AMOEBA: Robust Location Privacy Scheme for VANET

Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran

***Abstract*— Communication messages in vehicular ad hoc networks (VANET) can be used to locate and track vehicles. While tracking can be beneficial for vehicle navigation, it can also lead to threats on location privacy of vehicle user. In this paper, we address the problem of mitigating unauthorized tracking of vehicles based on their broadcast communications, to enhance the user location privacy in VANET. Compared to other mobile networks, VANET exhibits unique characteristics in terms of vehicular mobility constraints, application requirements such as a safety message broadcast period, and vehicular network connectivity. Based on the observed characteristics, we propose a scheme called *AMOEBA*, that provides location privacy by utilizing the *group navigation of vehicles*. By simulating vehicular mobility in freeways and streets, the performance of the proposed scheme is evaluated under VANET application constraints and two passive adversary models. We make use of vehicular groups for anonymous access to location based service applications in VANET, for user privacy protection. The robustness of the user privacy provided is considered under various attacks.**

***Index Terms*— Vehicular ad hoc network, security, location privacy, safety, liability, tracking.**

I. INTRODUCTION

THE LARGE scale and frequent usage of vehicles has given rise to the pressing need for regulation of vehicular traffic and improvement of vehicle safety on freeways and streets. Consequently, upon recognizing the safety enhancement, and other potential economic benefits that can result from enabling both communication between vehicles and vehicular feedback to an ad hoc network, there have been concerted efforts to network intelligent vehicles [1], [2], [3].

In the Vehicular Ad hoc Network (VANET), intelligent vehicles can communicate among themselves (Vehicle-to-Vehicle (V2V) communications) and with road-side infrastructure (Vehicle-to-Infrastructure (V2I) communications). The VANET enables useful functions, such as cooperative driving and probe vehicle data, that increase vehicular safety and reduce traffic congestion, and offer access to Location Based Service (LBS) applications; see Section II-B. However, there are various challenges in networking as well as VANET-specific security and privacy issues that remain in order to make VANET a reality [4], [5], [6], [7], [8], [9]. For example, ensuring the safety rendered by the V2V communications tests the VANET connectivity [4] and the authenticity and integrity of the communications [8]. On the other hand, the unique requirement of maintaining the liability of vehicles when accidents occur, necessitates that vehicles be identifiable at any given time, hence giving rise to privacy concerns [6].

For vehicle liability and safety in VANET, any broadcast message from a vehicle must contain a verifiable identity as well as authentic data that may include accurate vehicle location in safety enhancing applications [8]. Moreover, advances in localization technologies enable accurate location estimation of vehicles based on transmission signal properties such as signal strength [10], [11], and the locations of wireless nodes in outdoor environments can be estimated with high resolution in the order of few meters [12], [13]. Consequently, the broadcasts of any vehicle in VANET can reveal the vehicle's identity as well as location, and can be misused to track movement of a vehicle by linking its traversed locations.

A. Problem Statement

In this paper, we address the mitigation of unauthorized location tracking of vehicles, and the alleviation of profiling of LBSs accessed from the service providers by vehicles.

The location tracking of any vehicle provides access to the past and current locations of the vehicle, including the locations that have been visited (i.e. locations of intermediate destinations of the vehicle), leading to the following vulnerabilities. First, the location history of the vehicle user can be accumulated over time. Secondly, when combined with geographical maps and additional information, the visited locations of the vehicle can be associated with places of interest, thereby enabling inference and profiling of personal interests of the vehicle user. Both of the above attacks present *threats to the location privacy* of the vehicle user [8]. Further, the location information of vehicles can be misused for crimes [9], such as abductions or automobile thefts.

Additionally, the location tracking of any vehicle also enables the identification of the LBS application accessed at any location. Therefore, location tracking can additionally result in profiling of the LBS applications accessed by the vehicle, which enables inference of personal interests of the vehicle user, presenting *threats to the user privacy*.

Location privacy protection schemes for mobile networks can be general classified as regulatory [54], policy-based [55], and anonymity-based approaches [15], [16], [50]. In this paper, we focus on the anonymity-based approaches that can mitigate the location tracking of a target by providing the target with an *anonymity set* [14], [37]. Such approaches consider *anonymity in terms of unlinkability*, i.e. the relation between two items of the target that is of interest to an

Manuscript received Feb 23, 2007; revised July 4, 2007. A preliminary version of this work [42] was presented in the workshop on *Embedded Security in Cars (ESCAR)*, Cologne, Germany, Nov. 29-30, 2005.

Krishna Sampigethaya and Radha Poovendran are with the Network Security Laboratory (NSL), Department of Electrical Engineering, University of Washington, Seattle, WA 98195-2500, USA (e-mail: rkrishna@u.washington.edu; rp3@u.washington.edu).

Mingyan Li is with The Boeing Company, Phantom Works, Mathematics and Computing Technology Division, Seattle, WA 98124-2207, USA (email: mingyan.li@boeing.com).

Leping Huang is with Nokia Research Center, Tokyo, 153-0064, Japan (email: Leping.Huang@nokia.com).

Digital Object Identifier 10.1109/JSAC.2007.071007.

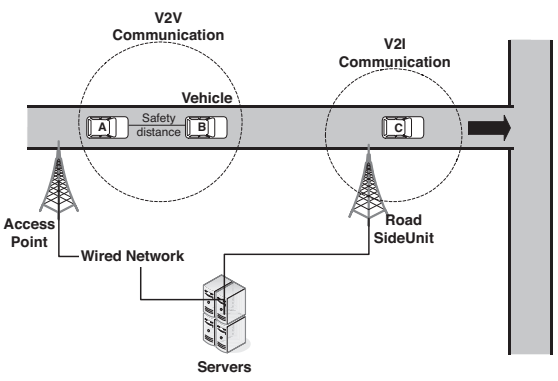


Fig. 1. Illustration of inter-vehicle communication and the components involved. The circles indicate communication between the enclosed nodes.

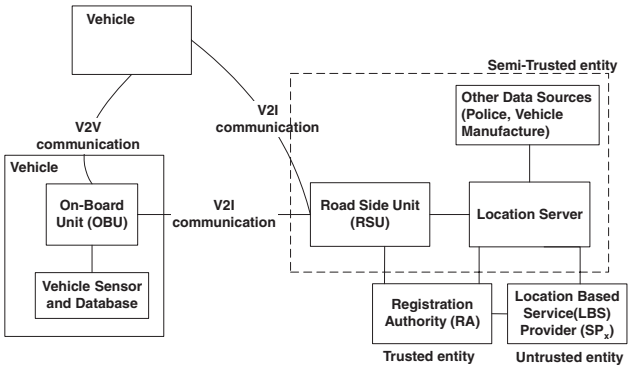


Fig. 2. Illustration of an inter-vehicle communication system model with trust assumptions.

adversary (e.g. two successive locations of the target) is not traceable [52]. Therefore, as in [15], providing unlinkability between the target's two successive locations can disable its location tracking. Further, as in [16], unlinkability between the accessed LBS application and the target location can reduce profiling of LBS applications accessed by the target.

However, unlike previous anonymity-based location privacy protection mechanisms such as in [15], [16] (see Section VI-C), in this paper we propose solutions that account for the constraints posed by vehicular mobility and VANET applications (see Section II-C) as well as an adversary that is capable of accurate location estimation of vehicles (see Section II-A).

We make the following contributions in this paper. We identify that the group navigation of vehicles can be used for location privacy and user privacy in VANET, and propose a scheme called *AMOEBA* consisting of: (i) The *group concept*: grouping vehicles to mitigate the location tracking of any target vehicle. The group concept also provides robust anonymous access to prevent the profiling of LBS applications accessed by any target vehicle; (ii) A random silent period during join technique that enables any target vehicle to increase location privacy at opportune places during navigation, but potentially at the cost of safety and liability. (iii) A solution that utilizes the power control capability of vehicles to balance the tradeoff between safety/liability and location privacy.

The rest of the paper is organized as follows. Section II describes the VANET system model and adversary models considered, and the unique constraints of VANET. Section III presents the proposed AMOEBA. Section IV discusses robustness of AMOEBA against attacks on user privacy, safety and liability. Section V evaluates location privacy enhancement by the proposed solutions. Section VI compares related work with AMOEBA, and Section VII concludes the paper.

II. System Model

Fig. 1 illustrates a typical VANET that consists of vehicles, access points on the road side, and a collection of location servers. Vehicles move on roads, sharing collective environmental information between themselves, and with the servers via access points. Fig. 2 illustrates a detailed view of the system model considered. A vehicle is enabled with an on-board communication unit for V2V and V2I communications, and sensors (for example, GPS) and database units to collect environmental information (for example, vehicle location, vehicle speed, tire pressure). The communication unit of the access points are called *Road Side Units (RSU)*, which are connected to *location server* by a wired network. The location server records all the data forwarded by the RSUs, and processes the data together with information from other data sources, for example, vehicle manufacturers, police, traffic management centers, and weather information centers. The location server also provides an interface for the *Service Providers (SP)* that offer location based services. In addition, a trusted *Registration Authority (RA)* provides authentication and authorization services to both vehicles and LBS providers.

As in [5], [8], we assume a suitable public key infrastructure is available in the VANET. Before joining the VANET, each vehicle registers with the trusted RA. Each service provider registers with the RA and obtains a public/private key pair. During registration, each vehicle i is pre-loaded with a set of w *pseudonyms* denoted $\{PID_{i,k}\}_{k=1}^{w}$, a public/private key pair $(K_{PID_{i,k}}, K_{PID_{i,k}}^{-1})$, and a corresponding public key certificate $sign_{RA}(K_{PID_{i,k}})$ for each pseudonym $PID_{i,k}$. Notation used in this paper is in Table I. Each vehicle also registers for LBSs of interest. Only the trusted RA knows the link between the real identity of vehicle and its associated pseudonyms. We assume communication protocols require a pseudonym as source address in broadcasts from each vehicle.

A. Trust Assumptions and Adversary Models Considered

The Registration Authority (RA) is a trusted entity in the system model; see Fig. 2. The RSUs and location server are only semi-trusted, i.e. they operate as expected, but can reveal data to an adversary. The RSUs can estimate location of a vehicle based on the vehicle's transmission signal. Additionally, since an adversary may deploy compromised vehicles in the network, we assume that vehicles are untrusted.

We study privacy protection of the vehicle operators under a global passive adversary, a restricted passive adversary, and a local active adversary models. A *Global Passive Adversary (GPA)* (e.g. "Big Brother" surveillance [8]) can locate and track any vehicle in a region-of-interest by eavesdropping its broadcasts. The GPA leverages the deployed infrastructure RSUs and utilizes the adversarial RSUs deployed to estimate the locations of all broadcasts in the region-of-interest.

Compared to the GPA, a *Restricted Passive Adversary (RPA)* (e.g. a compromised service provider [16]) is limited

TABLE I
STANDARD NOTATION USED IN THIS PAPER

Notation	Description
i	A entity/node in the VANET.
$i \rightarrow j$: m	Entity i broadcasts a message m to entity j.
$i \rightarrow j \rightarrow k$: m	Entity j forwards a message m from i to k.
G_j	A group j of nodes in the VANET.
$\mathcal{N}$	Set of all n nodes in the VANET, i.e. $\|\mathcal{N}\| = N$.
$\mathcal{G}$	Set of all g groups in the VANET, i.e. $\|\mathcal{G}\| = g$.
$\mathcal{H}$	Set of groups in the VANET. $\mathcal{H} \subseteq \mathcal{G}$.
L_{max}	Maximum size for a group.
GL_j	Group Leader of group G_j.
GID_j	Group ID of group G_j.
$PID_{i,k}$	k^{th} pseudonym of node i. Each node i has a set of w pseudonyms, $\{PID_{i,k}\}_{k=1}^{w} = \{PID_i\}$.
A_{GL_j}	ID of GL_j. Note that $A_{GL_j} = GID_j \|\| 0^y$, where y is size (in bits) of node ID field.
A_{aa_j}	LBS application access address selected from an address range for group G_j.
$A_{i,j}$	ID of node i that is a member of group G_j. Note that $A_{i,j} = PID_{i,k}$ or $A_{i,j} = GID_j \|\| A_{aa_j}$.
$A_{broadcast}$	Broadcast address for network.
$A_d \|\| A_s \|\| data$	Destination address || Source Address || Data.
$speriod$	Random silent period. $speriod_{min} \leq speriod \leq speriod_{max}$.
$bperiod$	Safety message broadcast period.
s_{min}, s_{max}	Minimum and maximum speed limits for a node.
p_{update}	Probability a vehicle updates pseudonym/ID.
R_{max}	Maximum number of broadcast repetitions.
T_{max}	Maximum waiting period for an ACK or a reply.
W_{max}	Maximum waiting period for a group join request.
$x \|\| y$ or (x, y)	x concatenated to y.
$\{x\}$	A set of elements.
K_x, K_x^{-1}	Public and private key pair of entity x.
$k_{x,y}$	Pairwise symmetric key of two entities x, y.
k_{G_j}	Symmetric key of group G_j.
$c = E_{K_x}(m)$	Encryption of message m with public key K_x.
$D_{K_x}(c)$	Decryption of ciphertext c with private key K_x^{-1}.
$E_{k_x}\{.\}$, $D_{k_x}\{.\}$	Encryption and Decryption with symmetric key k_x.
$sign_i(m)$	Digital signature on message m with private key of entity i.
$h(m)$	Cryptographic hash of a message m. Also, $h^n(m) = h(h^{n-1}(m))$, $n \geq 2$.
q_i	A secret quantity of node i.
S_i	A seed of an entity i.
l_i	Location of an entity i.
$d(l_i, l_j)$	Euclidean distance between two locations l_i, l_j.

in its location tracking capability in a region-of-interest, since it can only leverage the deployed infrastructure RSUs for eavesdropping and estimating locations of vehicle broadcasts. Hence, as seen later in Section V-F, the region over which the RPA can track vehicles is dependent on the vehicle transmission range and the distance between any two successive deployed RSUs.

A *Local Active Adversary (LAA)* (e.g. a stalker [16]) adaptively compromises single-hop neighbors of a target, and colludes with GPA or RPA to threaten user privacy by revealing information over side channels (see Section IV-A). However, we assume that location tracking by LAA is equivalent to a technically unresolvable physical pursuit by a stalker, and is not a location privacy threat. Additionally, we do not consider communication jamming attacks to threaten privacy, since they block communications and reduce traceability. But the LAA can threaten safety and liability by injection of misleading data and impersonation [8] (see Section IV-C).

We note that an eavesdropper may have other means to track a target vehicle, e.g. sensor application data such as video from traffic monitoring cameras that allow visual identification of the target (e.g. color, license plate number). Further, recent studies show that target's wireless card can be identified by its unique physical layer properties, e.g. electromagnetic signature [18] or timing [19]. However, we consider the adversary does not employ such means that can involve significant effort for tracking even a single target vehicle, such as deploying expensive cameras with density sufficient for desired tracking resolution, or employing specialized hardware to capture and process electromagnetic signatures. In VANET, the adversary can use physical layer properties, such as signal strength, and commercial-off-the-shelf hardware to passively track multiple vehicles. In this paper, we limit our study to such an adversary.

