Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.9 No.2, 2020, pp.28-44

DOI: https://doi.org/10.51983/ajcst-2020.9.2.2170

Enhancing Location Privacy for Vehicular Ad Hoc Networks

Hesiri Weerasinghe [1] and Huirong Fu [2]
[1] Department of Computer Systems Engineering, Faculty of Computing and Technology,
University of Kelaniya, Sri Lanka
[2]Department of Computer Science and Engineering, Oakland University Rochester MI USA
E-mail: hesiri@kln.ac.lk

(Received 6 August 2020; Revised 22 August 2020; Accepted 19 September 2020; Available online 28 September 2020)

***Abstract* - Communication messages in Vehicular Ad-hoc Networks (VANETs) can be used to track movement of vehicles. In this paper, we address the problem of movement tracking and enhance location privacy without affecting security and safety of vehicles. By considering unique characteristics of VANETs, we firstly propose a synchronized pseudonym changing protocol based on the concept of forming groups among neighboring vehicles. Secondly, we analytically evaluate the anonymity and unlinkability of the proposed protocol. Finally, we do a series of simulations to evaluate the performance of our protocol in real VANET environments such as Manhattan and Urban. Simulation results show that our protocol is feasible and produces excellent performances. The main advantages of our protocol compared with the existing approaches include: 1) it makes larger anonymity set and higher entropy; 2) it reduces the tracking probability; 3) it can be used in both safety and non-safety communications; and 4) Vehicles need not suspend regular communication for changing pseudonyms.**

Keywords: **Vehicular Ad Hoc Networks, Communication, Movement of Vehicles**

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are mobile ad hoc networks proposed to enhance vehicular safety and traffic management in transportation systems. VANET is a promising technology for efficient traffic management and avoiding auto accidents that cost thousands of human lives and billions of dollars annually. A VANET consists of vehicles equipped with On Board Units (OBUs), Road Side Units (RSUs), and other off-the-road entities such as administrative and application servers physically connected to RSUs. By using Vehicle-to-Vehicle (V2V) communications and Vehicle-to-Infrastructure (V2I) communications, vehicles can communicate not only with other vehicles but also with the infrastructure to enhance vehicular safety, improve traffic management and enhance the quality of driving with other online services.

Due to wireless communication's involvement in life critical safety applications and the close relationship between people's day-to-day life with transportation systems, both security and privacy are essential for vehicular communications [1-6, 13, 45, 47]. Wireless communication makes VANETs highly vulnerable to various types of security threats. Since the safety of vehicles and passengers highly depends on safety applications, VANETs must be protected from all kinds of security vulnerabilities and threats to make the VANETs safe and trusted. Hence, sender authentication, message integrity, non-repudiation and authorization are recognized as basic security requirements for VANETs [1, 4-6, 45]. Further, since VANETs will become an important part of the future transportation system, any security mechanism that does not preserve the privacy of drivers may not be feasible for successful implementation in real vehicular network environment. Moreover, privacy of the drivers must be protected to attract people for VANET applications. Privacy in VANETs can be described in terms of anonymity and location privacy. The former represents the concept of hiding the real identity information from others while the latter represents the concept of protecting location and movement information from others.

According to the IEEE1609.2 draft standard [29], vehicles have to regularly broadcast safety beacons with essential safety information such as identity, location, direction and speed of the vehicle over neighbouring vehicles. In addition, a message signature and the public key certificate of the message sender should be included in each message. Since these messages are broadcasted among unknown neighbouring vehicles, encryptions of these messages are not feasible. Hence, some of the critical private information of a vehicle such as identity, location and movement information could easily be exposed to others by which it makes vehicles highly vulnerable for some serious threats such as crimes and profiling [5-6]. Moreover, with traditional PKI schemes, keys and certificates of a vehicle can easily be used to track the movements of the vehicle.

Even though anonymity in secure vehicular communications can be achieved by using pseudo Public Key Infrastructures (pseudo PKI) [5, 6] for vehicular networks, adversaries are still able to track the movements of a vehicle for profiling driver's behaviours. Even though anonymity in vehicular communications can be achieved by using pseudonyms (anonymous identifiers and keys) for secure communications, adversaries are still able to track the movements of a vehicle for profiling a driver's behaviour. Further, different locations of a vehicle in VANETs can easily be exposed to adversaries due to the nature of the vehicular communications. However, location privacy of a vehicle could still be achieved by hiding relationships among different locations of the same vehicle. Even though frequently changing pseudonyms have been

proposed to achieve the unlinkability among locations of a vehicle [4,5], temporal and spatial relationships between two messages with two successive pseudonyms of the vehicle can still be used to link these two locations of the same vehicle. Hence, adversaries can still track the movements of vehicles, even though vehicles frequently change their pseudonyms. Moreover, instead of using pseudonyms PKI, group signatures have been proposed to achieve anonymity and unlinkability in vehicular communications. However, revocation of a malicious vehicle in group signature schemes requires significantly higher computational and communication resources from each member, so that revocation is not feasible in large scale and highly dynamic vehicular networks. Therefore, long-term group management schemes are not suitable for VANETs.

In this paper, location privacy of VANETs is enhanced by avoiding movement tracking. To achieve this goal, a synchronized pseudonym changing protocol that enhances the unlinkability between two successive pseudonyms of a vehicle is proposed to avoid spatial and temporal relationships between these two pseudonyms. The contribution of this work is threefold. First, a synchronized pseudonym changing protocol based on the concept of forming stable groups among neighbouring vehicles is proposed.

Second, the anonymity and unlinkability of the proposed protocol is analytically evaluated. Finally, a series of simulation studies have been conducted to evaluate and compare the performance of the proposed protocol in different VANET environments, such as Manhattan and Urban scenarios.

The main advantages of the proposed protocol are: 1) By synchronizing group of neighbouring vehicles to change pseudonyms simultaneously, this protocol increases the level of anonymity and unlinkability; 2) By avoiding spatial and temporal relationships between pseudonyms, this method reduces the probability of tracking vehicles; 3) This protocol can be used to preserve location privacy with all typical VANET applications; 4) Since vehicles always actively participate in regular communications, this proposed protocol does not adversely affect the vehicle's safety or the communication security; and 5) This protocol provides conditional traceability for authorities to handle any liability related issues when required.

The rest of the paper is organized as follows. First, Section II introduces the system model. Section III completely describes the proposed protocol.

Section IV presents the performance evaluation metrics used to evaluate the privacy. Section V theoretically analyses the performance of the proposed protocol. In Section VI, simulation results are analysed in details. Section VII discusses some of the related works. Finally, Section VIII concludes.

II. SYSTEM MODEL

A. VANET Model

A typical VANET consists of vehicles, *Road Side Units* (RSUs), administrative entities and other service providers. As shown in Figure 1, vehicles use both safety applications and other non-safety applications by using V2V and V2I communications. A vehicle that is participating in the safety application frequently broadcasts (at least, once every 300ms) its location, speed and direction as well as specific road conditions such as accidents and black ice over the neighbourhood. Consequently, receiving vehicles adapt their actions according to the received information from others. Other non-safety applications may include traffic monitoring and management, infotainment, online service, etc.

Each vehicle is equipped with an *On Board Unit* (OBU) that contains all the required equipment to handle data processing functions as well as V2V and V2I communication functions of VANETs. RSUs are access points that function as gateways between vehicles and infrastructure, and are fixed at different road side locations and physically connected to the infrastructure to communicate with both vehicles and other infrastructure entities. These RSUs are managed by the trusted authorities such as the Department of Transportation or the Secretary of the State. Further, a Registration Authority (RA) provides registration services for vehicles. All vehicles and service providers are registered with the RA in the VANET.

B. Trust Model

To provide all the required security services such as authentication, message integrity, non-repudiation and access control, trust between entities should be managed accurately. Trust among VANET entities, such as vehicles, RSUs and other service providers is maintained using keys and certificates issued by a trusted authority. Although VANETs have been considered as a type of ad hoc network, centralized administration systems can still be used to manage some required functions due to fair connectivity between vehicles and authorities.

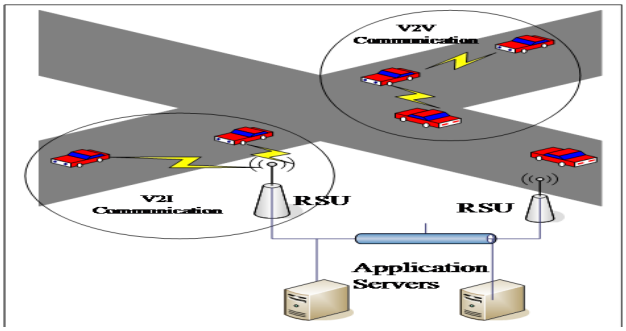


Fig.1 V2V and V2I Communication Scenarios

A Public Key Infrastructure (PKI) has been implemented in the VANET, and trusted Certification Authorities (CAs) manage keys and certificates for the network. For example, the Secretary of the State may work as the trusted CA for its own state and cross certifications are used to handle trust among CAs. Since these keys and certificates can be used to identify and track vehicles, each vehicle uses a pseudo identifier (PID), a pseudo public/private key pair with the pseudo public key certificate issued by the CA, which are collectively called a pseudonym, for secure anonymous communications. Even though these pseudo keys and certificates do not include any identification information of the vehicle/driver, the real identity of the vehicle associated to a pseudonym can only be revealed by the CA. In addition, these pseudo keys and certificates (pseudonyms) are frequently changed either by using a large set of pre-loaded certified pseudonyms [4, 5], or by frequently acquiring short term certified pseudo keys from RSUs as described in [30].

