_outcome_ack contains quantities required for authentication by AS when node re-associates with AP **/
i, j: randomly choose $sp_{min} \leq sp \leq sp_{max}$
i, j: remain silent for $silent\_period$
endif
endif
endif

Appendix D

For a node to appear with a new identifier during $[t_0 + sp_{min}, t_0 + sp_{max}]$, where t_0 is the time instance at which the target enters a silent period, a necessary condition is the node going into a silent period during $[t_0 - (sp_{max} - sp_{min}), t_0 + (sp_{max} - sp_{min})]$. Given that the node becomes silent at t_s with $t_s \in [t_0 - (sp_{max} - sp_{min}), t_0 + (sp_{max} - sp_{min})]$ and randomly chooses a silent period in $[sp_{min}, sp_{max}]$, the probability that the node exits during $[t_0 + sp_{min}, t_0 + sp_{max}]$ is:

$$\begin{cases} \frac{t_s - (t_0 + sp_{min} - sp_{max})}{sp_{max} - sp_{min}} & \text{for } t_0 - (sp_{max} - sp_{min}) \leq t_s < t_0 \\ \frac{(t_0 - sp_{min} + sp_{max}) - t_s}{sp_{max} - sp_{min}} & \text{for } t_0 \leq t_s \leq t_0 + (sp_{max} - sp_{min}) \end{cases}$$

By assuming that t_s is uniformly distributed in $[t_0 - (sp_{max} - sp_{min}), t_0 + (sp_{max} - sp_{min})]$, the average probability of a node entering silent period in $[t_0 - (sp_{max} - sp_{min}), t_0 + (sp_{max} - sp_{min})]$ and reappearing in $[t_0 + sp_{min}, t_0 + sp_{max}]$ is: p_s=

$$\begin{aligned} &= \int_{t_x}^{t_0} \frac{t_s - t_x}{sp_{max} - sp_{min}} * \frac{1}{2(sp_{max} - sp_{min})} dt_s \\ &\quad + \int_{t_0}^{t_x} \frac{t_x - t_s}{sp_{max} - sp_{min}} * \frac{1}{2(sp_{max} - sp_{min})} dt_s \\ &= 1/2, \end{aligned}$$

where $t_x = t_0 - sp_{max} + sp_{min}$. Using Swing and Swap, a node enters a random silent period only after changing velocity. Under the Random Way Point (RWP) mobility model, the probability that a node changes its velocity $[t_0 - (sp_{max} - sp_{min}), t_0 + (sp_{max} - sp_{min})]$ is $\frac{2*(sp_{max} - sp_{min})}{avgT_m}$, where $avgT_m$ is the average time of a node spending in each segment before choosing a new destination and is given in [6]. Therefore, the probability of a node reappearing during $[t_0 + sp_{min}, t_0 + sp_{max}]$, when using Swing and Swap under the RWP, is the probability of being silent during $[t_0 - (sp_{max} - sp_{min}), t_0 + (sp_{max} - sp_{min})]$ times p_s, i.e., $\frac{2*(sp_{max} - sp_{min})}{avgT_m} * \frac{1}{2} = \frac{(sp_{max} - sp_{min})}{avgT_m}$.