B. Application Scenarios Considered

Herein, we consider three typical VANET applications – cooperative driving, probe vehicle data, and Location Based Service (LBS). *Cooperative driving* is based on V2V [20], where adequately equipped vehicles maintain a very short separation (intra-convoy spacing) between each other and move smoothly with a pre-defined speed (convoy speed), while communicating frequently. For example, in a cooperative driving prototype in [21], vehicles broadcast safety messages containing their status information (e.g. location, velocity, acceleration) every 500 ms. The advantage of cooperative driving is the increase in safety and highway capacity from the automation and close coordination of vehicles [20].

The *probe vehicle data* [22] represents a class of V2I communication based applications that monitor road and traffic conditions by collecting information from vehicles equipped

with short range radio (e.g. DSRC, 802.11p) or existing long-range communication devices (e.g. cellular network). Apart from the measured data, the probe data may include vehicle identity, roadway segment identity, communication link time and location, as well as the operational status of the probe vehicle's equipment [22]. The RSU sends probe data requests over a capture range [22], and vehicles in the capture range reply to these requests. The period between broadcasts of probe replies from vehicles depends on the application requirement. For example, according to [23], a typical broadcast interval of probe data for real-time congestion estimation is 3 minutes when probe car volume is 1 vehicle/min.

A *LBS application* obtains and makes use of the most recent location of vehicles to provide a requested service [16]. For example, a service in VANET may be a query by a vehicle to find the shopping mall closest to its current location. We note that in all three applications considered, the V2V and V2I communications can be utilized by the GPA and the RPA to obtain network identifiers and location estimates of the communicating vehicles. However, it is assumed that none of the application data contains information explicitly identifying vehicle users (e.g. social security numbers, house addresses).

Next, the various constraints of vehicular networks applicable to the problems addressed in this paper are presented.

C. Mobility and Application Constraints of VANET

VANET poses constraints such as in mobility of vehicles, and in safety application requirements. The mobility of vehicles can be observed to have the following unique characteristics [24]: (1) The movement of vehicles is *spatially restricted* due to geographical constraints. For example, as illustrated in Fig. 1, the movement of vehicles is restricted to the lanes, in both streets and freeways. (2) The vehicles are *spatially dependent* on each other in movement due to the dependent velocities. For example, a succeeding vehicle A (following) modifies its velocity in order to keep a minimum safety distance [25] from a preceding vehicle B (being followed), as illustrated in Fig. 1. Further, since vehicles exhibit large variability in speed by assuming maximum as well as minimum speeds during mobility, the VANET connectivity can be *intermittent*, with the mobile communication link quality degrading significantly with inter-vehicular distance [4].

The safety applications in Section II-B impose constraints in terms of the maximum period between two broadcasts from a vehicle. In cooperative driving, the maximum period between two safety message broadcasts can vary in 100 ms - 500 ms [8], [21]. Whereas, the maximum period between probe reply broadcasts can be on the order of seconds to few minutes [23].

Therefore, overall, any privacy enhancement solution approach for VANET must take into account these constraints.

III. Proposed Location Privacy Scheme for VANET

In this section, the proposed AMOEBA and its privacy enhancement techniques are described.

A. Use of Silent Period to Provide Unlinkability Between Locations in V2V Applications

In order to achieve unlinkability between two locatable broadcasts, a vehicle can simply update its pseudonym between broadcasts. But, as observed in [15], despite pseudonym update a mobile node can still be tracked. The temporal and spatial relation between the new and old locations of the mobile node maintains the linkability between the new and old pseudonyms. As a solution to this problem, the use of a *random silent period* between update of pseudonyms was proposed in [15]. Therefore, by enforcing that the vehicle remains silent for a randomly chosen period, we can provide unlinkability for the vehicle in VANET as described below.

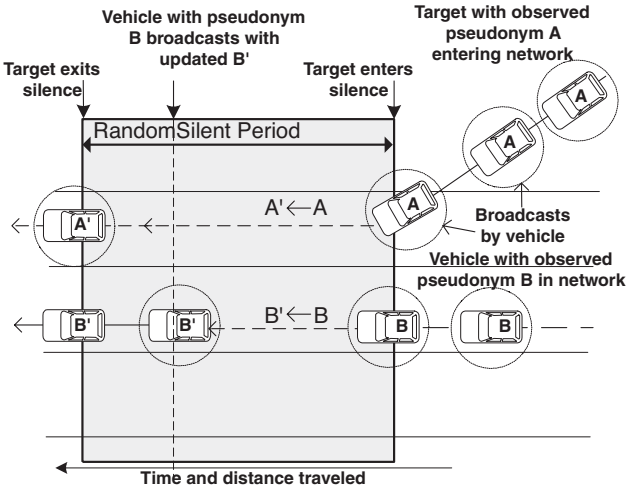


Fig. 3. Illustration of the effect of random silent period when used by a vehicle during network join. A target vehicle entering the network, broadcasts with pseudonym A, and then goes into silence. If a neighboring vehicle updates its pseudonym from B to B' during this silent period, then an adversary can be misled to consider pseudonym B' (and hence, the associated neighbor vehicle's location) to be that of the target vehicle, provided the target vehicle updates to A' before its next broadcast.

Fig. 3 illustrates the scenario where a target vehicle enters/joins a network, initially broadcasts safety messages, then remains silent and updates it's pseudonym from A to A', and finally broadcasts with A' after a random silent period. If one of the neighboring vehicles also updates pseudonym from B to B', during this silent period, then the adversary can be misled to track the neighboring vehicle as the target. Thus, the random silent period technique during a join can mitigate tracking of vehicles. The evaluation of the mitigation of vehicle tracking using the random silent period during a join is in Section V-E.

However, for cooperative driving, the maximum silent period is limited by the *safety message broadcast period*, i.e. period between two safety message broadcasts, which is on the order of hundredths of millisecs [8]. With maximum silent period limited to the order of hundredths of millisecs, it is possible to track vehicles based on temporal and spatial relation between locations, as will be seen in Section V-D.

An increase in the random silent period enlarges the safety message period, and the resulting location privacy level is obtained at the cost of safety. As a solution, we propose vehicles be silent when merging and/or changing lanes, e.g. when joining freeway via an on-ramp or leaving the freeway via an off-ramp compared to when moving in lanes. The ramps that allow vehicles to merge into lanes in freeways are relatively safer locations compared to freeway mainlines [27]. The use of such a solution can achieve a balance between privacy and safety enhancement under the GPA model. The

inherent uncertainty in vehicle movement during lane merging/changing increases location privacy compared to mainlines where vehicles move straight as shown by us in [26]. At the same time the accident rate is lower when merging/changing lanes compared to when keeping lanes [27], [28].

On the other hand, while under the constraint of the safety message broadcast period the random silent period technique does not alleviate tracking by GPA, it can still successfully alleviate tracking by RPA as shown later in Section V-F.

Next, we present the group concept for extending random silent period without lowering safety in V2I applications.

B. Use of Group Concept to Extend Silent Period in V2I Applications

The following observations motivate the group concept.

(1) As noted in Section II-C, the mobility of vehicles is spatially restricted and spatially dependent. Hence, vehicles in geographical proximity can navigate as a group. These vehicles will have the same average velocity due to the spatial dependency and similar direction due to the spatial restrictions, over a period of time.

(2) Vehicles in geographical proximity often measure redundant information such as road and traffic conditions. When using probe vehicle data, where the vehicles respond to measured data requests received from the infrastructure, not all the vehicles need to reply.

(3) A group of navigating vehicles within a distance $r_0/2$, where r_0 is vehicle transmission range, are geophysically proximate and can maintain full connectivity, and the group communication does not suffer any significant signal degradation. For instance, given that $r_0 = 300$ m is a typical value [1], it is shown in [4] that signal-to-noise ratio (SNR) for mobile communication between vehicles within a distance of 150 m on a freeway is adequate to provide reliable communication.

Based on the above observations, we propose to enable vehicles to form a *group during navigation*. In order to form a group, each group member vehicle must be able to hear the broadcast of every other group member (i.e. within distance $r_0/2$). Thus ensuring that a fully connected network graph exists within the group (based on observation (3)). Since vehicles in a group will move relative to each other and on average have the same velocity (based on observation (1)), a group can be represented by a single vehicle that is referred to as the *group leader*. The election of a group leader is randomized among the *group members*, as described in the Group Leader Rotation protocol in Appendix A. The full connectivity within group enables group operations in which all the group members can participate. The different group protocols of AMOEBA are provided in Appendix A.

For V2I based applications, such as probe vehicle data, it is sufficient if only the group leader communicates on behalf of the group/group member (based on observation (2)). Consequently, remaining vehicles in group can be silent for an extended random period of time that is bounded by the time they stay in the group. As discussed in the previous section, a random silent period can alleviate location tracking of vehicles. Therefore, for applications not requiring very frequent periodic broadcast from all vehicles (order of hundredths of millisecs), the location privacy level can be increased by the extended random silent period from vehicular groups.

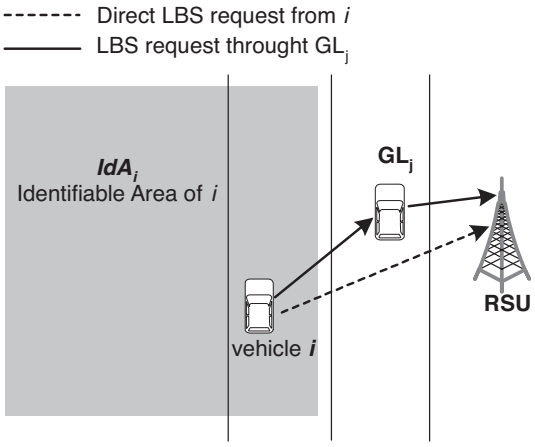


Fig. 4. Illustration of access to a LBS application by a vehicle i which is member of the group G_j, with the group leader vehicle being GL_j. If i requests LBS directly using a pseudonym, then location of i can be linked to LBS, and since i is located in an identifiable area IdA_i (shaded area), the real identity of i is revealed and linked to LBS application. If i requests LBS through the group leader GL_j, then it can mitigate the linkability with LBS.

In probe data application, where typically vehicles send probe replies once in several seconds, the use of the group concept provides the following advantages: (i) The silent period of a group member is extended, if the vehicle does not change groups between two probe data requests. (ii) Unnecessary overhead and redundancy in neighbors broadcast of possibly redundant probe data is reduced, since only the group leader replies to the RSU with probe data. (iii) Pseudonym updates for thwarting adversarial tracking over t are reduced (where t is the maximum probe reply broadcast period). This will reduce the number of pseudonyms used for a target navigating in a group during t. In comparison, a target not in a group must broadcast at least one probe reply during t.

Further, the group concept can be leveraged to protect user privacy when vehicles tracked by the GPA are accessing LBS applications, as seen next.

C. Leveraging Group to Provide Unlinkability Between Vehicle Location and LBS Application

In order to allay profiling of the LBS applications accessed by a target vehicle, it is necessary to provide unlinkability between them. However, this does not always prevent profiling of LBS applications accessed by the target. Fig. 4 illustrates a scenario where a vehicle i is navigating in an *identifiable area* IdA_i that is uniquely associated with its real identity [16]. An identifiable area can be defined by means of geographical information available on i (e.g. geocoded postal addresses [16]). The adversary can assume that any broadcast in IdA_i over a time period is most likely from i, hence associating all pseudonyms overheard in IdA_i with i. Thus, the mitigation of tracking of i in IdA_i is not possible. If i accesses a LBS application in an identifiable area, then by estimating the location of the LBS request broadcast the global adversary can link i's pseudonym as well as i's real identity with the application, leading to breach of privacy of the user of i.

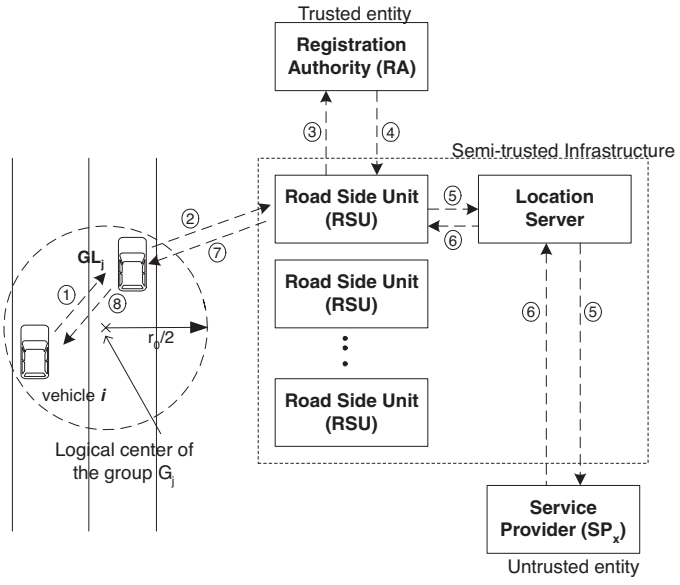


Fig. 5. Illustration of the anonymous access to LBS application provided to a vehicle i which is member of the group G_j with the group leader vehicle being GL_j. The sequence of steps in the protocol are indicated in the figure.

Therefore, to reduce profiling of LBS applications accessed by a target vehicle, the target's location during access must be unlinkable to the application. This approach is taken in [16], where the target's location is distorted in temporal and/or spatial dimensions. Based on this idea, the group concept enables a solution by providing unlinkability between the location of LBS application request broadcast and the LBS application requested. As shown in Fig. 4, the vehicle accessing the LBS application makes use of the group leader as a *proxy for anonymous access*. This solution protects user privacy even if vehicle is tracked by GPA, as will be seen in Section IV-A. The anonymous access protocol is described below.

1) Protocol Description: Fig. 5 provides a visual description of the anonymous access protocol and the steps involved. To maintain clarity of exposition, the pseudocode for Anonymous Access protocol is provided in the Appendix B. From Fig. 5 it can be seen that upon receiving the LBS application request from vehicle i (in Step 1), the group leader GL_j of i's group G_j forwards the request with its own pseudonym and location, to the registration authority RA via the RSU (in Step 2-3). The RA validates the application request, and then provides a session key $k_{x,i}$ to both the service provider (SP_x) and vehicle i (Step 4-7). This key is used to encrypt and secure the subsequent communication that takes place between i and the SP_x. GL_j broadcasts the communication received from SP_x (via RSU) to the group (Step 8). Therefore, i anonymously receives service from SP_x.

On termination of the application, the SP_x as well as vehicle i provide the application transaction details to the RA, which acts as the arbiter and resolves any disputes. Note that in order to lower the load of the RA, anonymous payment based protocols such as [29], can be used in the LBS application access. However, such a payment scheme is not provided here, since it is out of scope of this paper.