No relationship can be found between any two pseudonyms of the same vehicle. Furthermore, to prevent link layer and network layer tracking, each vehicle simultaneously changes its network and link layer addresses with the pseudonyms. As usual to all PKI systems, trustworthiness in VANETs is also maintained by using public key certificates issued by the CA. Hence, an entity only trusts another entity if the second entity has an unexpired and unrevoked public key certificate issued by the CA. Furthermore, here we assume that the vehicular PKI system can efficiently identify malicious entities and can successfully revoke them within a reasonable time.

According to the IEEE 1609.2 draft, every message in V2V and V2I communications should contain the sender's digital signature on the message and the public key certificate issued by a trusted authority to achieve authentication, message integrity and non-repudiation. So, vehicles use certified pseudo keys for signing messages and the receiver verifies valid signatures by using the attached public key certificate and the CA's public key. Since vehicles always trust the CA, vehicles verify the validity of the sender by using the public key certificate issued by the CA without knowing the real identification of the sender.

C. Threat/Adversary Model

There are two main threats against location privacy in any mobile scenario: location disclosures, in which the location information of a vehicle is disclosed to others; and movement tracking, in which others can continuously track movements of a vehicle for a long period of time. With the VANET specific characteristics such as wireless radio communication, message broadcasting among neighbors and location disclosure of vehicles cannot be avoided. However, since vehicles are communicating anonymously with pseudo keys and certificates, disclosing an individual location of a vehicle might not be a great threat to the vehicle's privacy.

Even with the anonymous communication, movement tracking of a vehicle can cause various privacy problems like profiling. Hence, in VANETs, movement tracking is considered as a serious threat for location privacy. So the unlinkability among different locations of a vehicle is the main concern of this paper.

Since it is not feasible to use different pseudo keys and certificates for each message, each pseudonym is used for a reasonably short period of time (3 -5 minutes [4, 5]). Moreover, the set of messages from a vehicle with the same pseudonym is called a trajectory, and each vehicle has different trajectories for each pseudonym. Even though frequently changing pseudonyms are used to achieve anonymity and unlinkability, if an adversary is able to correlate two trajectories with different pseudonyms of a vehicle, unlinkability could not be achieved. Adversaries can accurately correlate consecutive pseudonyms of a vehicle by using speed, direction, spatial and temporal relationships between messages with successive pseudonyms, so that regardless of the pseudonym changing, adversaries can continuously track the movements of a vehicle. Furthermore, if only one vehicle changes its pseudonym along in a monitored area, adversaries can simply correlate two pseudonyms since all other pseudonyms remain the same. Two types of adversaries, global passive adversary and active local adversary, have been identified as main threats for the location privacy of vehicles in VANETs [20, 32]. The former can eavesdrop and monitor vehicular communication messages globally to track vehicular movements while the later can closely follow the communications of specific vehicles to link their consecutive pseudonyms by using spatial and temporal relationships among messages.

In this paper, only the VANET related location privacy threats and adversaries are considered, even though it is possible to use some other expensive and sophisticated non-VANET-related tracking techniques for vehicular tracking. Hence, vehicular tracking with some other techniques such as high resolution cameras and electromagnetic signature identification hardware is out of the focus of this paper.

III. SYNCHRONIZED PSEUDONYM CHANGING PROTOCOL

In this section, the *synchronized pseudonym changing protocol* (SPCP) is proposed to enhance the location privacy of vehicles in VANETs without adversely affecting the security and safety of vehicles. This proposed protocol enhances location privacy by mitigating the movement tracking of vehicles implemented by both global passive adversaries and active local adversaries. The VANET model and the PKI based trust model described in Section II are applied for the proposed protocol. Further, the proposed protocol preserves the location privacy of VANETs against the threats and adversaries described in Section II.

At a high level, the proposed SPCP works as follows. To mitigate the movement tracking of vehicles, the proposed protocol enhances the unlinkability between consecutive pseudonyms of the same vehicle in two ways. First, the proposed protocol minimizes/avoids the spatial and temporal relationships between messages from two consecutive trajectories of the same vehicle. Second, it increases the number of vehicles that simultaneously change their pseudonyms. With the proposed protocol, each vehicle uses frequently changing pseudonyms for secure and anonymous communications as described in the system model. Each vehicle joins a temporary group before it changes its pseudonym if it can find an existing group in the current neighbourhood. Otherwise, it forms a temporary group as a group leader and invites other vehicles to join the group. Feasibility of stable group/cluster formation and management in VANETs has been discussed in several research studies [5, 14, 19, 20, 34-37]. In order to perform both of the above functions, the vehicle must have a valid pseudo public key certificate issued by the CA. After a vehicle joins a group, instead of using its own pseudonyms, a vehicle uses the group credentials such as a member private key, a group public key and the public key certificate for secure anonymous communication. After a short lifetime of a group, all the group members simultaneously change their pseudonyms and start communications by using their new pseudonyms.

Due to the use of group credentials for communications, the temporal gap between two consecutive pseudonyms of a vehicle is the same as the time in which the vehicle stays in the group. Moreover, this temporal gap makes a larger spatial gap between old and new pseudonyms due to the higher moving speed of vehicles. Therefore, it is certain that the proposed protocol always reduces the temporal and spatial relationships between two consecutive pseudonyms with the increase of group lifetime. Further, this proposed protocol can almost guarantee that more than one vehicle changes pseudonyms simultaneously due to the group based synchronization among vehicles. With the above two techniques, the proposed protocol guarantees a higher level of unlinkability among different locations of the same vehicle.

The following subsections describe the preliminaries and the required phases of the proposed SPCP protocol.

A. Short Group Signatures

Short group signatures [28] have been proposed to efficiently manage security in group environments. In group signature schemes, an entity called Group Manager (GM) handles all the group operations within the group. The GM generates and manages all the public parameters and algorithms for the group, in addition to the group public key and its own private key. When a new member joins the group, the GM generates a unique private key, which can be used with the common group public key, for the member. Messages signed by the group member's private key can be verified by using the group public key. Even though only the membership of the group can be verified with the group signatures, the Group Manager can identify the identity of the group member by using the member's signature. With the short group signature method, revocation of a group member is highly expensive, since all the remaining group members either have to regenerate their member private keys according to Group Manager's instructions, or have to acquire new member private keys from the group manager in each revocation. Therefore, efficient revocation of a group member in dynamic vehicular environment may be impossible. With this fact, groups with longer lifetimes are not suitable for the VANETs. Moreover, with these group signature methods, Group Manager should be highly reliable, since it can track all the members. Otherwise, to preserve member privacy, the role of the Group Manager should be distributed between at least two entities such that no one is able to track group members without the collaboration of the others.

This protocol applies the system model described in Section II. Each vehicle registers with the registration authority and has pseudonym identities, relevant public/private keys, certificates and other algorithms as well as parameters to handle required cryptographic operations as in [5], or according to [49] vehicles can acquire temporary pseudonym keys and certificates from RSUs. In either case, the proposed protocol prevents tracking between old and new credentials. The rest of this section describes the details of the proposed protocol.

B. Initialization Phase

At the initial vehicle registration, in addition to regular VANET parameters described in Section II, each registered vehicle is uploaded with the required algorithms and parameters for the proposed protocol by the CA. A modified version of the short group signature algorithm proposed in [28] is adapted to handle group signatures in vehicle groups because of the higher accuracy and efficiency. Unlike other group signature methods, this proposed protocol divides the group management responsibilities between the RA/CA and temporary group leaders to avoid member identifications by the temporary group leaders. Hence, the RA/CA works as the Group Manager for all the temporary groups and the group leader of a temporary group only functions as the key-handler for the group. With a collaboration of the temporary group leader, only the RA (the group manager) can identify the group member that sends a specific message with its group signature. At the initial vehicle registration, the CA generates a set of parameters as follows. Let G_a , G_b and G_T be multiplicative bilinear groups of prime order p that have g_a and g_b as the generators of G_a and G_b respectively. The strong Diffie-Hellman property is holding on these three groups. Further, ω is a computable isomorphism such that $\omega(g_b) \rightarrow g_a$, and ρ is a bilinear map with non-degeneracy properties such that $\rho : G_a \times G_b \rightarrow G_T$. Next, RA selects its group handling secrets (γ_a, γ_b) in a

way $\gamma_a, \gamma_b \in Z_p^*$ such that $x^{\gamma_a} = y^{\gamma_b} = z$ where $x, y \in G_a$, and $z \leftarrow G_a \backslash \{1_{Ga}\}$. Finally, all the vehicles are loaded with the public group parameters $(g_a, g_b, p, \omega, \rho, x, y, z, H)$ required for the group operations of the proposed protocol. The parameter H is a hash function such that $H : \{0,1\}^* \rightarrow Z_p$.