2) Application Address Range and Group Key: When generating a LBS request, vehicle i does the following: (i) randomly chooses an available address A_{aa} from a *application address range* of the group G_j as the source address, and, (ii) encrypts the application request with a *group key* k_{G_j}. The two parameters, A_{aa} and k_{G_j}, are obtained by each member of group G_j from the leader GL_j when joining G_j (see Group Join protocol in Appendix A). These two parameters can mitigate traceback from GL_j to i (during Step 1 of the Anonymous Access protocol) as follows.

Since the random address A_{aa} is not associated with i, the LBS request from i cannot be associated with any of its pseudonyms, making the LBS request unlinkable to i. Moreover, by providing the application address range, a vehicle's set of w pseudonyms is conserved. However, since a global adversary can overhear all broadcasts in G_j, it can trace i by relating the location of the overheard LBS request broadcast sent from i to GL_j, with the overheard safety message broadcast of i in G_j as follows. Vehicles broadcast safety messages on the order of hundredths of millisecs. If i broadcasts a LBS request, then the time difference between the safety message broadcast containing $PID_{i,k}$ and the LBS request broadcast containing A_{aa} is small. This implies that the distance between locations of the two broadcasts from i is small. Therefore, the GPA computes the distances of the locations $\{l_a\}_{k \in G_j}$ of all safety broadcasts of group G_j from the location l_{LBS} of the LBS request broadcast, and identifies vehicle i whose location during safety broadcast is closest to location of the LBS request broadcast, i.e. target = $\arg\min_{a \in G_j} d(l_a, l_{LBS})$, where $d(l_a, l_{LBS})$ is the Euclidean distance between locations l_a, l_{LBS}.

On the other hand, the encryption of the LBS request with k_{G_j} prevents tracing of i based on the format of the LBS request message broadcast to GL_j (in Step 1 of the Anonymous Access protocol). Nevertheless, the adversary may still differentiate a LBS request based on its appearance as an encrypted broadcast in G_j, from the otherwise unencrypted communications in G_j. Hence, because the LBS request broadcast from i to GL_j (in Step 1) can be linkable to i, the following mechanism is proposed to prevent identification of the LBS app_x accessed by i from SP_x.

3) Group Leader as a MIX: In order to prevent trace back of LBS request broadcasts in G_j, the group leader GL_j *functions as a MIX* [30] and performs the following.

(i) *Changes appearance of the LBS request*. The GL_j decrypts the LBS request from i with k_{G_j}.

(ii) *Changes the order of arrival of LBS requests*. Apart from LBS request of i, GL_j waits for more LBS requests from at least one other member in G_j. The batch of requests are then forwarded to the RSU in a random order.

The adversary cannot identify the LBS request from i by correlating the appearance of broadcasts from i to GL_j and from GL_j to RSU (in Step 2), or by correlating the order of requests sent to GL_j and to the service providers (in Steps 4, 5). Thus, unlinkability can be provided between location of i and the accessed LBS app_x. However, the GPA can collude with compromised vehicles to identify the LBS accessed by i, and breach privacy of the user of i, as discussed next.

IV. Discussion of Attacks on AMOEBA and Defense Mechanisms

This section addresses attacks on the privacy and security of the group concept, and group concept limitations.

A. Attacks on User Privacy

The GPA can collude with the LAA for following attacks on the privacy of users accessing LBSs in the VANET.

1) Deterministic Mixing of LBS Requests: In order to link a vehicle i to the accessed LBS application app_x, a compromised group leader can mix the LBS requests using a pre-loaded, adversary-known permutation, instead of mixing randomly as in Section III-C.2. Based on this known order of requests forwarded by GL_j, the GPA can trace the LBS request from i up to the RA (Step 1-3 of the Anonymous Access protocol). When the requests with application information are forwarded by RA to the service provider in the same order (in Steps 4, 5), the GPA can identify and link app_x with i.

The attack described above can be addressed using a *verification of mixing* scheme at GL_j. Any verified incorrect mixing will allow the group members (including i) to detect that GL_j is corrupt. In the mixnet literature, robust mechanisms have been proposed to verify that a MIX operates as expected, i.e. to verify the change in appearance and order of the inputs due to the mixing (see [31] for an overview of mixnet verification mechanisms). Nevertheless, the proposed scheme requires a verification mechanism to ensure that a random permutation is used by the leader to change the order of LBS requests. The change in appearance of the requests is due to decryption with group key k_{G_j} known to all members of G_j, and hence readily verifiable. The following mechanisms are proposed to verify the random permutation for mixing of LBS requests.

(i) *Random time delay in LBS request*. In this approach each vehicle i accessing an LBS in the group will provide in the LBS request, a random time delay, $t_{r_i} \in \{0, t_{max}\}$, where t_{max} is a fixed maximum time limit. Upon collecting a predetermined batch size b of two or more LBS requests from members of G_j, the leader GL_j initiates the forwarding of requests. The order of forwarding is determined by the order of time delays in the requests, beginning from the request with the smallest delay and ending at the request with the largest delay. Since the LBS requests are encrypted with the group key, only the group members are aware of the time delays and can anticipate the order of forwarding. Therefore, any incorrect mixing by the leader will be detected by the members.

(ii) *Joint generation of seed for random permutation* $\pi : b \rightarrow b$. All group members in G_j participate in the joint generation of a *group seed*, $S_{G_j} = \odot_{i \in G_j} S_i$, for the random permutation $\pi = f(S_{G_j})$, where S_i is the local seed contributed by member i. $\odot$ represents an operation on the local seeds (such as a exclusive-or operation) to generate the group seed. f is a pseudorandom function. In order to robustly generate (i.e. in the presence of two or more colluding group members) a random group seed, a distributed protocol such as in [32] can be integrated in the leader rotation protocol (discussed below).

2) Disclosure of Group Secrets: So far it is assumed that GL_j or any member of G_j will not disclose group secrets (i.e. group key, application address range, group seed, or order of mixing to the GPA) through a side channel. With knowledge of group secrets the GPA can breach user privacy. For example, with the knowledge of the group seed S_{G_j}, the GPA can correlate requests received and forwarded by GL_j, leading to the attack based on deterministic mixing. Such attacks can be defended by decorrelating the order of requests using a cascade of MIXes [30] or by periodically updating the group secrets. Based on these approaches the following are proposed.

(i) *Trusted RA as a Second MIX*. Since the RA participates in forwarding of LBS requests, the RA can additionally mix[1] them – change of appearance from decryption of requests with private key of RA and random re-ordering of decrypted requests – before forwarding them to service providers (in Step 4 of the Anonymous Access protocol). The mixing by RA prevents the adversary from successfully correlating requests received and forwarded by RA, defending deterministic mixing by GL_j and attacks based on group secrets.

(ii) *Periodic Group Leader Rotation*. The attacks based on group secrets can be alleviated by a periodic, Group Leader Rotation protocol (in Appendix A). During leader rotation, the group participates in generating a new group seed S_{G_j}, and the new leader distributes a new group key (in Step 7 of Group Leader Rotation protocol). Hence, both the group seed and key are updated. Note that the effectiveness of the leader rotation against attacks is determined by the rotation period which fixes the vulnerability window against attacks.

3) Tracing Based on Group Secrets: For identifying target i during LBS access, a compromised GL_j can provide an incorrect group key k'_{G_j} when i joins the group, enabling identification of LBS requests from i based on encryption with k'_{G_j}. Such attacks can be defended by using the RA as a second MIX for LBS requests and by the periodic leader rotation.

4) Collusion Between New and Old Leader: If the new and old leaders collude, then a periodic leader rotation mechanism cannot prevent the attacks based on disclosed group secrets, since the updated group key selected by the new leader can be a pre-loaded quantity that is known to GPA. Therefore, to address such collusion based attacks, the election of the group leader must be randomized. This can be achieved by means of a randomized leader election protocol, such as in [32], that is robust up to a number of colluding group members.

5) Dummy LBS Requests: When a target vehicle broadcasts a LBS request, a compromised group member can broadcast $(b-1)$ dummy LBS requests, and if the leader mixes and forwards the b requests, then the LBS being accessed by the target is successfully identified. This attack is similar to the blending attack proposed in [33], where for tracing inputs through a MIX the adversary selectively controls the inputs entering the MIX. Defense mechanisms for this attack include increasing the mixing batch size b or the use of timed pool mixing [34] where some requests are retained in a pool and forwarded in later batches. Such approaches increase the adversarial effort needed to trace LBS requests.

[1]With the group leader as a first MIX, the RA is not burdened with participating between initiation and termination of LBS access.

B. Limitations of the Group Concept

In the group concept, the node functioning as the group leader incurs computational overhead in executing the above group protocols and defense mechanisms. Additionally, the leader sacrifices its location privacy by continually revealing its locations in the V2I applications. However, the periodic group leader rotation protocol distributes the leader role over time amongst the group members, thereby distributing overhead and loss of privacy of the leader in that group.

Further, proposed use of the leader as a proxy for LBS access presents lack of end-to-end connectivity between the service provider and group members. Although VANET routing and its security are assumed to be out of the scope of this paper, we note that inherent limitations of the group, such as lack of route transparency and leader presenting a single point-of-failure for members accessing services, are well-known drawbacks of the Network Address Translation (NAT) routing.

Furthermore, use of mixing and defense mechanisms, such as random delay in mixing, by the group leader can incur latency in LBS access by the group members. Several studies in the mixnet literature have investigated this well-known tradeoff between anonymity and latency [35].

C. Active Attacks on Safety and Liability

The LAA can perform the following security attacks on the safety and liability of a target vehicle.

1) Attack on Vehicle Safety: The LAA in VANET can misbehave and broadcast incorrect data to attack neighboring vehicles [36]. However, in AMOEBA, since each vehicle signs the broadcast safety messages (in Step 1 of Cooperative Navigation protocol in Appendix A), the misbehaving vehicle will be held liable for providing incorrect data. However, in order to detect such attacks on vehicle safety, each vehicle must be able to detect the incorrect safety messages. In [36], a scheme is proposed to detect incorrect data, by enabling each vehicle to maintain its own observations of the neighborhood (such as estimated locations of neighboring vehicles) and check data received from neighbors for any inconsistencies.

2) Attacks on Vehicle Liability: In order to evade liability, the LAA can participate with a random pseudonym in the VANET. However, such an attack is prevented in AMOEBA, since broadcast from each vehicle must include a pseudonym and a certificate from the RA containing the pseudonym (in Step 1 of Cooperative Navigation protocol). The LAA can also attempt to impersonate i using one of its overheard pseudonyms and the associated certificate [8]. Such impersonation attacks are avoided in AMOEBA by making each vehicle sign the broadcast message and include the certificate from RA containing the public key corresponding to the pseudonym used (Step 1 of Cooperative Navigation protocol). Similar defense mechanisms are considered in [7], [8].

Apart from attacks on user privacy by the GPA colluding with the LAA, and attacks on safety and liability by the LAA, the GPA can perform passive attacks on location privacy of a user based on location tracking of its vehicle in the VANET. Therefore, the next section evaluates the mitigation of location tracking of a target vehicle that can be achieved by AMOEBA.

V. Evaluation of VANET Location Privacy

In this section, first, the potential tracking methods that can be employed by an adversary to link two locations of a target vehicle are described, followed by evaluation of location privacy under the tracking methods considered.

A. Tracking of Vehicles

In order to link two visited locations of the target an adversary needs to (i) identify an *anonymity set* [37] of the target — defined as the set of vehicles that are indistinguishable from the target, with the set including the target itself — and, (ii) choose a potential candidate for target.

1) Identifying an Anonymity Set: In order to identify the anonymity set containing the candidates for the target, the adversary performs the following. Given the target's last observed location l_{known} at time t, and based on all possible movements (i.e. a range of possible velocities) of the target, a *reachable area* A_r from l_{known} is determined by the adversary. The reachable area represents the region in which the target is expected to reappear with a new pseudonym. Fig. 6 illustrates a typical reachable area of a target vehicle as the half ring bounded by the lane layout, determined at t using the known achievable speed range $[s_{min}, s_{max}]$, and the minimum and maximum silent period values, $speriod_{min}$, $speriod_{max}$, respectively. Note that it is assumed that the restricted mobility of vehicles prevents them from taking certain directions, and also that the adversary possesses knowledge of the speed range and the silent period range. All vehicles that update their pseudonym at least once in the reachable area during $[t+speriod_{min}, t+speriod_{max}]$ are candidates for the target, and constitute elements of the target's anonymity set.

2) Choosing a Potential Candidate from Anonymity Set: Upon identifying the target's anonymity set, for tracking a target the adversary must choose a potential candidate from the anonymity set to be the target. Based on how the potential candidate is chosen, the following two types of tracking methods are considered in this paper.

(i) *Simple Tracking:* In this method, the adversary assumes that each element of the anonymity set is *equally likely* to be the potential candidate for the target, and hence, randomly chooses an element as the target. Fig. 6(a) illustrates the simple tracking of a vehicle where, given a set of three vehicles A, B, C that update pseudonym in the reachable area, the adversary randomly chooses one of the three vehicles to be the target.