C. Group Formation Phase

With the proposed protocol, a vehicle has to form a temporary group, unless it finds a suitable neighbouring group to join before it changes the pseudonym. Figure 2 shows the detailed steps of forming a group. Before changing a pseudonym, the vehicle first listens to leader-notification beacons from existing groups in the close neighbourhood for a *threshold* period of time. If a vehicle cannot find a group leader that travels in a smaller relative speed with itself and drives within a communicable distance, the vehicle initiates the group forming process as a new group leader. First, the new group leader selects a private key $\lambda \in Z_p^*$ for itself and e group public key $PuK_G = g_b^{\lambda}$. Next, the new group leader sends a signed authorization request to the CA with the group public key PuK_G and its current pseudonym credentials such as pseudo identifier *PID*, pseudo public key and the public key certificate issued by the CA. After receiving the authorization request, the CA first verifies the public key certificate of the vehicle and the message signature of the request, and then issues a group identification number and a short-term certificate for the group public key, only if the new group leader is valid and trusted. The proposed protocol simply avoids the possibility of the same vehicle frequently becoming a group leader by not issuing group public key certificates twice to the same vehicle within a specific period of time, for example within 30 min. Hence, outsiders, adversaries with revoked certificates or any vehicle with expired certificates cannot form a group and cannot become a temporary group leader. At the end, the CA stores the (PuK_G , *PID)* pair for future references.

After receiving the group public key certificate from the CA, the new leader is authorized to perform its group operations. The leader starts broadcasting leader-notification beacons over the neighborhood with its position and speed in addition to the message signature and group public key certificate. These leader-notification beacons are regularly broadcasted in every *beacon-interval*. If none of the vehicles join the group within the first *t* time period, for example first 60 seconds, the group leader may initiate group join protocol again. The new group is only valid until the group public key certificate expires, so the lifetime of the new group (group expiration time/group lifetime) is determined by the expiration time of the group public key certificate issued by the CA.

It should be further noticed that any entity that does not have a valid group public key certificate issued by the CA cannot claim as a group leader and none of the vehicles join a group without verifying the validity of the leader. Further, communication overhead on the CA can be reduced by fairly distributing mirrors of the CA over the region.

Vehicle	CA
If (No suitable group found to join)	
1. selects computes group public key $PvK_{GL} = \lambda \in_R Z_p^*$	computes group public key $PuK_G = g_b^{\lambda}$
2. computes $REQ = (PID \mid PuK_G \mid ts)$ $M = Enc_{PuK_{CA}}(\mathrm{Re}q \mid Sig_{PvK_V}(Req) \mid PuK_V \mid Cert_{CA}(PuK_V))$	
3. sends *M* to the CA	M →
	4. decrypts M with PvKCA
	5. Verifies the $Cert_{CA}(PuK_V)$
	6. Verifies the $Sig_{PvK_V}(REQ)$ with PuK_V
	7. Checks the validity of *PID* and PuK_V using *CRL*
	8. if (vehicle is valid) && (the vehicle is not issued a certificate within last threshold period) generates $Cert_{CA}(PuK_G)$
	9. sends *R* to the vehicle
	← R
10. decrypts R with PvKV	
11. Verifies the $Sig_{PvK_{CA}}(RES)$ using PuK_{CA}	
12. starts sending leader-notifications	
13. listens for join-requests	

Fig. 2 Group Formation Protocol

D. Group Joining Phase

Before changing pseudo keys and certificates, each vehicle has to join an existing group in the neighbourhood. The detailed steps of joining a group are shown in Figure 3. Vehicles identify the neighbouring groups by listening to the leader-notification beacons, which include position, speed and direction of the group leader, in addition to the public key certificate of the leader, from other groups. A vehicle initiates the group-joining process with the nearest group leader, who has the smallest relative speed and drives within a communicable distance. In this way, the proposed protocol always maintains stable vehicle groups in the dynamic VANET environment.

In the group joining process, vehicles first check the validity and the trustworthiness of the group leader by using public key certificates and the process continues only with valid and trusted group leaders. Next, the vehicle sends a join-request to the group leader with its signature, the pseudo identifier *PID* and pseudo public key certificate issued by the CA, in addition to position, speed and direction of the vehicle. The group leader authenticates both the vehicle and the join-request using the attached signature and the pseudo public key certificate. After verification, the group leader generates a unique secret key, (*A* ,*q*) for the new member, such as $q \in Z_p^*$ and $A = g_a^{1/(\lambda+q)}$, where λ is the leader's private key. These member private keys can be used with the common group public key (PuK_G).

Next, the group leader stores a record (*A*, *PID*) for the new member. The group leader should keep all the member records (list of (*A*, *PID*)) for several days for future references. More importantly, none of the actual identification information of the member vehicle is exposed to the group leader since pseudonyms do not contain any of them. Finally, group credentials, such as member private key, group public key, public key certificate, group identifier, and common set of temporary identifiers that can be selected and be used randomly, are sent to the new member vehicle. The member private key should be encrypted with the new member's pseudo public key, so that it can only be decrypted by the vehicle with associated pseudo private key. After receiving these group credentials, the vehicle becomes a new group member and starts communication with these group keys instead of its own pseudonyms. To maximize the privacy of the whole system, all the vehicles in the group perimeter may join the group, even though they are not intending to change their pseudonyms shortly.

E. Group Operations Phase

Each group member uses its temporary group private/public keys instead of its own pseudo keys for secure communications while in the group. To comply with the IEEE 1609.2 requirements, each group member uses the group identifier and the member private key to sign all the outgoing messages and the group public key certificate issued by the CA is attached to each message for authentication. If the receiving vehicle is a member of the same group as the sender, it will simply verify these message signatures by using their common group public key. Otherwise, the receiving vehicle first verifies the group public key by using the attached public key certificate and the CA's public key and then it will verify the message signature by using the group public key. Member vehicles in a group can be involved in all of the regular VANET applications and other required services without any restrictions. Therefore, the group operations do not adversely affect any of the regular VANET applications and services.

Signatures of any group member can be verified by using the common group public key without exposing the signer. Furthermore, even the group leader cannot identify the sending members from the received message signatures and no one can link two signatures from the same group member. Hence, the privacy of the member vehicles can be fully preserved. Even though the group leader has a list of current pseudonyms of all group members, it cannot track any of the member vehicles using their communication messages. When resolving liability issues, only the CA can calculate the member private key *A* of liable member by using the CA's group handling secrets (γ_a, γ_b), the message signatures and the group public key certificate belong to the group member. With the collaboration of the associated group leader, the RA/CA can find out the pseudo identifier of the source associated to the member private key, so the real identity of the message signer can be revealed whenever a liability related issue has to be resolved. This can be done even after the group has been dissolved, since the CA has the required information (K_G , *PID)* to map the group public key to the group leader's *PID*. Therefore, the proposed protocol provides the conditional privacy whenever required.

F. Pseudonym Changing Phase

After sufficient time, all the group members simultaneously change their pseudonyms and start communication using the new pseudonyms. With the proposed method, the group leader reminds all group members about the expiration time of the group, and all the group members simultaneously change their pseudonyms at the specified time. Since all member vehicles change their pseudo identifiers and certificates that are used to join the group, the group has to be dissolved and all the member vehicles independently start communications by using their new pseudonyms. Further, they also change the current signal strength level to another level before they send the first packet with the new pseudonym. Moreover, if any vehicle moves out from the full connectivity region of its group perimeter before the end of the group lifetime (if a member does not hear leader notification beacons from its group leader for a *threshold* time), it is eventually considered as having left the group. In this case, the vehicle changes its pseudonym if the vehicle

has been in the group for a sufficient amount of time, for example 60s, to avoid spatial and temporal relationships between two pseudonyms. Otherwise, the vehicle either joins another group or forms a new group before it changes its pseudonym.

Since a vehicle uses group identifiers and group keys for a sufficient time period between two consecutive pseudonym identifiers, the temporal and spatial properties of the old and new pseudonyms of the same vehicle are significantly different. Moreover, since all of the group members, including the group leader, simultaneously change their own pseudo identifiers that are not used in the group membership period, the set of new pseudonyms that belonged to all the previous group members can only be mapped to the set of vehicles. However, an individual pseudonym cannot be mapped to an individual vehicle. Thus, adversaries cannot easily link two consecutive pseudonyms of the same vehicle for continuous tracking. Further, we do not need to use silent periods between two pseudonyms to avoid relationships of the two pseudonyms.

Hence, with the proposed protocol, vehicles can always participate in regular communications without interfering normal operations of the VANETs. This preserves the accuracy of the data and the quality of life critical safety applications. This means that the proposed protocol does not adversely affect the safety and the security of the vehicles.

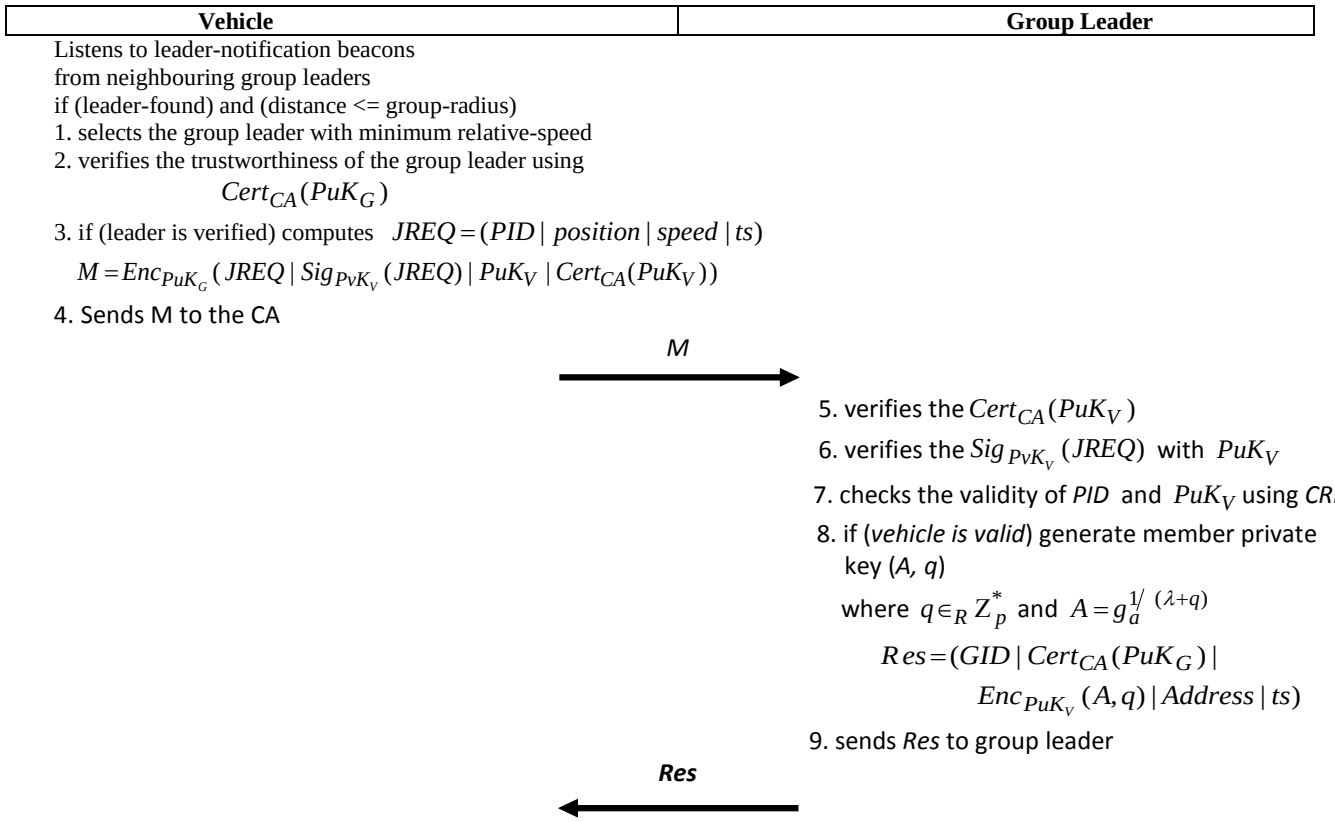


Fig. 3 Group Joining Protocol

IV. PERFORMANCE METRICS

For a short period of time, each vehicle uses a pseudo identifier, a pseudo public/private key pair and a public key certificate issued by the CA, which are collectively called pseudonyms and do not include any identifying information of the vehicle. Within this time, the vehicle only uses this pseudonym for all of its outgoing messages. After the end of each period, the vehicle changes its pseudonym and continues communications with the new pseudonym for another short period of time. Even though these pseudonyms do not contain any personal information, adversaries use a sequence of messages from the same pseudonym to track the vehicle's movement. However, with the proposed protocol, each vehicle joins a temporary group and uses group credentials for communications in between its two consecutive pseudonyms. The proposed protocol assumes that a vehicle uses different pseudonym identifiers

at different period of time and two vehicles do not share a pseudonym for communications. Hence, each pseudonym is unique for a vehicle. However, within a group, a common group identifier and a common group public key are shared for their communications.

Let *ID* be a pool of pseudonym identifiers that contains all possible identifiers for all the vehicles. According to [17], trajectory T_i for pseudo identifier $i \in ID$ can be defined as a series of actions with the same sender identity *i*. Therefore, a trajectory is associated with a pseudonym identifier rather than a vehicle. In the VANET scenarios, each vehicle has several trajectories, one for each pseudonym identifier that it has used. However, all actions executed by all the group members belong to the same trajectory with the group identifier, since all the vehicles in a group share the group identifier and the common group public key for all of their communications.

Let $p(i,j) \in P$ be the attacker's a-posterior probability of correlating two trajectories T_i and T_j on the source of actions. Then for each pseudonym identifier *i*, $\sum_{j \in ID} p(i,j) = 1$

Based on [17], we define three metrics for performance evaluation.

Definition 1–Anonymity set (AS) of a target: Given a pseudonym identifier $i \in ID$ and its trajectory T_i, the anonymity set AS_i of the pseudonym identifier *i* is defined as

$$AS_i = \{ j \mid j \in ID, \exists T_j \ \ s.t. \ \ p(i,j) \neq 0 \} \quad \text{.....(1)}$$

Hence, the AS_i includes all pseudonym identifiers whose trajectory T_j may be correlated to T_i. In other words, AS_i contains all the vehicles that cannot be distinguished from the target. Next, we define the size of the anonymity set as $|AS_i|$, the number of elements of the AS_i, which is a measure of location privacy for pseudonym identifier *i* [17].

Definition 2–Entropy of an anonymity set: The entropy *Hi* of the anonymity set AS_i can be defined as

$$H_i = -\sum_{j \in AS_i} p(i,j) \times \log_2(p(i,j)) \text{ . ..... (2)}$$

This represents the level of uncertainty in the correlations that the trajectory T_i has with all other trajectories T_j.

Definition 3–Tracking probability: The tracking probability Pt_i of a target identifier *i* can be defined as

$$Pt_i = P(|AS_i| = 1) \quad \text{.....(3)}$$

This is the probability that the size of the anonymity set is equal to one. In other words, the probability that the anonymity set of a target only contains the target itself.

V. THEORETICAL ANALYSIS

In this section, the anonymity and the unlinkability of the proposed protocol is analytically evaluated in terms of size of an anonymity set, entropy of an anonymity set and tracking probability.

In order to track the movements of a vehicle, adversaries have to continuously link consecutive pseudonyms (or trajectories with consecutive pseudonyms) of the vehicle. This can be achieved by correlating last message of a trajectory to the first message of the next trajectory of the same vehicle.

By knowing the location of the last message and the speed and direction of the vehicle, adversaries can predict the possible area from which the vehicle may send the first message with the new pseudonym. Therefore, adversaries can determine the anonymity set for the target as the set of vehicles that start communications with new pseudonyms from the predicted area. The possibilities of correlating each of the different vehicles (new pseudonyms) in the anonymity set to the target are equally likely unless some of them have specific temporal and spatial relationships.