(ii) *Correlation Tracking:* Under correlation tracking, the adversary estimates a location of the target in the reachable area A_r, and then chooses a candidate for the target as the element of the anonymity set that updates pseudonym and appears closest to the estimated location. As illustrated in Fig. 6(b), after determining A_r, based on target's last known location l_{known}, $speed$, and $direction$ at time t the adversary can estimate target's location l_{est1} in A_r at a future time $t + t_1$. The adversary chooses vehicle B that updates and appears closest to l_{est1}. Correlation tracking is repeated in A_r after each broadcast period $bperiod$, until the maximum silent period $speriod_{max}$ is reached. The adversary obtains up to n estimated target positions $\{l_{esti}\}_{i=1}^{n}$ at times $\{t+t_i\}_{i=1}^{n}$, where $t_i = speriod_{min} + (i-1)bperiod$, with $t_i \leq speriod_{max}$, and

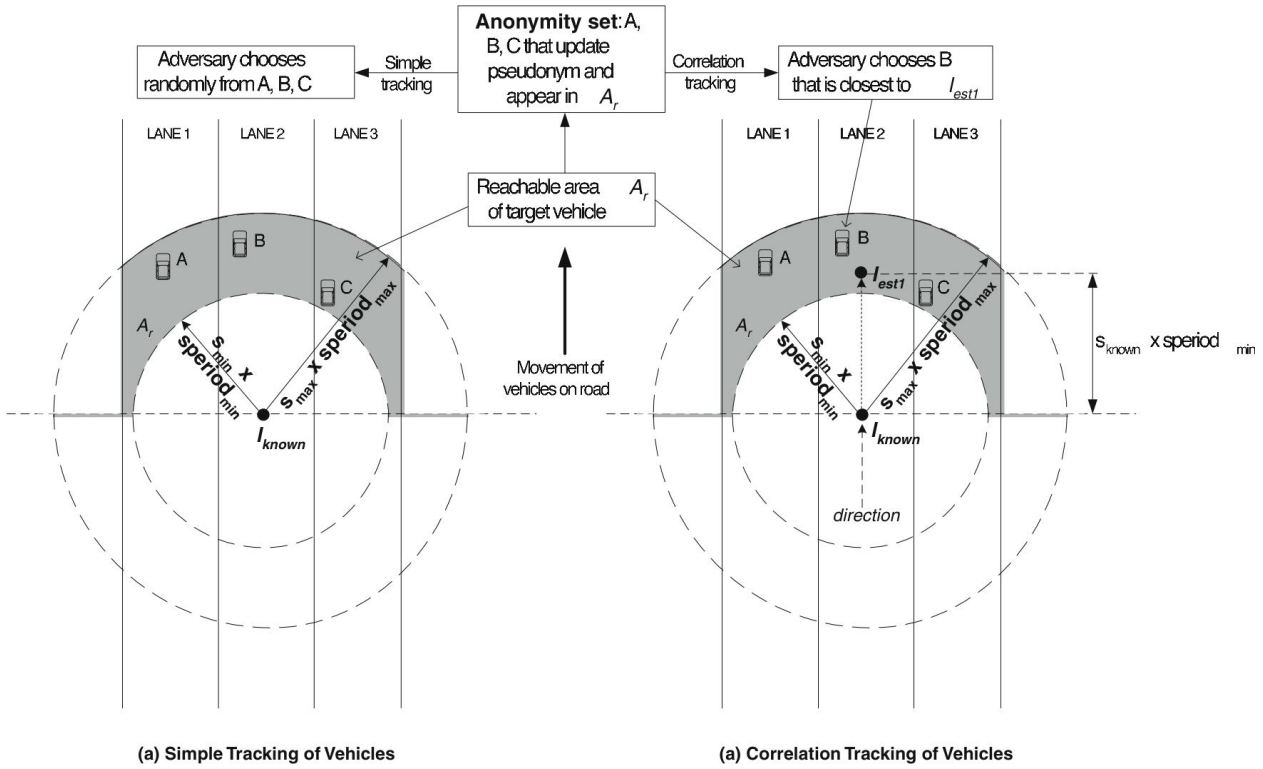


Fig. 6. Illustration of simple tracking and correlation tracking of vehicles. s_{min}, s_{max} are the minimum and maximum speed limits, and, $speriod_{min}, speriod_{max}$ are the minimum and maximum silent period values, respectively. The reachable area A_r is defined by the minimum reachable distance d_{min} and maximum reachable distance d_{max}, where $d_{min} = s_{min} \times speriod_{min}$, $d_{max} = s_{max} \times speriod_{max}$. In the case of periodic broadcast, $speriod_{min} = speriod_{max} = bperiod$, where $bperiod$ is the broadcast period. All vehicles that update pseudonym in A_r are included in target anonymity set. (a) Simple tracking of target: A vehicle from the anonymity set is randomly chosen to be the potential target. (b) Correlation tracking of target: Location l_{est1} is estimated at time $t + t_1$, using the observed velocity (i.e. speed s_{known}, $direction$) of target at last observed position l_{known} at time t, where $t_1 \in [speriod_{min}, speriod_{max}]$. Vehicle from anonymity set that is closest to l_{est1} is chosen as potential target. Since vehicles may not change direction frequently, they become susceptible to correlation tracking, as shown in the evaluation.

up to n target candidates from the anonymity set. Therefore, using correlation tracking the adversary can assign a non-uniform probability distribution to the target anonymity set. An element i that is chosen as a candidate at m of n estimated target positions in A_r is assigned a probability of $p_i = m/n$. The element in the anonymity set that has the highest probability will most likely be chosen to be the target.

For evaluating the mitigation of location tracking, the level of anonymity provided to the target must be measured, i.e. the level of unlinkability [14] between two locations of the target. Before evaluating anonymity under the two tracking methods by simulation, an analytical evaluation of the anonymity level under the simple tracking method is presented below.

B. Analytical Evaluation of Anonymity

In order to evaluate the level of anonymity (unlinkability) achieved in a VANET the following performance measures are used: (i) the *entropy* of the distribution of elements of anonymity set, and (ii) the *maximum tracking time*. Anonymity set was introduced by Chaum [37], and the size of anonymity set was shown to be a good indicator of anonymity level, when the elements of the anonymity set have a uniform distribution [17]. However, for an anonymity set with a non-uniform distribution, the entropy of the distribution was shown to be a more suitable metric for anonymity level [17], as will be illustrated in Section V-D. Let the anonymity set of a target be denoted by S_A, and the size of anonymity set be denoted as $|S_A|$. Let the probability that an element 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 S_A, is given by $H(p) = -\sum_{i=1}^{|S_A|} p_i \log_2 p_i$. The second measure, *maximum tracking time* of a target, denoted by T_{track}, is defined here as the maximum cumulative time that the target anonymity set size remains as one.

It is assumed that vehicles are uniformly distributed on streets or freeways with density ρ. Although uniform density neglects the constraints imposed by the street layout, Seskar et al. [38] showed that uniform distribution is sufficient for estimation of the number of vehicles crossing cell boundaries in mobile cellular networks, when the street layout is not symmetric and the velocities and densities are properly related. In the simulation, it is assumed that the arrival rate and the departure rate are the same. Therefore, the total number of vehicles in the vehicular network deployment region, denoted by N, and the density of vehicles remain the same statistically.

Given vehicles are uniformly distributed, the number of vehicles in area A, denoted by $\nu(A)$, distributes according to spatial Poisson process as [39]: $Pr\{\nu(A) = i\} = \frac{(\rho A)^i}{i!} e^{-\rho A}$, with average as ρA.

Suppose that a global adversary is tracking a target by overhearing the broadcast of the target, and is using the *simple tracking method*. The duration between each broadcast can be regarded as silent period, denoted by $speriod$. First, consider

TABLE II
SIMULATION SETUP. p_x - PROBABILITY OF CHANGING DIRECTION.

Parameter	*Setting*	
Mobility model	Freeway	Manhattan (Street) $p_0 = 1/2$, $p_{\pi/2} = 0.25$, $p_{-\pi/2} = 0.25$
Safety distance	20 m	10 m
Region	4 lanes, 5km length, one direction, 3m lane separation	3 × 3 uniform street grid, 2km length, 0.5km street separation, 2-lane one-way street or 2-lane two-way street, 3m lane separation
Traffic volume	3000 vehicles/hour/lane	1000 vehicles/hour/street
Node Density	[100, 500] vehicles/lane	[50, 250] vehicles/street
Node Speed	[72, 144] km/hr	[36, 72] km/hr
Node Acceleration	[0, 5] m/sec^2	[0, 2] m/sec^2

the scenario that every vehicle will use a new pseudonym in each broadcast. As seen in Section V-A.2, any vehicle that appears in the reachable region with a *new* pseudonym is a candidate for the target to the adversary.[2] Given that there is at least one vehicle, the target, in the reachable area A_r, the probability that the target can be uniquely identified at each transmission, denoted by p_{track}, is:

$$\begin{aligned} p_{track} &= Pr\{\nu(A_r) = 1 | \nu(A_r) \geq 1\} \\ &= \frac{Pr\{\nu(A_r) = 1\}}{1 - Pr\{\nu(A_r) = 0\}} = \frac{\rho A_r e^{(-\rho A_r)}}{1 - e^{-\rho A_r}}. \end{aligned} \quad (1)$$

The expected maximum tracking time is:

$$\begin{aligned} E\{T_{track}\} &= \sum_{i=1}^{\infty} i p_{track}^{i-1}(1 - p_{track}) E\{speriod\} \\ &= \frac{E\{speriod\}}{p_{track}}. \end{aligned} \quad (2)$$

The expected size of the anonymity set of a target is:

$$\begin{aligned} E\{|S_A|\} &= E\{\nu(A_r) | \nu(A_r) \geq 1\} \\ &= \frac{E\{\nu(A_r)\}}{1 - Pr\{\nu(A_r) = 0\}} = \frac{\rho A_r}{1 - e^{-\rho A_r}}. \end{aligned} \quad (3)$$

Using simple tracking, each element of S_A is equally likely to be the target, the expected entropy of the anonymity set of the target is:

$$\begin{aligned} E\{H(p)\} &= -\sum_{i=1}^{E\{|S_A|\}} \frac{1}{E\{|S_A|\}} \log_2 \frac{1}{E\{|S_A|\}} \\ &= \log_2 E\{|S_A|\}. \end{aligned} \quad (4)$$

Next, consider the case that a vehicle will update its pseudonym with probability $p_u \leq 1$ at each broadcast. In this scenario, the anonymity set of the target is equal to l for $l \geq 2$, if and only if *(i)* the target updates its pseudonym, and *(ii)* there are $l - 1$ other vehicles updating their ID's, out of $\nu(A_r) - 1$ vehicles, which is the number of vehicles in A_r excluding the target. Given the number of vehicles in A_r, the number of vehicles broadcasting with new ID's is binomially distributed. For $l \geq 2$:

$$\begin{aligned} &Pr\{|S_A| = l\} \\ &= \sum_{i=l}^{N} Pr\{|S_A| = l | \nu(A_r) = i\} Pr\{\nu(A_r) = i | \nu(A_r) \geq 1\} \\ &= \sum_{i=l}^{N} \binom{i-1}{l-1} (p_u)^l (1 - p_u)^{(i-l)} \frac{(\rho A_r)^i e^{-\rho A_r}}{i!(1 - e^{-\rho A_r})}. \end{aligned}$$

The probability p_{track}, when the pseudonym update probability of each vehicle is p_u, is:

$$\begin{aligned} &p_{track}(p_u) \\ &= 1 - \sum_{l=2}^{N} Pr\{|S_A| = l\} \quad (5) \\ &= 1 - \sum_{l=2}^{N} \sum_{i=l}^{N} \binom{i-1}{l-1} (p_u)^l (1 - p_u)^{(i-l)} \frac{(\rho A_r)^i e^{-\rho A_r}}{i!(1 - e^{-\rho A_r})}. \end{aligned}$$

Then, the above $p_{track}(p_u)$ can be applied to Eq. (2) to obtain the expected maximum tracking time. Next, the average size of the anonymity set is:

$$\begin{aligned} &E\{|S_A| \text{ for given } p_u\} \\ &= \sum_{l=2}^{N} l \cdot Pr\{|S_A| = l\} + 1 \cdot (1 - \sum_{l=2}^{N} Pr\{|S_A| = l\}) \\ &= 1 + \sum_{l=2}^{N} (l - 1) Pr\{|S_A| = l\}. \end{aligned} \quad (6)$$

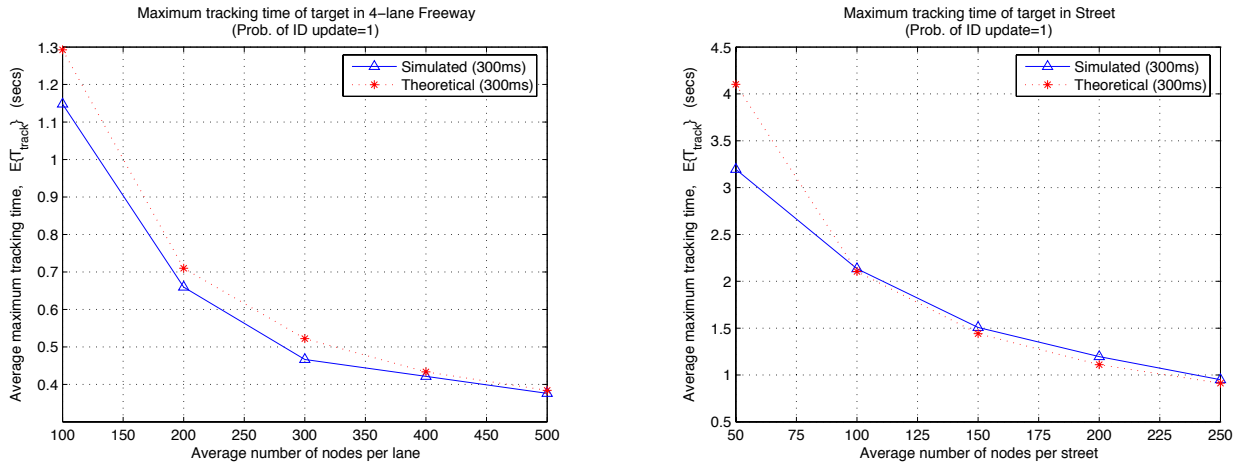
Using Eq. (6) in (4), the entropy using simple tracking can be obtained. Letting $p_u = 1$, it is easy to verify that Eq. (5) and (6) reduce to Eq. (1) and (3), respectively.

C. Simulation Setup

In order to capture the salient features of vehicular mobility, the following mobility models proposed in [24] are considered in this paper: (1) *Freeway*, and (2) *Manhattan* referred hereon as *Street* model. Table II summarizes the chosen simulation settings for these two models. In addition to the *car following behavior* [25] for modeling the speed of a succeeding vehicle at a *safety distance* from the preceding vehicle, we further incorporate the *changing lane behavior* [40] to model the movement of the succeeding vehicle. The succeeding vehicle can change lanes, after a tolerance time, if no vehicle is within safety distance of the new position.

The 4-lane setting for a freeway and the 2-lane setting for a street are chosen to represent a common scenario encountered in North America, Europe, and other parts of the world. The

[2]We assume that vehicles periodically broadcast around the same time. Then the number of vehicles in the reachable area will be the number of new pseudonyms in target anonymity set. Also note that an adversary cannot distinguish vehicles based on the order of broadcast due to random access.



(a) (b)

Fig. 7. Maximum Tracking Time of a target under global adversary model, and safety broadcast period of 300 ms. (a) 4-lane freeway, with different number of vehicles per lane. (b) street model, with different number of vehicles per street.

arbitrary settings for the simulation region of both mobility models can be generalized. The traffic volume and density are approximated from [16], where 24-hour traffic volume estimates are provided based on real traffic data.[3] The range for the average number of vehicles per lane (street) covers different traffic densities including the scenarios in [16].

Initially, vehicles are uniformly distributed in the lanes. For each lane/street, the inter-arrival and departure process is exponential with the rates set to be the same, leading to almost the same average number of vehicles per lane/street over time. Each data point in the simulation plots presented is an average of more than 100 iterations. The border effect of the bounded simulation region on the vehicle mobility is accounted for by making the vehicle randomly reappear in the region.

Due to the higher traffic volume, the average number of vehicles per lane for the freeway is higher compared to the street model. This setting holds under the assumption that there is free flow movement of vehicles, i.e. without taking into account any congestion that may arise in the streets. Currently the simulations do not model traffic lights, stop signs at intersections or the length of vehicles. Communication traffic models are ignored as well.

D. Location Privacy under Global Passive Adversary

This section evaluates the average anonymity for a vehicle when the adversary overhears all broadcasts of all vehicles.