Let *T* be the duration between the time when a vehicle enters the group and the time when the group is dissolved. Further, vehicles are entering and leaving any area of interest with the average rate of *r*. Let *X* be the number of vehicles leaving the group within the time period *T*. Since the number of arriving vehicles to the area and the number of departing vehicles from the area follow the Poisson distribution [24], the variable *X* has a Poisson probability distribution, i.e.,

$$X \sim Poisson(\lambda_1) \rightarrow X \sim Poisson(rT),$$

where $\lambda 1 = rT$, the average number of vehicles leaving the group within time *T*. Then,

$$P(X = k) = \frac{(rT)^k}{k!} e^{-rT} \quad \text{.....(4)}$$

Vehicles are uniformly distributed over the roads with the average density of *d*. Let *a* be the group radius, that is, the maximum distance from the group leader to any vehicle in the group, *A* be the area that can be covered by a group leader, and *Y* be the number of vehicles that stay within the group perimeter when the group is dissolved. According to [25], *Y* distributes according to the Poisson process, i.e,

$$Y \sim Poisson(\lambda_2) \rightarrow Y \sim Poisson(dA),$$

where $\lambda 2 = dA$, the average number of vehicles in a group perimeter. Then

$$P(Y=k)=\frac{(dA)^k}{k!}e^{-dA} \quad \text{.....(5)}$$

Consider the set *V* defined as follows

$$V=\left\{\begin{array}{l} v\in ID \mid v \text{ is a pseudonym identity of any vehicle} \\ \text{that leaves the group within the time period } T \text{ or} \\ \text{a pseudonym identity of any vehicle that stays} \\ \text{within a group leader's range when the group} \\ \text{dissolves} \end{array}\right\}$$

When a target vehicle enters a group, it starts to use common group credentials, such as a group identifier, a group public key and the group public key certificate. Since all other members also use the same group credentials, attacker cannot distinguish the target from other members. The target either leaves the group before the group is dissolved or stays until the group is dissolved. Therefore, the anonymity set AS_i of an entering vehicle's pseudonym identifier *i* contains all the vehicles that leave the group within the time period *T*, as well as all the vehicles that stay within the group perimeter when the group is dissolved. Hence, the anonymity set AS_i is equal to the set *V*, that is $|ASi| = X + Y$. Thus,

$$|AS_i| \sim Poisson(\lambda_1+\lambda_2) \rightarrow |AS_i| \sim Poisson(rT+dA).$$

Thus, the probability of |ASi| = k can be defined as

$$p(|AS_i|=k)=\frac{(rT+dA)^k}{k!}e^{-(rT+dA)} \quad \text{.....(6)}$$

A. Size of the Anonymity Set

Anonymity set is defined for individual targets. To find the average size of the anonymity set of a target, the expected size of the anonymity set of a target should be derived. With the proposed protocol, an anonymity set contains at least the target itself. Thus $|ASi| >= 1$.

Theorem 1–Expected size of the anonymity set: The expected size of the anonymity set of a target *i* in the proposed pseudonym changing protocol is

$$E\{|AS_i|\}=\frac{rT+dA}{1-e^{-(rT+dA)}} \quad \text{.....(7)}$$

where *r* is the average rate of vehicle entering and leaving, *d* is the average vehicle density in the roads, *T* is the average time until the group is dissolved from the time that the target vehicle enters the group and *A* is the area covered by the group.

Proof. The expected size of the anonymity set, given that $|AS_i| >= 1$, can be defined as

$$E\{|AS_i|\}=E\{|AS_i| \,\big|\, |AS_i|\geq 1\}$$

Since |ASi| = X+Y. Thus

$$\begin{aligned} E\{|AS_i|\} &= E\{X+Y \mid X+Y\geq 1\} \\ &= \frac{E\{X+Y\}}{p(X+Y\geq 1)} \\ &= \frac{E\{X+Y\}}{1-p(X+Y=0)}. \end{aligned}$$

Since $|AS_i| \sim Poisson(rT+dA)$, we have $E\{|AS_i|\}=rT+dA$. Then, from Equation (6), with k = 0, we get $P(|AS_i|=0)=e^{-(rT+dA)}$. Thus,

$$E\{|AS_i|\}=\frac{rT+dA}{1-e^{-(rT+dA)}}$$ □

B. Entropy of the Anonymity Set

To measure the level of uncertainty of linking two pseudonym identifiers, the entropy of the anonymity set of a target should be evaluated.

Theorem 2–Entropy of the anonymity set: Entropy Hi of the anonymity set of a target i in the proposed pseudonym changing protocol is

$$H_i=\log_2(rT+dA)-\log_2\left(1-e^{-(rT+dA)}\right) \quad \text{.....(8)}$$

Proof. According to Equation (2), entropy of the anonymity set can be defined as

$$H_i=-\sum_{j\in AS_i} p(i,j)\times\log_2(p(i,j)),$$

where *p(i,j)* is the probability of correlating pseudonym identifier *j* from the anonymity set to the target *i*. All pseudonym identifiers in the anonymity set have equal possibility to match with the target. So, for all pseudonym identifiers *j*, we have

$$p(i,j)=\frac{1}{E\{|AS_i|\}}$$

Then the expected entropy of the anonymity set can be expressed as

$$\begin{aligned} H_i &= -\sum_{j\in AS_i}\frac{1}{E\{|AS_i|\}}\times\log_2\left(\frac{1}{E\{|AS_i|\}}\right) \\ &= -\frac{1}{E\{|AS_i|\}}\times\log_2\left(\frac{1}{E\{|AS_i|\}}\right)\times\sum_{j\in AS_i}1 \end{aligned}$$

$$= -\log_2(\frac{1}{E\{|AS_i|\}})$$

$$= \log_2(E\{|AS_i|\})$$

From Equation (7), we have the value for the expected size of the anonymity set. Then

$$H_i = \log_2\left(\frac{rT+dA}{1-e^{-(rT+dA)}}\right)$$

$$= \log_2(rT+dA) - \log_2\left(1-e^{-(rT+dA)}\right) \square$$

C. Tracking Probability

Tracking probability of a target is the probability that the anonymity set contains only the target itself.

Theorem 3–Tracking probability of target i: Tracking probability, *Pt*i of a target *i* in the proposed pseudonym changing protocol is

$$Pt_i = \frac{rT+dA}{e^{(rT+dA)}-1} \quad \text{..... (9)}$$

Proof. The tracking probability of a target vehicle, given that the anonymity set contains at least one vehicle, can be defined as

$$Pt_i = P(|AS_i| = 1 \mid |AS_i| \geq 1)$$

$$= \frac{P((|AS_i| = 1) \cap (|AS_i| \geq 1))}{P(|AS_i| \geq 1)}$$

$$= \frac{P(|AS_i| = 1)}{1-P(|AS_i| = 0)}$$

From Equation (3), $P(|AS_i| = 0) = e^{-(rT+dA)}$ and $P(|AS_i| = 1) = (rT+dA)e^{-(rT+dA)}$. Thus,

$$Pt_i = \frac{(rT+dA)\, e^{-(rT+dA)}}{1-e^{-(rT+dA)}}$$

$$= \frac{rT+dA}{e^{(rT+dA)}-1}. \square$$

VI. SIMULATIONS AND PERFORMANCE EVALUATIONS

By using simulations, the performance of the proposed synchronized pseudonym changing (SPCP) protocol is evaluated and compared in different vehicular ad hoc network environments. The performance of the proposed scheme is evaluated in terms of size of the anonymity set, entropy of the anonymity set, and tracking probability which are described in previous sections. Moreover, theoretical models developed in previous sections are validated by these simulations.

A. Simulation Setup

The Network Simulator, ns-2 [26], is used to simulate the proposed pseudonym changing protocol for VANETs. In order to absorb real mobility features of vehicular environment, Manhattan and Urban mobility scenarios generated by using GMSF [27] are used for all simulation experiments. With the Manhattan mobility scenario, vehicles are driving in a grid-based road network while with the urban scenario; vehicles are driving according to a real urban road network from a Swiss geographic information system. Further, a simple car-following model, a traffic light model and real vehicular speed patterns are employed to control vehicular mobility in all of the simulation scenarios. Physical and link layers of the ns-2 protocol stack are configured according to the IEEE 802.11p specifications [43]. Unless we explicitly state different number of vehicles, a total of 250 and 400 vehicles are evenly distributed over a 3000m X 3000m area for the urban and Manhattan scenarios, respectively. Each vehicle broadcasts safety beacons with its location and speed in every 500ms. Furthermore, RSUs are evenly distributed over the area in a way that at least one RSU is available within a communication e of every road section.

TABLE 1: DEFAULT SIMULATION PARAMETERS

Group Lifetime	120s
Group Radius	300m
Terrain area	3000m X 3000m
Simulation time	600s

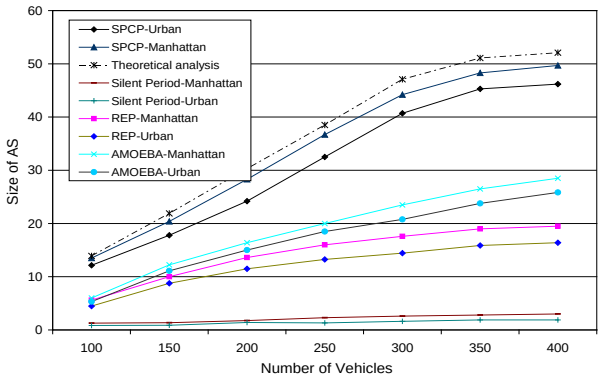
The above performance evaluation metrics are measured by varying three protocol parameters: the number of vehicles, group radius, and group lifetime. For each case, simulation is run for 600s and the average values of each measurement are taken from 100 simulation runs with different seed values. Table 1 lists all default parameters for the entire simulations.