Fig. 7 shows that the average maximum tracking time of a target, $E\{T_{track}\}$ for a typical safety message broadcast period of 300 ms. It can be seen that $E\{T_{track}\}$ reduces to the safety message broadcast period with increase in the number of vehicles per lane (street). This implies that with increase in number of vehicles per lane (street), a single pseudonym update can provide the target with an anonymity set of adequate size (at least two on average). However, for a correct estimate of anonymity provided under simple and correlation tracking, the entropy of the anonymity set distribution must be evaluated.

Fig. 8(a), 8(b) show the entropy of the anonymity set provided to a target in the freeway, when it updates pseudonym between two of its safety message broadcasts. The probability that any vehicle updates its pseudonym, p_u, determines how many neighboring vehicles of target update pseudonym along with the target. Hence, with an increase in p_u, it is expected that as in Fig. 8(b), the entropy of the target anonymity set increases from the minimum value of 0.

Fig. 8(c), 8(d) show the achievable entropy in the street map. By comparing Fig. 8(a)–8(b), with Fig. 8(c)–8(d), it is seen that the variation in the entropy is identical, but, the entropy in streets is lower. This is due to the relatively lower vehicle density in streets as discussed in the previous section, since in this paper only lower traffic volume for the streets is considered relative to the freeway. Note that Fig. 7, and 8 also show the theoretical maximum tracking time and the entropy of anonymity set, derived from Eq. (2), (4), respectively.

From Fig. 8 it can be observed that as the safety message broadcast period is increased from 100 ms to 500 ms, the level of anonymity increases with number of vehicles per lane (street) using simple tracking. However, for correlation tracking the entropy remains close to 0 even with increase in vehicles per lane (street), indicating successful tracking of vehicles. The reason is that since spatial imprecision is small in cooperative driving and vehicles tend to not change direction in short time intervals, there is temporal and spatial relation between visited locations. This additional knowledge can be used by the GPA to assign different levels of uncertainties to the nodes in target anonymity set, consequently degrading entropy of the anonymity set distribution.

The above observation related to Fig. 8 also illustrates that compared to the anonymity set size, the entropy is a suitable

[3]Average number of vehicles N in a lane of length L m, given vehicle average speed S m/sec and traffic volume V vehicles/hour/lane is: $N = \frac{VL}{3600S}$. For freeway model: $V = 3000$, $S = 30$m/sec, $L = 5000$m, gives $N \approx 139$, and for simplicity it is rounded to 150 vehicles/lane. For street model: $V = 1000$, $S = 15$m/sec, $L = 2000$m, gives $N \approx 37$, and is rounded to 50 vehicles/lane. Since each street has 2 lanes, $N = 100$ vehicles/street.

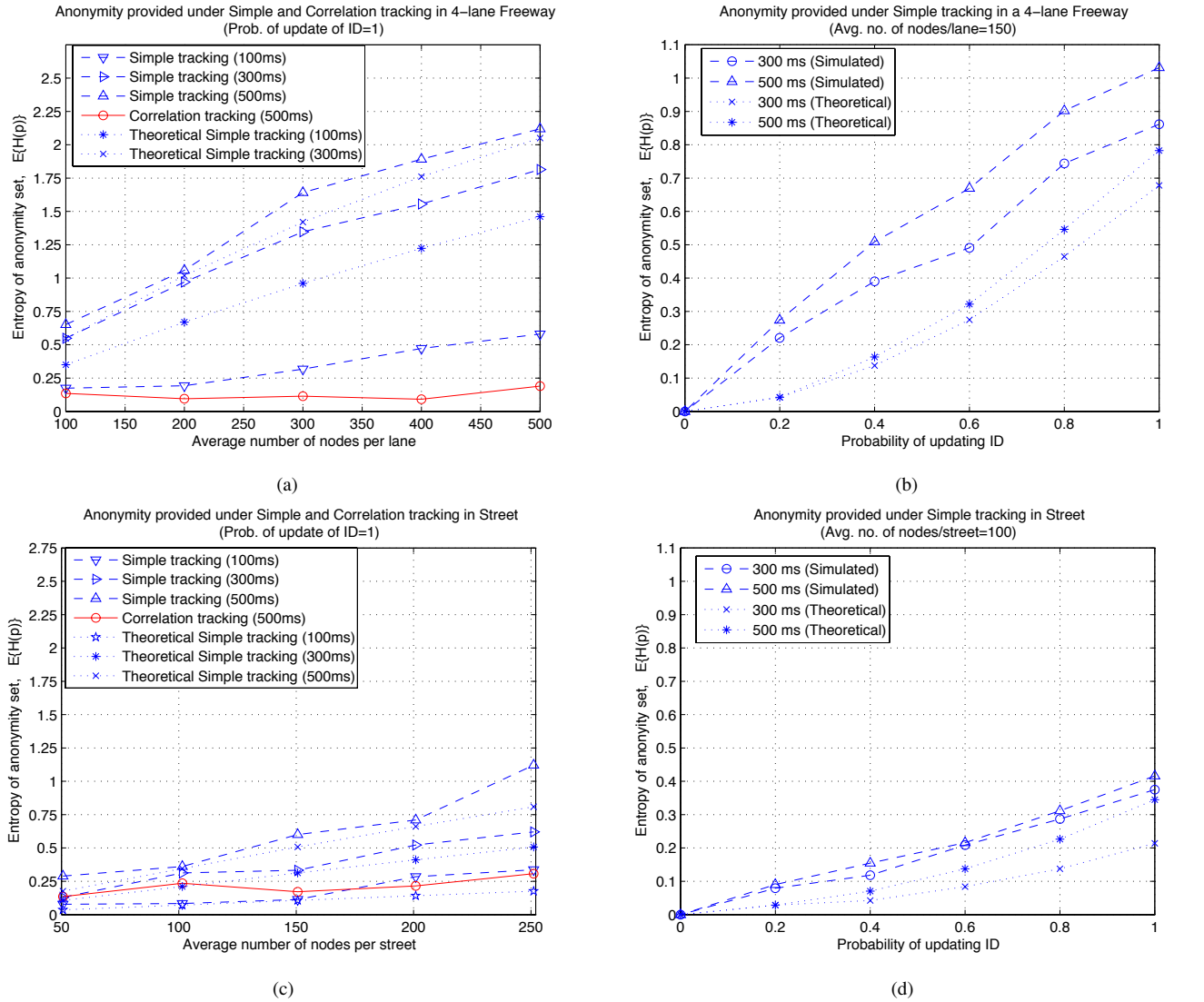


Fig. 8. Average anonymity provided to a target when it updates pseudonym, under tracking by GPA, with safety broadcast period being either 100 ms, 300 ms, or 500 ms: (a) 4-lane freeway with different number of vehicles (nodes) per lane. (b) 4-lane freeway with different probability of updating pseudonym. (c) street model with different number of vehicles per street. (d) street model with different probability of updating pseudonym.

metric to quantify anonymity level under the adversary model considered in our study. The anonymity set size is the same under simple and correlation tracking. However, entropy captures the non-uniform distribution assigned to the anonymity set by the adversary with additional available information from correlation tracking. Next, the alleviation of tracking by the proposed random silent period during a join is evaluated.

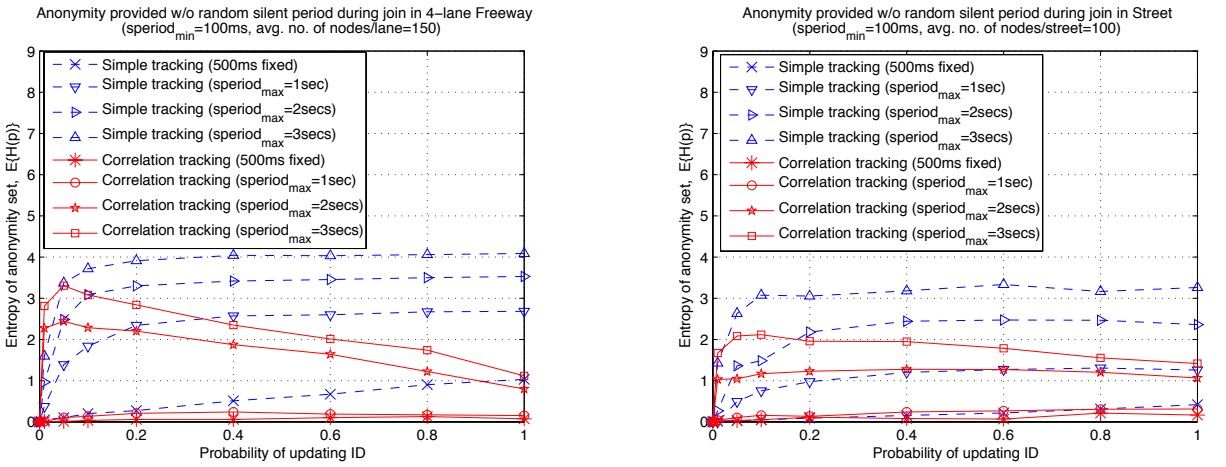
E. Location Privacy Enhancement with Silent Period

Fig. 9 shows the entropy that can be achieved under simple and correlation tracking by the GPA, when a vehicle joining the network remains silent for a random period between a minimum value of $speriod_{min} = 100$ ms and a maximum value of $speriod_{max}$. With an increase in $speriod_{max}$ from 1 sec to 3 secs, there is a significant increase in the anonymity level under simple tracking. But, in the case of correlation tracking a similar gain is not achieved. Fig. 9 and 10 show that the maximum silent period must be increased to at least 2 sec for an entropy of at least 1 bit under correlation tracking.

Fig. 9 also compares the entropy provided with and without using a random silent period when the vehicle broadcasts safety messages every 500 ms. For example, Fig. 9(a) shows that for 150 vehicles/lane in a 4-lane freeway, compared to a fixed broadcast period of 500 ms, the random silent period with $sp_{max} = 3$ secs provides a relative gain in entropy of approximately 100% to 300% under correlation tracking.

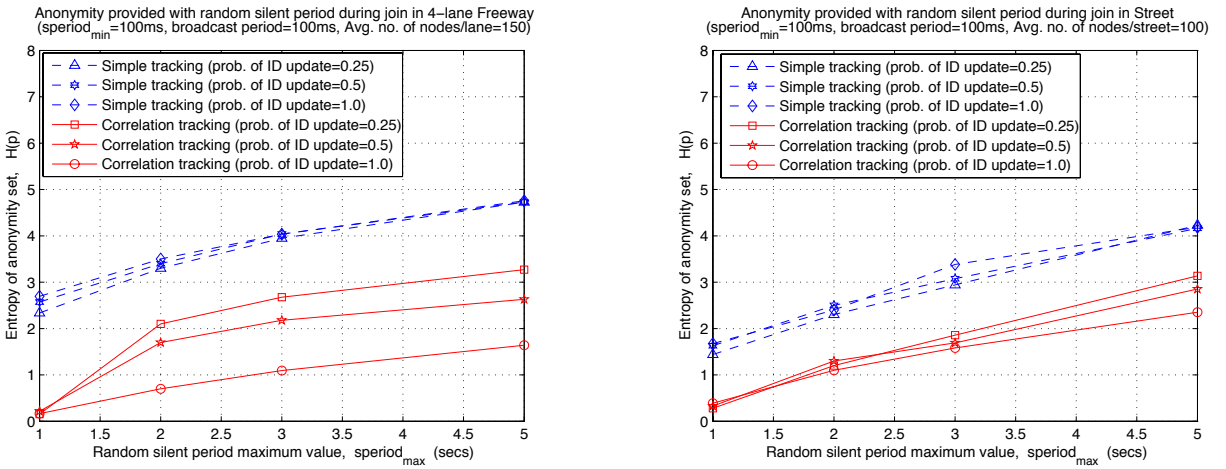
Interestingly, from Fig. 9, it can be observed that when the probability p_u increases, (i) the entropy under simple tracking for a given silent period increases only marginally, and (ii) the *entropy under correlation tracking decreases*. The reason for only a marginal increase in entropy under simple tracking is that with $p_u > 0$, if a vehicle updates two or more times in the reachable area, it is included only once in the anonymity set. As a result, the effect of increase in p_u on the anonymity set size is limited by the number of updating vehicles rather than the number of updates by each vehicle in a reachable area.

On the other hand, using correlation tracking, the adversary has a set of estimated positions in the reachable area, and for each position, the closest vehicle that updates pseudonym is chosen as a target candidate. Hence, if a vehicle A appears closest to an estimated position, and then updates pseudonym after every broadcast period (i.e. $p_u = 1$), it will most likely



(a) (b)

Fig. 9. Enhancement in anonymity obtained from tradeoff of the fixed safety message broadcast period of 500ms with random silent period during network join, under GPA. (a) 4-lane freeway. (b) street model.



(a) (b)

Fig. 10. Enhancement in anonymity obtained under simple and correlation tracking by GPA with different values for random silent period during network join. (a) 4-lane freeway. (b) street model.

be the closest to most of the subsequent estimated positions in the reachable area. This results in A having a high probability of being chosen as the target. Therefore, the anonymity set when $p_u = 1$ will have a lower entropy than when $p_u < 1$.

From the simulation study presented so far, it can be observed that for anonymity under correlation tracking the vehicles joining the network must remain silent for a random period greater than the fixed safety message broadcast period. This results in an increase in the spatial imprecision between two observed locations of the target compared to that achievable at 500 ms or lower values, and improves the entropy as seen in Fig. 9. However, when the broadcast period is 500 ms or less, this solution presents a tradeoff between anonymity and safety, since increasing the silent period can reduce the safety of the target's neighboring vehicles. For example, from Fig. 10(a), although a vehicle with $p_u = 0.5$ can be provided with an anonymity set with entropy of more than 1 bit, the vehicle and its neighbors may not broadcast for a maximum period of 2 secs. Next, we evaluate a solution that balances the tradeoff between safety/liability with location privacy.

F. Location Privacy under Restricted Passive Adversary

In order to model tracking by a RPA, we make use of an observation in [8] about the restricted coverage of RSUs because of their separation. This observation is illustrated in Fig. 11, where the RSU separation (RSU_{sep}) and the safety message broadcast range (r_0) define the geographical regions called *overheard* and *non-overheard* regions. As seen in Fig. 11, in the overheard region all safety message broadcasts are received by the RSU. However, the RSUs are unable to overhear safety message broadcasts in the non-overheard region. As described in Section II-A, since the RPA model leverages only on RSUs it can only track vehicles overheard by RSUs, i.e. only in the overheard regions.

Since vehicles can be assumed to be capable of controlling their transmission range, they can communicate with RSUs if needed in the non-overheard region. As shown in Fig. 11, the group leader vehicle increases its transmission power to reply to a probe request from RSU, i.e. we take into account that safety message broadcast range for vehicles can be smaller than broadcast range of other VANET applications.