B. Impact of Number of Vehicles on Privacy

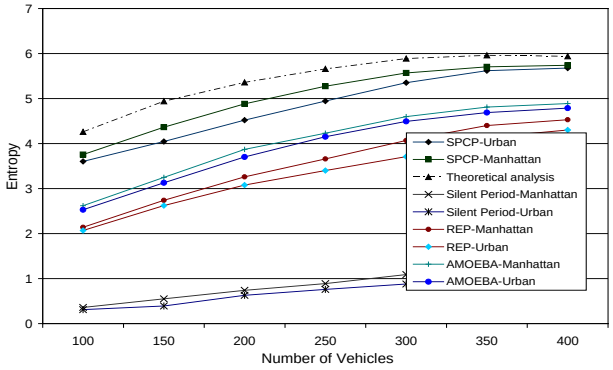
First, the impact of the number of vehicles on the performance of the proposed SPCP protocol is studied by varying the number of vehicles from 100 to 400 with the increment of 50 in both urban and Manhattan scenarios. In addition, privacy of the proposed protocol is compared with the privacy of the three frequently cited protocols, silent period method [16-17] (with the silent period of 1s), REP [32] and AMOEBA [19-20] over a different number of vehicles in both urban and Manhattan scenarios. Figure 4 shows the impact of the number of vehicles in the network on the performance of the proposed protocol and the performance of the silent period method, REP and AMOEBA. As can be seen, vehicular density on roads directly affects the level of privacy provided by the proposed protocol.

In Figure 4 (a), the average values of the size of the anonymity set of a target vehicle are plotted. Since the number of vehicles that are supposed to change their pseudonyms increases with the vehicular density, a higher number of vehicles in the network always produces a higher number of members in each group. Hence, a higher vehicular density always produces a larger anonymity set and higher level of unlinkability and privacy. Further, the size of the anonymity set rapidly increases with the number of vehicles, since the anonymity set includes all group members as well as all the other vehicles in the group perimeter when the group dissolves. It can be seen that the size of the anonymity set is always larger than one.

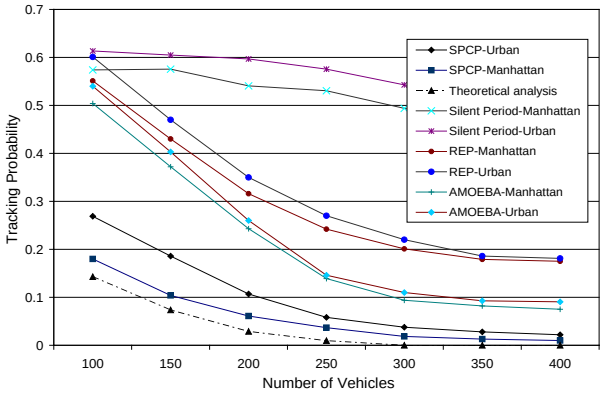
So, the unlinkability between two successive pseudonyms of a vehicle is fully preserved by the proposed pseudonym changing protocol. Moreover, as shown in the Figure 4 (a), regardless of the number of vehicles or the length of the silent period, the silent period method always produces a smaller anonymity set than that of the proposed method since short silent periods are not long enough to make a larger anonymity set. So, the level of unlinkability produced by the silent period method is always lower than the level of unlinkability produced by the proposed method. Hence, it is obvious that the proposed protocol significantly outperforms the silent period method in terms of location privacy. However, the length of a silent period cannot be extended due to the cost of vehicular safety. Moreover, the proposed SPCP protocol always produces higher performance than REP and AMOEBA protocols.



(a)Size of the Anonymity Set vs. Number of Vehicles



(b).Entropy vs. Number of Vehicles



(c).Tracking Probability vs. Number of Vehicles

Fig.4 Effect of the Number of Vehicles

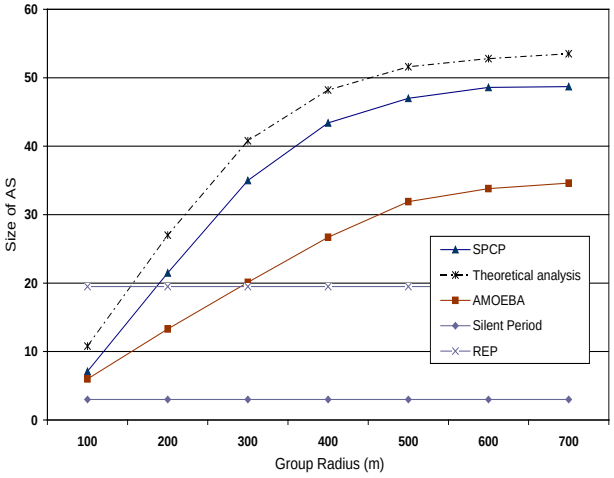
Figure 4 (b) shows the impact of the number of vehicles on entropy. Since the higher vehicular density reduces the ability of isolating target vehicles, the entropy also increases with the number of vehicles. Hence, higher vehicular densities always provide higher levels of uncertainty for adversaries. Moreover, the Manhattan scenario always provides a higher level of entropy than the level of entropy provided by the urban scenario due to the evenly distributed road network of the Manhattan scenario. As shown in Figure 4 (b), the silent period method always produces a lower level of entropy than that of the proposed method. As a consequence, it gives a lower level of uncertainty than the uncertainty provided by the proposed method.

As shown in Figure 4 (c), tracking probability is also affected by the number of vehicles. Even though the average minimum size of the anonymity set is not reduced to one, there is a small probability that the actual size of the anonymity set could become one if a vehicle is unable to find an existing group or another vehicle in its communication range to form a group before it changes the pseudonym. Since a higher vehicular density reduces the number of isolated vehicles, a higher number of vehicles always make smaller tracking probabilities. Moreover, as shown in Figure 4 (c), the silent period method always produces a higher tracking probability than the proposed method since smaller silent periods are not long enough to avoid spatial and temporal relationships between two successive pseudonyms. So, the possibility of tracking vehicles with the silent period method is quite higher than that of the proposed method.

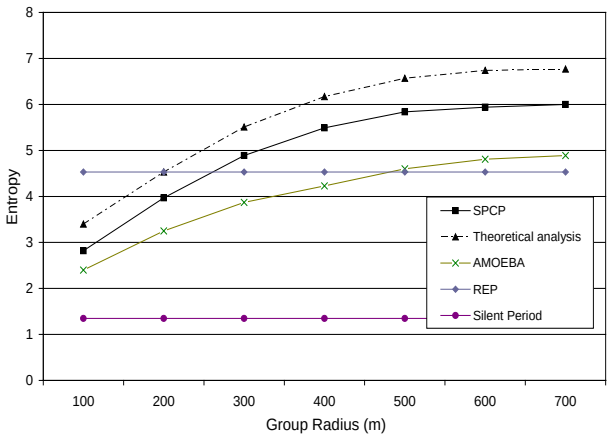
As can be observed in these figures, theoretical results are fairly equivalent to the simulation results. Hence, the derived analytical models for the proposed protocol can be validated. Nevertheless, the slight deviation between theoretical and simulation results can be described as a cause of complex mobility patterns.

C. Impact of Group Radius on Privacy

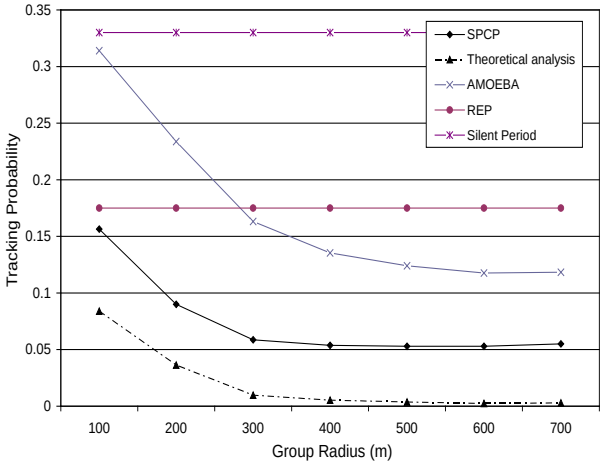
In this section, the effect of group radius on the level of privacy provided by the proposed protocol is studied in Manhattan scenario. Moreover, the performance of the proposed protocol is compared with AMOEBA [20], REP [32] and silent period [16-17] methods. The group radius is varied from 100m to 700m with the increment of 100m. Several observations on Figure 5 can be made. As can be seen, the group radius directly affects the privacy performance of the proposed SPCP protocol and a higher group radius always provides a higher level of privacy. However, the group radius has a zero affect on the performance of the REP and silent period methods since the groups are not involved in these protocols.