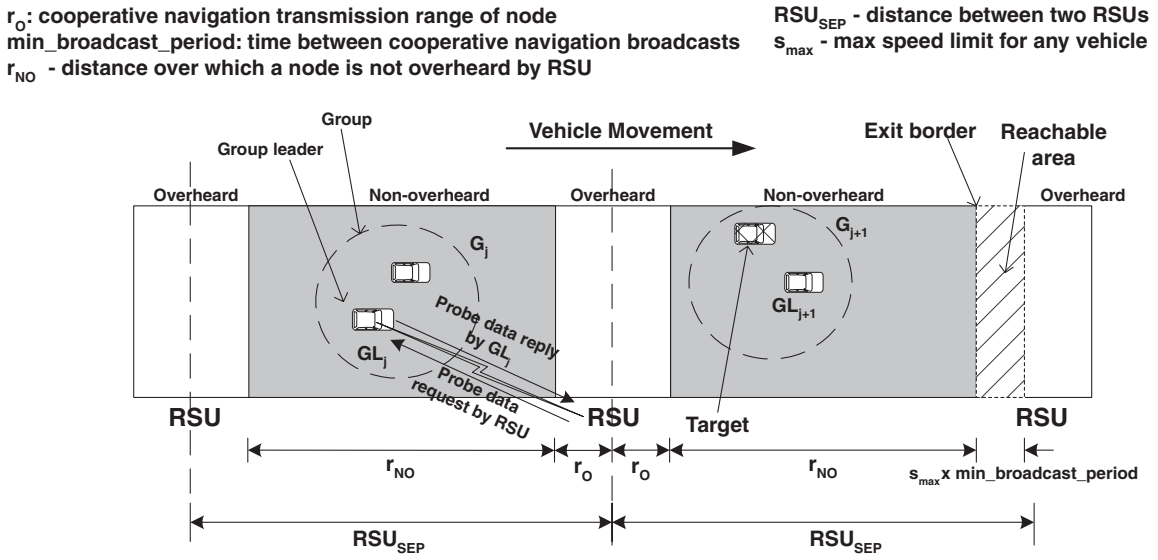


Fig. 11. Illustration of overheard and non-overheard regions in the path of vehicles, due to the separation between RSUs.

Given the above scenario, if the target vehicle updates its pseudonym in the non-overheard region and there is at least another vehicle in the non-overheard region that updates pseudonym, then the adversary may not be able to track the target when it exits the non-overheard region. The target anonymity set will include all the vehicles that update their pseudonym in the non-overheard region along with the target. Fig. 12 shows that an increase in RSU separation, increases the entropy of the target anonymity set distribution under simple tracking and correlation tracking.

G. Comparison of Silent Period with RSU Separation

Comparing the mitigation of tracking by silent period and by RSU separation, it is seen that the two are similar in approach. Both ensure a time period in which the target will move without being overheard, thereby increasing the spatial imprecision between two observed locations of the target. With RSU separation, a larger silent period is provided *without lowering safety*. The time that a vehicle remains in the non-overheard region while broadcasting safety messages, varies from $[(RSU_{sep} - 2r_0)/s_{max}, (RSU_{sep} - 2r_0)/s_{min}]$, where s_{min}, s_{max} are the minimum and maximum vehicle speeds, respectively. If the $RSU_{sep} = 1$ km, 2 km, the silent period range is $[10, 20]$ secs, $[35, 70]$ secs, respectively, for a freeway. As a result, an increase in RSU_{sep}, increases the time period of being not overheard, resulting in enhancement of anonymity as shown in Fig. 12. Further, Fig. 10 justifies this observation that anonymity is improved with increase in $speriod_{max}$.

Note that as shown in Fig. 11, with the known exit border of the non-overheard region, the reachable area is located only at the exit border, and fixed by s_{max} and the minimum safety broadcast period.[4] The anonymity set includes all vehicles that update in the reachable area over the time period

[4]Nevertheless, despite the reachable area being the same with increase in RSU_{sep}, the time period for which anonymity set is computed increases, resulting in increase in anonymity with RSU_{sep} under simple tracking.

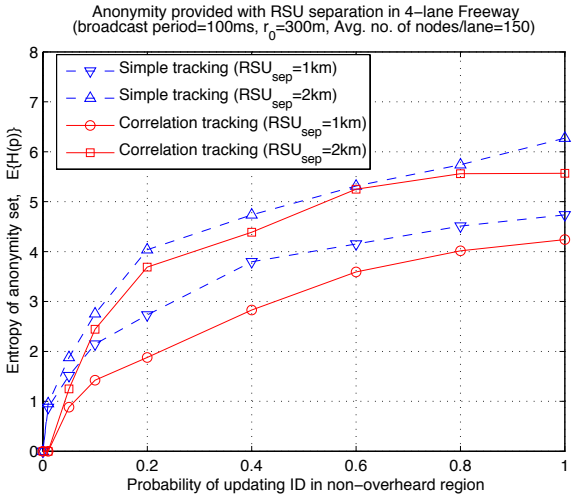


Fig. 12. Enhancement in anonymity obtained from RSU separation accounting for tracking by RPA.

$[(RSU_{sep} - 2r_0)/s_{max}, (RSU_{sep} - 2r_0)/s_{min}]$. Therefore, increase in probability of an ID update in the non-overheard region, increases the anonymity set size and hence the entropy under simple tracking. In correlation tracking, since there is a single estimated position in the reachable area, each vehicle in the anonymity set can appear close to this position at most once over the silent period range. This increases anonymity set size, i.e. the number of vehicles chosen as potential target candidates, and improves entropy.

VI. Related Work

A. VANET Security and Privacy

Only recently, the security and privacy issues in VANET have begun to attract attention from both academic and corporate research communities. In [5], [43], the various security and privacy challenges in vehicular networks are discussed. Hubaux et. al. from EPFL [6], [7] provide a general security framework to analyze the threats and challenges to security

and privacy in VANET. They propose several interesting solutions for VANET security such as *Electronic License Plates* (ELPs) that are unique cryptographically verifiable numbers equivalent to traditional vehicle license plates, and *location verification* based on verifiable multilateration for VANET liability. Dötzer et. al. from BMW research, have separately addressed privacy in VANET [9], and also security of V2I safety communications between vehicles and traffic light units [44]. In [8], Raya and Hubaux propose a scheme for providing anonymity to vehicle users in VANET, by enabling vehicles to update their keys only when changing direction. Most recent works on VANET security have studied the effect of changing pseudonyms on routing [46], and secure group formation [47]. However, none of the above works analyze the location privacy under tracking by a global passive adversary, nor study user privacy protection when vehicles access LBS applications.

In other related VANET security work, Golle et. al. [36] address the problem of an adversary injecting malicious data into the network, and propose a general approach to evaluate data validity, with each node searching for possible explanations for its collected data. ISO/TC204 [45] is responsible for the global standardization activity of ITS. The privacy issue in probe data application is a working issue in WG16 of ISO/TC204. However, in comparison with our work, they use a weaker adversary model by assuming that RSUs are trusted and not capable of location estimation, and take a policy-based approach to protect user privacy from service providers.

B. Mobility Models for VANET

Due to the emerging interest in VANET, there have been efforts to model the mobility of vehicles. Recognizing the restricted and dependent mobility of vehicles, Bai et al. in [24], propose two models – Freeway and Manhattan mobility models – for mobile ad hoc network simulation. Both of these models account for the spatial dependency between nodes and restricted movement of nodes in a freeway and a street map. We utilize slight variants of these models in our study, by incorporating additional parameters such as lane changing [40]. The study by Saha and Johnson in [48], accounts for restricted movement on real map data, and uses the current vehicle traffic conditions to determine the path of nodes to their respective destinations. However, they do not take into account the spatial dependency between the nodes. Very recently, the STRAW model was proposed by Choffnes and Bustamante in [40], that unlike [48], takes into account the spatial dependency between nodes, but does not incorporate lane changing. In [49], an overview of some existing vehicle traffic simulators is given.

C. Location Privacy Enhancement for Mobile Networks

To protect users from location privacy threats, there are several research studies in mobile networks. Gruteser et al. [16], [41] have worked extensively on protecting location privacy in WLAN, and utilize vehicular traffic data for evaluating their proposed solutions. In [16], the adversary is capable of accessing information only at the service provider. On the other hand, AMOEBA assumes the adversary is capable of estimating locations of vehicular communications, thus leading to a stronger adversary model than in [16]. Adversary's ability to estimate vehicular locations leads to a target uncertainty distribution that is different from uniform distribution. Entropy is a better measure to capture this varying target uncertainty. Hence, instead of using the anonymity set size as in [16], we use entropy to capture the different degrees of uncertainty.

In related research, Beresford and Stajano [50] propose the concept of the MIX zone based on the idea of Chaum's MIX [30], to protect location privacy of LBS application users from service providers. The MIX zone for a group of users is a connected geographical region where no application is accessible. Because application providers do not receive any location information when users are in a MIX zone, the user identities are *mixed*. However, the users can still be tracked in MIX zones due to spatial and temporal relation between locations of a mobile node [50]. This weakness is addressed in [15], [51], where Huang et. al. propose random silent period technique to protect wireless user trajectory privacy. However, they only evaluate the performance of the random silent period for the mitigation of tracking pedestrians in WLAN using a random node mobility model, i.e. under unrestricted and independent mobility of nodes.

VII. Conclusion and Future Work

In this paper, we addressed the location privacy threats that emerge in VANET due to unauthorized tracking of vehicles based on their broadcasts, as well as potential user privacy threats due to identification of LBS applications accessed from vehicle. We proposed a scheme, called *AMOEBA*, that provides location privacy by mitigating the location tracking of vehicles, and protects user privacy by providing vehicles with anonymous access to LBS applications.

By taking into account group navigation of vehicles, and VANET application features such as redundancy of probe vehicle data, we identified that by combining neighboring vehicles into groups, it is possible to provide an extended random silent period. We showed that in the presence of a global passive adversary, an extended silent period can alleviate tracking of vehicles in V2I applications such as probe vehicle data. However, for cooperative driving application, it was seen that mitigation of tracking required an increase in the safety message broadcast period, resulting in a possible lowering of safety. Nevertheless, under the safety message broadcast period constraint, we addressed location tracking by a restricted passive adversary, and showed that it is possible to successfully alleviate the location tracking by utilizing the separation between road side units, and the transmission power control capability of vehicles.

We leveraged the vehicular group to provide unlinkability between location of a LBS request broadcast and LBS application requested. The robustness of the resulting anonymous access to LBS applications was considered under various attacks by a global passive adversary. Further, the robustness of the proposed scheme, against active attacks on vehicle safety and liability was discussed.

As part of our future work, we intend to evaluate the proposed solutions by simulations based on the mobility of vehicles that will incorporate intersection behavior due to traffic

signs and the effects of congested streets, combined with map data and with communication traffic models. Furthermore, we intend to use formal modeling as a methodology to verify security properties of the proposed group protocols.

ACKNOWLEDGMENT

The authors are grateful for the feedback of the anonymous reviewers. This work was supported in part by NSF grant ANI-0093187-002, ARO PECASE grant W911NF-05-1-0491, ONR YIP grant N00014-04-1-0479, and Boeing. 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. Office of Naval Research, or the U.S. Government, or The Boeing Company.

APPENDIX A

Protocols for Group Formation, Group Join, Group Leave, Group Operation in AMOEBA

In the sections below, we detail the various protocols involved in the proposed location privacy scheme for VANETs.

1) Group Join Protocol: Each vehicle (node) i, upon entering the network, periodically broadcasts safety messages for cooperative navigation. Also, node i simultaneously attempts to join one of the nearest existing groups. The node i listens for broadcasts from any neighboring group leader GL_j, and then requests GL_j for membership to group G_j. A group leader can be identified by its address included in its broadcasts. The y least significant bits of the group leader's address will be set to zero (see Group Formation protocol). GL_j verifies (using the spatial parameters of i included in the request) if i is in the range of all members of G_j since full connectivity is assumed within groups for the group leader rotation to be possible. GL_j also verifies the public key of i included in the request, and then provides i with the group key k_{G_j} and the LBS application address range of the group, encrypted with public key of i. The pseudocode of the group join protocol is given below.

Group Join Protocol (GROUP_JOIN)

1. i: listen for broadcasts from neighboring group leaders $\mathcal{H}$
if ($|\mathcal{H}| > 0$) and *(waited for* $\leq sp_{max}$*)*
2. i: identify $G_j \in \mathcal{H}$ that was last heard
3. i: change $PID_{i,k-1}$ to $PID_{i,k} \in \{PID_i\}$
4. $i \rightarrow GL_j$:
$request = A_{GL_j}||PID_{i,k-1}||join\_request$
where $join\_request = K_{PID_{i,k-1}}||sign_{RA}(K_{PID_{i,k-1}})$
$||location_i||velocity_i||acceleration_i||timestamp$
5. *if (verified* $K_{PID_{i,k-1}}$*)* and *(*$location_i$ *is within range of node* a, $\forall a \in G_j$*)*
$GL_j \rightarrow i$: $reply = PID_{i,k-1}||A_{GL_j}$
$||E_{K_{PID_{i,k-1}}}(k_{G_j}||app\_address\_range)$
else
GL_j: do not reply
endif
6. *if (received reply within* T_{max}*)*
i: set address $A_{i,j} = PID_{i,k}$
i: go to GROUP_OPERATION after random time period $sp_{min} \leq sp \leq sp_{max}$
else
i: identify $G_k \in \mathcal{H} \backslash G_j$
i: set $G_j = G_k$,
if (less than R_{max} *repetitions without any reply)*
i: go to Step 4
else
i: go to GROUP_FORM
endif
endif
else
i: go to GROUP_FORM
endif

The above protocol addresses location privacy threats due to the Global Passive Adversary (GPA) and Restricted Passive Adversary (RPA), since they are not able to correlate the updated pseudonym $PID_{i,k}$ of the target i after the group join with the target pseudonym before joining. In particular, since $PID_{i,k}$ is independently determined by i (in Step 3), the GPA/RPA cannot obtain it by eavesdropping or by compromising a group member/leader (LAA). Upon joining the group G_j (in Step 6), i enters a random silent period sp before executing the group operation protocol to mitigate correlation by GPA/RPA of its new location associated with $PID_{i,k-1}$ with its previous location associated with $PID_{i,k}$.

2) Group Formation Protocol: In the above protocol, the node i may not be successful in finding a group to join. The node then creates a group by means of the group formation protocol. i communicates with the RA via the RSU to obtain the group leader ID, GID_j, used in the group leader address A_{GL_j}. This interaction is needed to avoid collision of the group leader addresses, since, y least significant bits of the address are set to be zero, i.e. $A_{GL_j} = GID_j||0^y$. Similarly, collisions in the address range provided for LBS application access is avoided. The pseudocode for the protocol is below.