(a) Size of the Anonymity Set vs. Group Radius

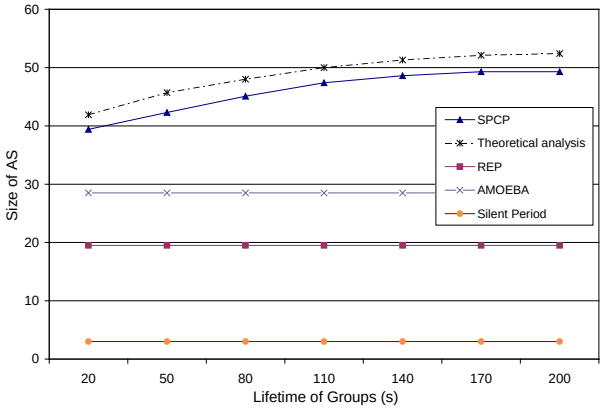


(b) Entropy vs. Group Radius

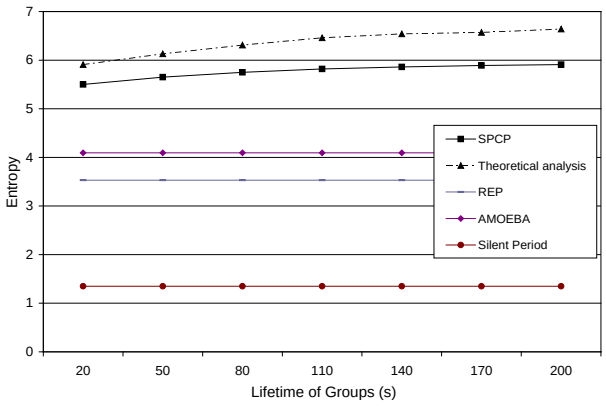


(c) Tracking Probability vs. Group Radius

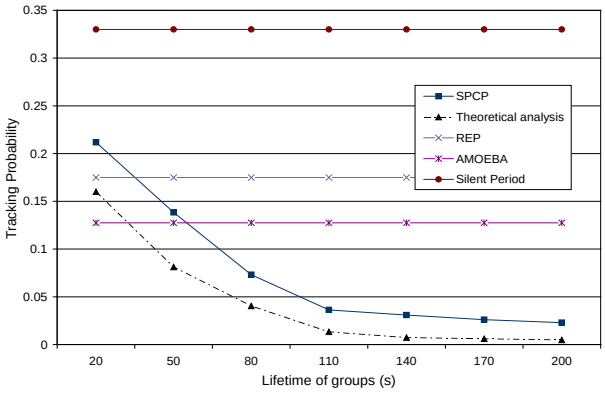
Fig. 5 Effect of Group Radius



(a) Size of the Anonymity Set vs. Group Lifetime



(b) Entropy vs. Group Lifetime



(c) Tracking Probability vs. Group Lifetime

Fig.6 Effect of Group Lifetime

The impact of the group radius on the size of the anonymity set of a target vehicle is illustrated in Figure 5 (a). A group with a higher radius can have more members and more vehicles in the group perimeter than a group with a lower radius since the radius defines the group boundaries. Hence, with a higher group radius, a larger number of member vehicles simultaneously change their pseudonyms, which results in a higher level of unlinkability. As shown in the figure, sizes of the anonymity set rapidly increase with the group radius.

Figure 5 (b) shows how the group radius affects the entropy. Similar to the anonymity set, the entropy also increases with the group radius. Since a higher radius always produces large groups with more group members, this makes it more difficult for adversaries to distinguish their targets from other group members.

Hence, a higher group radius provides a higher level of uncertainty in tracking, so that it always produces a higher level of entropy.It should be further noticed that the size of the anonymity set and the entropy rapidly increase with the group radius only until the radius reaches 400m. However, further increase of the group radius does not make significant improvement since larger distances between members and the group leader make loosened connectivity within the group so that some members may have to frequently change the group before changing a pseudonym.

The impact of the group radius on tracking probability is shown in Figure 5 (c). Although, the average size of the anonymity set is always greater than one, there is a very small probability that the actual size of the anonymity set for some vehicles becomes one.

This implies that even though most of the groups contain a large number of member vehicles, a few of the groups might only contain a single vehicle. Hence, there is a very small probability of tracking vehicles when they change their pseudonyms. The probability of vehicular tracking decreases with the increase of the group radius until the radius reaches 300m, since a higher group radius reduces the adversary's ability to isolate target vehicles. When the radius is further raised, the tracking probability slightly increases due to the loosened connectivity between group members and the group leader.

D. Impact of Group Lifetime on Privacy

Here, the impact of group lifetime on the proposed SPCP protocol is studied in Manhattan scenario by varying group lifetime from 20s to 200s with the increment of 30s. Moreover, the performance of the proposed protocol is compared with AMOEBA [20], REP [32] and silent period [16-17] methods. Figure 6 shows the impact of group lifetime on the location privacy provided by the proposed SPCP protocol. However, the group lifetime has a zero affect on the performance of the AMOEBA, REP and silent period methods since the groups are not involved in REP and silent period method and lifetime is not a parameter in AMOEBA protocol.

In Figure 6 (a), average values of the size of the anonymity set of a target vehicle have been shown. As shown in the figure, the size of the anonymity set is not significantly affected by the group lifetime, since the group lifetime has very little impact on the total number of members in a group. Even though the impact of the group lifetime is very little, the size of the anonymity set of a target vehicle slightly increases with the group lifetime.

Figure 6 (b) shows how the group lifetime affects the entropy, and as can be seen, the affect of the group lifetime on the entropy is negligible. Hence, by increasing the lifetime of a group, we cannot expect a better level of entropy from the proposed protocol.

Finally, the impact of the group lifetime on the tracking probability is evaluated, and the simulation results are presented in Figure 6 (c). Even though the size of the anonymity set and entropy are not noticeably affected by the group lifetime, with the proposed protocol, tracking probability is significantly affected by the group lifetime.

This is because spatial and temporal relationships between two consecutive pseudonyms of a member vehicle highly depend on the group lifetime. Since a longer group lifetime reduces these relationships between pseudonyms, the tracking probability, as shown in the figure, exponentially decreases with the increase in the group lifetime until the lifetime reaches 110s.

However, further increase of the lifetime does not significantly improve the privacy since larger lifetime may eventually cause members to quit the group before the end of the group lifetime due to higher dynamic nature. Therefore, higher lifetime is not recommended for temporary groups since it decreases the privacy performance.

VII. OVERHEAD OF THE PROPOSED PROTOCOL

In this section, the computational and communication efficiency and the overhead of the proposed protocol are evaluated. In addition to usual communication activities, the proposed protocol introduces two other communication scenarios, group forming and group joining, which introduce additional communication and computing operations to the network. Here, we consider the communication and processing delay and the bandwidth overhead of the proposed protocol. With the group forming phase, the group public key certificate request and the response messages between a vehicle and the CA introduce some additional overhead to VANETs. A request message contains a group public key (28 bytes), a pseudo identifier (4 bytes), a timestamp (2 bytes), an ECDSA signature (40 bytes) and a public key certificate (121 bytes), so that each request message is 195 bytes long. A response message contains a group public key certificate (121 bytes), the CA's signature (40 bytes) and some other required parameters such as a group identifier (4 bytes), a temporary addresses range (4 bytes) and a timestamp (2 bytes). Hence, the response is totally 171 bytes. However, this group forming process is executed only when a vehicle needs to change its key with no other neighboring groups available to join. Therefore, these request and response messages do not make significant bandwidth overhead in VANETs.

Another two additional messages are introduced to the VANETs by group joining phase. Group joining request from a vehicle to a group leader contains position (2 bytes), speed (2 bytes), pseudo identifier (4 bytes) and timestamp (2 bytes) in addition to the message signature (40 bytes) and public key certificate (121 bytes), which totals 171 bytes. Meanwhile, the response from a group leader totally costs 159 bytes which contains the group identifier (4 bytes), the member private key (28 bytes), the timestamp (2 bytes), the address range (4 bytes) and the group public key certificate (121 bytes).

Next, the computational efficiency for both group forming and group joining phases is evaluated. Figure 7 shows the communication delay and the success probability for both group forming and group joining operations. Elliptic Curve Cryptographic (ECC) operations such as pairing operations and point multiplications are the two main time consuming operations in all of these functions. According to [44], the latest OBU includes a specifically designed crypto-accelerator that can compute around 2500 ECC operations per second. With these specifications, a pairing operation costs 0.4ms and a point multiplication operation only costs 0.06ms. Therefore, both the ECDSA signature verification and certificate verification can be done in less than 1ms, and a certificate can be created within 0.5ms.