Group Formation Protocol (GROUP_FORM)

if (no group heard in GROUP_JOIN*)* or *(no group leader replied in* GROUP_JOIN*)*
1. i: choose $PID_{i,k} \in \{PID_i\}$
2. $i \rightarrow RSU$: $leader\_notification = A_{broadcast}||PID_{i,k}||K_{PID_{i,k}}||sign_i(K_{PID_{i,k}})$
3. RSU, RA: verify $K_{PID_{i,k}}$, and generate:
$E_{K_{PID_{i,k}}}(GID_j||address\_range||$
$sign_{RA}(GID_j||address\_range||timestamp))$
4. $RSU \rightarrow i$: broadcast $reply = PID_{i,k}||A_{RSU}||$
$E_{K_{PID_{i,k}}}(GID_j||address\_range||$
$sign_{RA}(GID_j||address\_range||timestamp))$
5. i: *if (received RSU reply within duration* T_{max}*)*
i: generate $A_{GL_j} = GID_j||0^y$
i: go to GROUP_OPERATION after random time period $sp_{min} \leq sp \leq sp_{max}$,
listen for join_request
i: *if (no* GROUP_JOIN *request)* and *(waited for duration* W_{max}*)*
i: go to GROUP_JOIN

else
if (number of repetitions of broadcast $< R_{max}$*)*
i: repeat Step 2
else
i: go to GROUP_JOIN
endif
endif
endif

The protocol addresses location privacy and user privacy threats. The $address\_range$ in Step 3 is used to provide the random address A_{aa} for the anonymous access to LBS applications. We note that the $address\_range$ can directly generate A_{aa}, or alternatively, it can be used to obtain random y-bit numbers $xx...x$, that can construct the random address $A_{aa} = GID_j||xx...x$. Since the random address and group key are self generated by i, and the message from RA to RSU to i containing address range/new pseudonym is encrypted with the public key of i (Steps 3, 4), the GPA/RPA are not able to obtain these quantities for tracing i. Further, since the trusted RA signs and timestamps the message containing the new pseudonym and $address\_range$ (in Step 3), the protocol is secure even in the presence of a compromised RSU.

3) Group Leaving Protocol: The nodes in a VANET are highly mobile, and often a node may accelerate or change direction with time. Consequently, a node can go out of range of the group, thereby leaving its current group and joining another group near its new location. On the other hand, a node may update its pseudonym/address $A_{i,j}$. In either case, the leader GL_j of i's current group, must assume that i has left G_j. Therefore in the group leaving protocol, when GL_j does not receive any safety message broadcast with pseudonym of i (recorded when joining the group) for a maximum time D_{max}, GL_j assumes that either i has left the group or has updated its pseudonym/address $A_{i,j}$. Since in *cooperative navigation*, the nodes periodically broadcast navigational data with period T_n, the leader can set the period D_{max} to be a multiple of T_n. Node i will self determine if it is out of range of GL_j, and try to find a new group by executing the group join protocol. The pseudocode for **group leave protocol** is below.

Group Leaving Protocol (GROUP_LEAVE)

---

1. i: compute current distance from group leader GL_j
2. i: *if (going to be out of range from* GL_j *at* $leave\_time$*)*
i: go to GROUP_JOIN
endif
3. GL_j: *if (no broadcast is received from* i *for duration* D_{max}*)*
GL_j: delete entry of $A_{i,j}$ from current group member list
endif

Since there is no explicit communication, the protocol does not disclose any information to threaten privacy.

4) Group Operation Protocol: All the members of the group G_j participate in the group operation protocol, which consists of several subprotocols. The *cooperative navigation protocol* is used for safety enhancement. For the probe data application, we include an optional *probe data aggregation protocol*, where the leader aggregates data received from the members. The aggregated data is included in the reply from the leader to the RSU probe request in *probe data collection protocol*. As discussed in Section IV-A, the leader node cannot be provided location privacy, since it can be tracked based on its fixed pseudonym/address A_{GL_j}. Hence, periodically the role of leader is shared by the group members. This is implemented by the *leader rotation protocol*. The pseudocode for the **group operation protocol** is given below, followed by the various subprotocols.

Group Operation Protocol (GROUP_OPERATION)

---

1. G_j: go to COOPERATIVE_NAVIGATION
2. *for all* $i \in G_j \backslash GL_j$
i: listen to broadcast sent by GL_j and go to GROUP_LEAVE
endfor
3. G_j: optionally go to PROBE_DATA_AGGREGATION
4. GL_j: go to PROBE_DATA_COLLECTION
5. *if (leader rotation is needed)*
G_j: go to LEADER_ROTATION
else
GL_j: go to Step 3.
endif

In the **probe data aggregation protocol**, only a fraction of p nodes from G_j can broadcast data in each period T_d. The pseudocode for the probe data aggregation between the members of G_j is as follows. The function $aggregate\_data$ is a suitable spatial data aggregation algorithm, not given here since it is out of the scope of this paper.

Probe Data Aggregation (PROBE_DATA_AGGREGATION)

---

1. *for all* $i \in G_j \backslash GL_j$
$i \rightarrow GL_j$: $PDATA_i = A_{GL_j}||A_{i,j}||location_i||probe\_data_i$ with probability p
GL_j: record $PDATA_i$
endfor
2. GL_j: execute $aggregate\_data$ to perform aggregation of all the received $\{PDATA_a\}$ and $PDATA_{GL_j}$, and finally obtain $AGGREGATED\_DATA$
3. G_j: go to Step 1 every T_d

The GPA/RPA can eavesdrop the message from i in Step 1. However, since i broadcasts only with probability p, it is equivalent to using a maximum silent period of $|G_j|p$, assuming the group size remains static. Hence, with the use of random silent period in the protocol, the location tracking based on eavesdropped messages in Step 1 by GPA/RPA is mitigated. Next, the pseudocode for the **probe data collection protocol** is given below.

Probe Data Collection (PROBE_DATA_COLLECTION)

1. $RSU \rightarrow GL_j$: $probe\_data\_request = A_{broadcast}||A_{RSU}||request\_message$
2. GL_j: *if (no* $AGGREGATED\_DATA$*)*
   $data = location_{GL_j}||probe\_data_{GL_j}$
   else
   $data = location_{GL_j}||AGGREGATED\_DATA$
   endif
3. $GL_j \rightarrow RSU$: $reply = A_{RSU}||A_{GL_j}||data$

In Step 2, the leader checks for any data that was aggregated recently. If not, it broadcasts self-generated probe data. We do not detail the $probe\_data$ format here. Note that the $probe\_data\_request$ can specify data resolution, i.e. for high resolution aggregated data or for lower resolution self-generated data from the leader. The GPA/RPA can track the leader based on GL_j in the message in Step 3, until the next execution of leader rotation protocol.

In the **cooperative navigation protocol**, each node independently and periodically broadcasts a safety message every T_n. In order to ensure liability of the message originator and safety of the message receiver, we make each node to sign its safety message and include a timestamp to ensure message freshness. To enable verification, the node includes the public key certificate.

Cooperative Navigation (COOPERATIVE_NAVIGATION)

1. i: $NDATA_{i,j} = A_{broadcast}||A_{i,j}||$
   $sign_i(navigation\_data_i||timestamp)||sign_{RA}(K_{PID_{i,k}})$
2. *for all received* $NDATA_{a,x}$
   i: validate and store $NDATA_{a,x}$
   endfor
3. i: execute $safety\_computation$ using valid $\{NDATA_{a,x}\}$
4. *if (received* $intersection\_RSU$ *broadcast* $= A_{broadcast}||A_{IRSU}||location_{IRSU}$*)*
   i: *if (less than two replies heard)*
   $i \rightarrow intersection\_RSU$: $A_{IRSU}||A_{i,j}||navigation\_data_i$
   endif
5. i: go to step 1 every T_n.

The data format can be $navigation\_data_i = (location_i, speed_i, acceleration_i, direction_i, timestamp_i)$. In Steps 1-3, navigational data is communicated between vehicles. Step 3 is only illustrative of the use of navigational data for safety computation. There may be other applications for such data, not included here. The safety computation algorithm using navigational data of neighboring vehicles is out of the scope of this paper. Note that the GPA/RPA can use the safety message in Step 1 to estimate and locate i. However, the LAA is prevented from attacking safety or liability of i since Step 2 validates each received safety broadcast by verifying the signature contained in it, before taking them into account in the safety computation.

Step 4 is used to achieve *intersection vehicle collision avoidance* between two groups. To avoid redundancy, not all nodes in G_j need to communicate. However, due to critical nature of the collision avoidance problem, protocol reliability and vehicle safety must be ensured. Hence, two or more nodes from G_j must communicate with the intersection RSU. If we assume that the vehicle transmission range is smaller than the RSU range, the two or more nodes replying in Step 4 will be in proximity of the intersection RSU. Note that by reducing the number of broadcasts overheard by the GPA/RPA, Step 4 also protects location privacy.

As mentioned earlier, in order to provide location privacy for the group leader, it becomes essential to rotate the group leader role (periodically or on demand) among the group members. The following protocol is used to enable the **rotation of the group leader** role in the group G_j.

Group Leader Rotation (LEADER_ROTATION)

1. GL_j: *if (do not want to be group leader) or (end of rotation period)*
   $GL_j \rightarrow G_j$: $notification = A_{broadcast}||A_{GL_j}||$
   $E_{k_{G_j}}\{rotation\_time||leader\_rotation\_notification\}$
2. *forall* $i \in G_j \backslash GL_j$
   i: wait for random time $sp \leq sp_{max}$
   i: mask y least significant bits of $PID_{i,k+1}$, and set the masked $PID_{i,k+1}$ as $A_{GL_{j_{new}}} = GID_{j_{new}}$
   $i \rightarrow G_j$: $reply = A_{broadcast}||A_{i,j}||$
   $E_{k_{G_j}}\{leader\_role\_accept||A_{GL_{j_{new}}}\}$
   endfor
3. *if* (GL_j *receives the reply from two or more nodes in* G_j*)*
   GL_j: choose random node i from the nodes that replied
   $GL_j \rightarrow G_j$: $A_{broadcast}||A_{GL_j}||$
   $E_{k_{G_j}}\{leader\_role\_granted||A_{i,j}\}$
   else
   if (no reply is received within T_{max}*)*
   GL_j: go to Step 1
   endif
   endif
4. i: broadcast $leader\_notification = A_{broadcast}||A_{GL_{j_{new}}}||PID_{i,k+1}$
5. RSU: verify $leader\_notification$
6. $RSU \rightarrow i$: broadcast ACK if verified to be correct
7. i: *if (not received RSU* ACK *after waiting for* T_{max}*)*
   i: repeat the broadcast in Step 4
   else
   i: $A_{broadcast}||A_{GL_j}||E_{k_{G_j}}\{k_{G_{j_{new}}}||app\_address\_range\}$
   G_j: generation of group seed $S_{G_{j_{new}}}$
   endif

The protocol defends attacks by the LAA that can bias the group leader election. Steps 2-3 are used to implement the random election of the new leader to prevent the LAA from effecting a deterministic election in the group. As discussed in Section IV-A.4, to prevent collusion between the old and new leader vehicles, we can additionally incorporate a robust randomized election protocol in Steps 2-3. This ensures

the election of the new leader is truly random. Further, to prevent a compromised leader or a collusion between two or more members (less than a majority) from corrupting the new group seed ensuring random mixing of LBS requests, in Step 7 the group seed is generated as discussed in Section IV-A.1, i.e. by means of a distributed protocol in G_j such as in [32]. We note that the GPA possessing k_{G_j} can obtain the new group secrets $k_{G_{jnew}}$ and $S_{G_{jnew}}$ in Step 7. Hence, the generation of new group secrets defends only attacks by a collusion between RPA and LAA, and not by the GPA.

APPENDIX B

Protocol for Anonymous Access to LBS Application

Fig. 5 shows a node i in G_j accessing a LBS from service provider SP_x, and illustrates the protocol steps.

Anonymous Access Protocol (ANONYMOUS_ACCESS)

1. $i \rightarrow GL_j$: $app\_request\_message = A_{GL_j}||A_{aa}||E_{k_{G_j}}\{APP\_REQ\}$
   where $APP\_REQ = app_x\_request||E_{K_{RA}}(PID_{i,k}||sign_i(PID_{i,k})||h^n(q_i)||app_x)$
2. $GL_j \rightarrow RSU$: $forward\_message = A_{RSU}||A_{GL_j}||location_{GL_j}||APP\_REQ$
3. $RSU \rightarrow RA$: forward APP_REQ
4. RA: *if (app_x_request is valid)*
   compute $MSG = D_{K_{RA}}(E_{K_{RA}}(PID_{i,k}||sign_i(PID_{i,k})||h^n(q_i)||app_x))$
   else
   generate $reply = DENY\_REQ$
   endif
   if (app_x_request is for app_x) and *($PID_{i,k}$ in MSG is valid)* and *($PID_{i,k}$ has valid access to app_x)* and *($sign_i(PID_{i,k})||h^n(q_i)$ in MSG is valid)*
   generate $reply = app_x||E_{K_{SP_x}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp))||E_{K_{PID_{i,k}}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp))$
   else
   generate $reply = DENY\_REQ$
   endif
   $RA \rightarrow RSU$: $reply$
5. RSU: *if ($reply == DENY\_REQ$)*
   go to Step 15
   else
   $RSU \rightarrow SP_x$: send $app\_initiate = location_{GL_j}||E_{K_{SP_x}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp))$
   endif
6. SP_x: *if (received app_initiate from RSU)* and *(able to provide service)*
   compute $D_{K_{SP_x}}(E_{K_{SP_x}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp)))$
   if ($k_{x,i}$ is valid) and *(timestamp is not expired)*
   $SP_x \rightarrow RSU$: send $app\_initiate\_response$
   endif
   endif /* $app\_initiate\_response$ is also used to indicate the availability of the SP_x */
7. RSU: *if (received $app\_initiate\_response$ within T_{max1})*
   $RSU \rightarrow GL_j$: send $RSU\_response = A_{GL_j}||A_{RSU}||app_x||E_{K_{PID_{i,k}}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp))$
   else go to Step 15
   endif
8. GL_j: *if (received $RSU\_response$ within T_{max2})*
   $GL_j \rightarrow i$: $app_x||E_{K_{PID_{i,k}}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp))$
   else go to Step 15
   endif
9. *for all i in G_j*
   if (requested for app_x access)
   i: compute $decrypt = D_{K_{PID_{i,k}}}(E_{K_{PID_{i,k}}}(k_{x,i}||sign_{RA}(k_{x,i}, timestamp)))$
   i: *if (successfully obtained decrypt)*
   if ($k_{x,i}$ is valid) and *(timestamp is not expired)*
   i: go to Step 10
   else go to Step 15
   endif
   else
   i: ignore the broadcast from GL_j
   endif
   endif
   endfor
10. *while (1)* /* two-way communication session between node and SP */
   if (data to be sent to i)
   $SP_x \rightarrow RSU$: $E_{k_{x,i}}\{data\}$
   $RSU \rightarrow GL_j$: $A_{GL_j}||A_{RSU}||E_{k_{x,i}}\{data\}$
   $GL_j \rightarrow i$: $E_{k_{x,i}}\{data\}$
   i: decrypt data as $D_{k_{x,i}}\{E_{k_{x,i}}\{data\}\}$
   endif
   i: *if (no data received for T_{max3})* and *(no data to be sent to SP_x)*
   go to Step 11
   else
   if (data to be sent to SP_x)
   $i \rightarrow GL_j$: $A_{GL_j}||A_{aa}||E_{k_{G_j}}\{app_x||E_{k_{x,i}}\{data\}\}$
   $GL_j \rightarrow RSU$: $A_{RSU}||A_{GL_j}||location_{GL_j}||app_x||E_{k_{x,i}}\{data\}$
   $RSU \rightarrow SP_x$: $location_{GL_j}||E_{k_{x,i}}\{data\}$
   SP_x: decrypt $D_{k_{x,i}}\{E_{k_{x,i}}\{data\}\}$
   endif
   endif
   endwhile
11. $i \rightarrow GL_j$: $A_{GL_j}||A_{aa}||E_{k_{G_j}}\{APP\_FIN\}$
   where $APP\_FIN = app_x\_end||E_{K_{RA}}(PID_{i,k}||app_x||k_{x,i}||sign_i(session\_info||timestamp))$
   $GL_j \rightarrow RSU$: $A_{RSU}||A_{GL_j}||location_{GL_j}||APP\_FIN$
   $RSU \rightarrow RA$: forward APP_FIN
12. $SP_x \rightarrow RSU \rightarrow RA$: $SERVICE\_FIN = E_{K_{RA}}(SP_x||app_x||k_{x,i}||sign_{SP_x}(session\_info||timestamp))$
13. RA: *if (received APP_FIN)* and *(received $SERVICE\_FIN$)*
   RA: $D_{K_{RA}}(E_{K_{RA}}(PID_{i,k}||app_x||k_{x,i}||sign_i(session\_info||timestamp)))$
   RA: $D_{K_{RA}}(E_{K_{RA}}(SP_x||app_x$

$||k_{x,i}||sign_{SP_x}(session\_info||timestamp)))$

if (decrypted quantities are valid for session between i *and* SP_x*)* and *(*$session\_info$ *in both signatures match)*

RA: record the decrypted quantities
go to Step 15
else go to Step 14
endif

else

if (waited for T_{max4}*)* and *(not received* APP_FIN*)* and *(not received* $SERVICE\_FIN$*)*
go to Step 15
else go to Step 14
endif

endif

14. RA, *location server*, i, SP_x: resolve dispute between i and SP_x
15. i, SP_x, GL_j, RSU: terminate session

The protocol addresses location privacy threats by the GPA/RPA. The leader GL_j as a proxy provides unlinkability between i and app_x (and SP_x). Since in Step 1, i encrypts $PID_{i,k}$, the GPA/RPA can traceback only to the group G_j of i and the location of GL_j. The protocol also addresses attacks by the LAA on user privacy in Section IV-A.

Additionally, the protocol satisfies following security properties to counter other security threats to the LBS user and the service provider from LAA as discussed below. The protocol provides confidentiality. In Step 10, the use of session key $k_{x,i}$ enables restricted and authorized access to LBS. However, if the application is unrestricted and free then the use of the session key is not needed. The protocol provides authenticated and authorized access to the LBS. Only members of the mobile group G_j possess the group key k_{G_j}, and only an authentic member of G_j can access LBS via GL_j in Step 1. The Lamport's hash chain and signature in the LBS request is verified in Step 4 by the RA, ensuring authenticity of the request and of $PID_{i,k}$, respectively. Also, in Step 4 the RA includes signature and timestamp in the public key encryptions, to ensure that SP_x (in Step 6) and i (in Step 9) are guaranteed the authenticity of the encrypted session key received from an untrusted RSU. Finally, in Step 4, a predetermined list at the RA, containing the applications each pseudonym is authorized to access is used to authorize i.

The protocol provides non-repudiation in application access. Since the location server is the interface for the service providers, it maintains a transcript of the entire session between i and SP_x. The session can contain one or more transactions between i and SP_x. If i denies receiving a transaction or SP_x claims completing a transaction, then the trusted RA must resolve the dispute (in Step 14). The transaction details are obtained from both parties, and these details (e.g. transaction time) are cross checked with the location server transcript to identify the cheating entity. Note that even during dispute resolution, the identity of i is not revealed to SP_x. Therefore, the anonymity of i is preserved even if SP_x creates a dispute with the intention of breaching privacy of i.

REFERENCES

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

[2] Car-2-Car Communication Consortium. [Online]. Available: http://www.car-2-car.org/

[3] ITS America. [Online]. Available: http://www.itsa.org/

[4] J. Singh, N. Bambos, B. Srinivasan, and D. Clawin, "Wireless LAN performance under varied stress conditions in vehicular traffic scenarios," in *Proc. of the IEEE Vehicular Technology Conference (VTC 2002-Fall)*, September 2002, pp. 743–747.

[5] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *Proc. of the European Wireless Workshop*, February 2002.

[6] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[7] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *Proc. of Swiss Transport Research Conference*, March 2005.

[8] ——, "The security of vehicular ad hoc neworks," in *Proc. of the ACM Workshop on Security of Ad hoc and Sensor Networks (SASN)*, pp. 11–21, November 2005, pp. 11–21.

[9] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Proc. of the Workshop on Privacy Enhancing Technologies (PET)*, June 2005, pp. 197–209.

[10] T. S. Rappaport, J. H. Reed, and B. D. Woerner, "Position location using wireless communications on highways of the future," *IEEE Communications Magazine*, vol. 10, no. 1, pp. 33–41, October 1996.

[11] Y. Zhao, "Mobile phone location determination and its impact on intelligent transportation systems," *IEEE Trans. on Intelligent Transportation Systems*, vol. 1, no. 1, pp. 55–64, March 2000.

[12] C. Komar, and C. Ersoy, "Location Tracking and Location Based Service Using IEEE 802.11 WLAN Infrastructure," in *Proc. of the European Wireless Workshop*, February 2004.

[13] R. Singh, M. Guainazzo, and C. S. Regazzoni, "Location determination using WLAN in conjunction with GPS network," in *Proc. of the Vehicular Technology Conference (VTC-Spring)*, May 2004, pp. 2695–2699.

[14] A. Pfitzmann and M. Waidner, "Networks without user observability – design options," in *Advances in Cryptology – EUROCRYPT'85*. Springer-Verlag, LNCS 219, 1985, pp. 245–253.

[15] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC)*, March 2005, pp. 1187–1192.

[16] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of the ACM International Conference on Mobile Systems MobiSys*, May 2003, pp. 31–42.

[17] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proc. of the Workshop on Privacy Enhancing Technologies (PET)*, April 2002, pp. 41–53.

[18] K. A. Remley, C. A. Grosvenor, R. T. Johnk, D. R. Novotny, P. D. Hale, M. D. McKinley, A. Karygiannis, and E. Antonakakis," Electromagnetic signatures of WLAN cards and network security,"in *Proc. of the Fifth IEEE International Symposium on Signal Processing and Information Technology*, December 2005, pp. 484- 488.

[19] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D. Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," in *Proc. of the 15th Usenix Security Symposium*, August 2006, pp. 167–178.

[20] S. Kato, S. Tsugawa, K. Tokuda, T. Matsui, and H. Fujii, "Vehicle control algorithms for cooperative driving with automated vehicles and intervehicle communications," *IEEE Trans. on Intelligent Transportation Systems*, vol. 3, no. 3, pp. 155–161, September 2002.

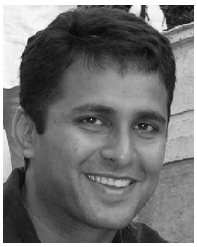
[21] R. Hochnadel and M. Gaeta, "A look ahead network (LANET) model for vehicle-to-vehicle communications using DSRC," in *Proc. of World Congress on Intelligent Transportation Systems*, November 2003.

[22] ITS probe vehicle techniques. [Online]. Available: http://tti.tamu.edu/documents/FHWA-PL-98-035_c5.pdf

[23] T. Fushiki, T. Yokota, K. Kimita, M. Kumagai, and I. Oda, "Study on density of probe cars sufficient for both level of area coverage and traffic information update cycle," in *Proc. of World Congress on Intelligent Transportation Systems*, October 2004.

[24] 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 the IEEE INFOCOM*, March 2003, pp. 825–835.

[25] R. W. Rothery, "Car following models," in *In N.H. Gartner, C. Messer, and A.K. Rathi, editors, Traffic Flow Theory, Chapter 4*., 2002.
[26] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-centric approaches towards maximizing location privacy," in *Proc. of the ACM Workshop on Privacy in Electronic Society (WPES)*, October 2006, pp. 19–28.
[27] Analysis of older drivers on freeways. [Online]. Available: http://www.hsisinfo.org/pdf/oldriver.htm
[28] Y. Iwasaki, "Japan's policies on research and development of the advanced cruise-assist system," in *Proc. of ITS World Congress*, 1999.
[29] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology - EUROCRYPT'01*, ser. LNCS, vol. 2045. Springer, 2001, pp. 93–118.
[30] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.
[31] M. Jakobsson, A. Juels, and R. L. Rivest, "Making mix nets robust for electronic voting by randomized partial checking," in *Proc. of the USENIX Security Symposium*, February 2002, pp. 339–353.
[32] A. Russell and D. Zuckerman, "Perfect information leader election in log* n + O(1) rounds," in *Proc. of the 39th Annual Symposium on Foundations Of Computer Science (FOCS)*, November 1998, pp. 576–583.
[33] A. Serjantov, R. Dingledine, and P. Syverson, "From a trickle to a flood: Active attacks on several mix types," in *Proc. of the International Workshop on Information Hiding (IH)*. Springer-Verlag, LNCS 2578, October 2002, pp. 36–52.
[34] A. Serjantov and R. E. Newman, "On the anonymity of timed pool mixes," in *Proc. of the Workshop on Privacy and Anonymity Issues in Networked and Distributed Systems*, May 2003, pp. 427–434.
[35] K. Sampigethaya and R. Poovendran, "A survey on mix networks and their secure applications," *Proceedings of the IEEE*, vol. 94, no. 12, pp. 2142–2181, December 2006.
[36] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. of the ACM Workshop on Vehicular Ad hoc Networks (VANET)*, 2004, pp. 29–37.
[37] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, pp. 65–75, 1988.
[38] I. Seskar, S. Maric, J. Holtzman, and J. Wasserman, "Rate of location area updates in cellular systems," in *Proc. of the IEEE Vehicular Technology Conference*, May 1992, pp. 694–697.
[39] A. M. Mathai, *An Introduction to Geometrical Probability: Distributional Aspects with Applications*. CRC Press, 1999.
[40] D. R. Choffnes and F. E. Bustamante, "An integrated mobility and traffic model for vehicular wireless networks," in *Proc. of the ACM Workshop on Vehicular Ad hoc Networks (VANET)*, September 2005, pp. 69–78.
[41] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," in *Proc. of the ACM Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH)*, September 2003, pp. 46–55.
[42] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *Proc. of the Workshop on Embedded Security in Cars (ESCAR)*, 2005.
[43] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang, "Framework for security and privacy in automotive telematics," in *Proc. of the 2nd International Workshop on Mobile Commerce (WMC)*, September 2002, pp. 25–32.
[44] F. Dötzer, F. Kohlmayer, T. Kosch, and M. Strassberger, "Secure communication for intersection assistance," in *Proc. of the International Workshop on Intelligent Transportation (WIT)*, March 2005.
[45] ISO/TC204:transport information and control systems (TICS). [Online]. Available: http://www.sae.org/technicalcommittees/tc204.htm
[46] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, "Impact of Pseudonym Changes on Geographic Routing in VANETs," in *Proc. of the European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, October 2006, pp. 43–57.
[47] M. Raya and A. Aziz and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. of the 3rd international workshop on Vehicular Ad hoc Networks (VANET)*, 2006, pp. 67–75.
[48] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad hoc networks," in *Proc. of the ACM Workshop on Vehicular Ad hoc Networks (VANET)*, October 2004, pp. 91–92.
[49] C. Schroth, F. Dötzer, T. Kosch, B. Ostermaier, and M. Strassberger, "Simulating the traffic effects of vehicle-to-vehicle messaging systems," in *Proc. of the International Conference on ITS Telecommunications*, June 2005.
[50] A. R. Beresford, "Location privacy in ubiquitous computing," Ph.D. dissertation, University of Cambridge, November 2004.
[51] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Towards modeling wireless location privacy," in *Proc. of the Workshop on Privacy Enhancing Technologies (PET)*, June 2005, pp. 59–77.
[52] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management A Consolidated Proposal for Terminology," version v0.25, December 2005.
[53] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when dislosing information," in *Proc. of the ACM Symposium on Principles of Database Systems (PODS)*, June 1998, pp. 188.
[54] European Union. Data protection directive (95/46/ec). Official Journal of the European Communities, L. 281:31, November 1995. [Online]. Available: http://www.cdt.org/privacy/eudirective/EU_Directive_.html.
[55] G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications, *IEEE Pervasive Computing*, 2(1):56–64, March 2003.



Krishna Sampigethaya is a PhD candidate in the Department of Electrical Engineering, and a graduate research assistant in the Network Security Lab (NSL) at the University of Washington. He is conducting research on secure electronic voting and location privacy in vehicular networks. He has also conducted research on airplane security in Math and Computing Division of Boeing Phantom Works, Seattle. He is expecting to complete his PhD in Summer 2007.

Mingyan Li is a advanced computing technologist at Boeing Phantom Works and an affiliate assistant professor in the Electrical Engineering Department at the University of Washington (UW). She received her PhD from Network Security Lab at UW in 2006. Her research interests include security and privacy in multi-user environments, sensor networks and RFID systems. She is leading Boeing-UW-Siemens collaboration on wireless and RFID security. She is a recipient of the 2006 UWEE Chair's Award and the 2003 Society of Women Engineers Graduate award.

Leping Huang is a member of research staff at Nokia Research Center and a visiting researcher at Center for Spatial Information Science of the University of Tokyo. He received his PhD from the University of Tokyo in 2006. His research interests include location privacy, mobility, security and radio resource management in next generation radio systems. He is currently working as a Nokia delegate in 3GPP Radio Access Networks (RAN) working group on next generation cellular system (3.9G) standardization.

Radha Poovendran is an Associate Professor and founding director of the Network Security Lab (NSL) at the Electrical Engineering Department of the University of Washington. He received his Ph.D. in Electrical Engineering from the University of Maryland, College Park in 1999. His research interests are in the areas of applied cryptography for multiuser environment, wireless networking, and applications of Information Theory to security. He is a recipient of the NSA Rising Star Award and Faculty Early Career Awards including NSF CAREER (2001), ARO YIP (2002), ONR YIP (2004), and PECASE (2005) for his research contributions to multiuser security, the Graduate Mentor Recognition Award from the University of California San Diego in 2006, and is invited to the Kavli Frontiers of Science Symposium organized by the National Academy of Sciences in 2007. He is a co-editor of the Springer Verlag book "Secure localization and time synchronization in wireless ad hoc and sensor networks."