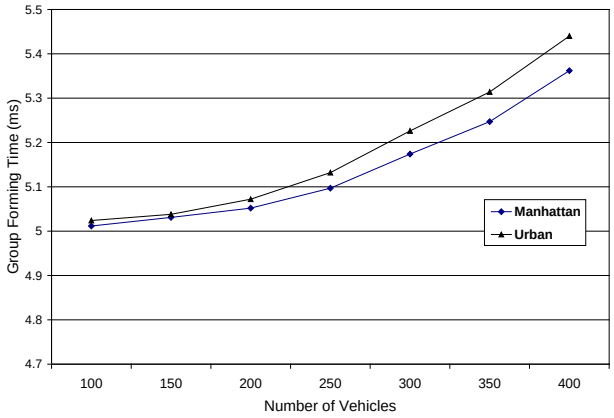
Figure 7 (a) shows that the average group forming time varies with the vehicular densities. This time includes the time for two signature verifications, two signature creations and an encryption/decryption in addition to the communication delay between a vehicle and the CA through a RSU. Since a vehicle only forms a group if it cannot find an existing group in the neighborhood, the number of group formations does not significantly increase with the number of vehicles. Even though vehicle density does not significantly affect the group forming delay, the delay slightly increases with the density since these vehicles create higher wireless traffic in the neighborhood. The success probability of forming groups is shown in Figure 7 (b), and the success ratio slightly decreases with the traffic density due to the increase of wireless traffic in the neighborhood. The average group joining delay for a vehicle is shown in Figure 7 (c). This delay includes two verifications, a signature creation and encryption/decryption operations between a vehicle and a group leader. Group joining delay also increases with the vehicular density due to the increase of wireless traffic in the neighborhood and the increase of simultaneous group joining requests from other neighboring vehicles.

VIII. RELATED WORKS

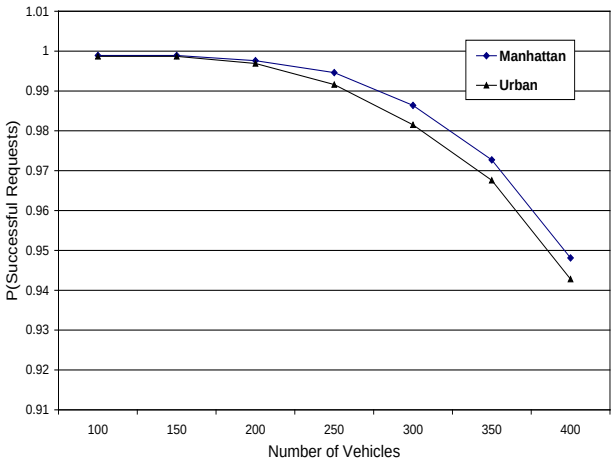
Even though, many research efforts have been done to improve the performance of VANETs, many of the security and privacy issues have yet to be addressed [1-6, 13, 45, 47]. Basic security architecture for VANETs was presented by [2] and [3]. Raya et al. [4] proposed frequently changing pseudonyms to provide anonymous communications in VANETs, and suggested to change these pseudonyms only when vehicles change their direction. Further, other research works [6, 11, 38, 40, 41] analysed the effect of frequently changing keys and pseudonyms on the accuracy and efficiency of the VANET protocols and applications. Protocols proposed in [13, 14, 30, 31, 38, 39] specifically focus on privacy-preserving key management schemes for VANET to provide anonymous communication. In [40], authors proposed a cross-layer privacy scheme for VANETs to avoid link-layer and network-layer tracking while changing pseudonyms.

Many research studies have been conducted to protect users from location privacy threats in mobile networks. Since most of these works are based on the anonymity and unlinkability, these location privacy protection methods have focused on improving the unlinkability among locations of a moving object. In [15], Beresford introduced MIX zones for mobile users to change pseudonyms. A MIX zone is an isolated area where none of the outsiders can listen to the inside communications and the users in the MIX zone cannot access any outside services. Therefore, outsiders cannot track movements of mobile objects in the MIX zone while mobile objects change their pseudonyms. However, using spatial and temporal relationships between two positions of a mobile user, others can map its two successive pseudonym identifiers. Further, these types of isolated zones are not feasible for VANETs due to its unrestricted and open nature of communications.

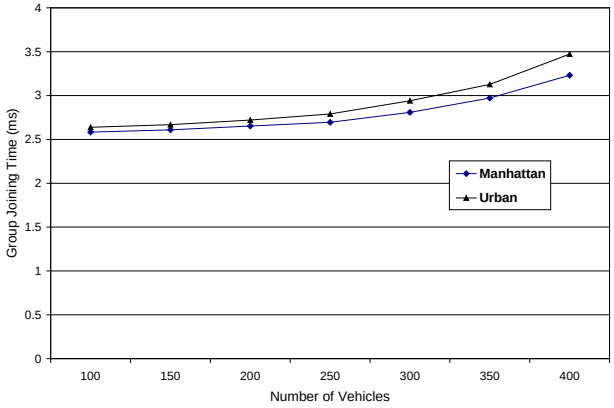
A similar concept is also proposed for VANETs by [41] in which road sections are categorized into two types of zones: observed zones and unobserved zones. Unobserved zones, areas where vehicles usually change their direction and speed, are pre-defined and reserved for changing pseudonyms. Although this makes it difficult for adversaries to predict the exact movements of vehicles within the unobserved zones, it is easy to deploy some specific eavesdropping techniques since these zones are predefined. Freudiger and Raya [18] proposed cryptographic mix zones (CMIX), pre-defined zones in junctions for changing pseudonyms, to protect the location privacy in VANETs. Within the CMIX zones, all the vehicles use encrypted communications by using a shared secret key acquired from the designated RSU in the zone. Therefore, this method protects all the sensitive information which can be used for tracking vehicles from outsiders. However, with this method, anyone who has the shared secret key can read all the messages and can easily map two pseudonym identifiers. Furthermore, since these zones are pre-defined, adversaries can specifically monitor these zones to map the pseudonyms. If the RSUs in the zone are compromised, adversaries can easily track the vehicles since they can easily acquire the shared secret key for the zone. The random silent period method was proposed to overcome movement tracking in mobile networks [16-17].



(a) Group Forming Time vs. Number of Vehicles



(b) Success Probability vs. Number of Vehicles



(c) Group Joining Time vs. Number of Vehicles

Fig. 7 Performance Overhead

With this method, mobile nodes turn off their transmitters for a period of time (silent period) and update their pseudonyms to protect location privacy by assuming that mobile nodes cannot be tracked unless they are communicating. However, the silent period has to be long enough to avoid temporal and spatial relationships between two successive pseudonyms. Nevertheless, longer silent periods may not be suitable for VANETs since life-critical safety applications require frequent exchange of safety messages in the neighbourhood. Hence, the length of the silent period is bounded by the interval of safety messages, which causes the trade off between privacy and safety of the vehicle.

AMOEBA [19-20] also uses extended random silent periods for changing pseudonyms. With this method, only a selected set of member vehicles actively participate in data probing and other applications. Since the safety application requires frequent information from all neighbouring vehicles for higher accuracy of the life-critical situations, this method is not suitable for safety and cooperative driving applications other than data probing and online services. Moreover, with this method, group members cannot directly communicate with non-member vehicles in the neighbourhood, so that critical safety applications may not be possible in the neighbourhood. More importantly, the deactivated transceivers in any vehicle are not suitable for any life-critical safety applications in VANETs.

The work done in Buttyan et al. [42] is an implicit combination of MIX zones and silent periods, which inherits drawbacks of both of the schemes. Furthermore, even with the lower speeds, silent periods are not recommended in road junctions since auto accidents are frequent in junctions.

Zhang et al. [31] used encrypted communications to protect the privacy of vehicles. Each vehicle uses a unique symmetric session key acquired from a RSU in the neighbourhood for its communications within the neighbourhood. Since each vehicle shares its session key

only with the neighbouring RSU, all the messages coming from the neighbouring vehicles can only be authenticated and verified by the RSU. Therefore, the RSU has to periodically distribute the validity information of all received messages over the neighbourhood. Since a vehicle cannot authenticate receiving messages itself and has to wait for verifications from the RSU, this method is not suitable for real-time, life-critical safety applications.

The REP protocol proposed in [32] focuses on protecting location privacy only under the Global Passive Adversaries. Since the time period between two consecutive pseudonyms is extremely small, the local adversaries who are tracking the vehicle movements can link two successive pseudonyms by using spatial and temporal relationships between these two pseudonyms. Even though a vehicle changes its pseudonym in a dense zone, this method cannot provide any privacy enhancement unless other vehicles change their pseudonyms at the same time.

In addition, to preserve the anonymity and unlinkabilty in VANETs, complete group signature based protocols such as GSIS [14] and hybrid methods [38] have been proposed. Even though group signature methods successfully provide unlinkability among different messages of the same vehicle, higher computational cost of revoking malicious vehicles makes these protocols not suitable for large scale mobile networks like VANETs. With the group signatures, every non-malicious member has to recalculate group parameters at each of the revocation to avoid malicious members. Since efficient and accurate revocation cannot be achieved with large number of vehicles, long-term group management is not feasible in VANETs. Moreover, changing pseudonyms individually may not avoid movement tracking of a vehicle since adversaries can simply link a new pseudonym to the previous pseudonym if no one else changes its pseudonym. As a consequence, most of these protocols assume that at least one more vehicle is also changing its pseudonym within the same period. But the dynamic nature of VANETs may not guarantee this assumption.

IX. CONCLUSIONS

In this paper, the problem of location tracking in VANETs was addressed. Considering the unique characteristics of VANETs, a group based pseudonym changing protocol is proposed to enhance the location privacy in VANETs. By joining to a group, vehicles can change the spatial and temporal properties of two successive positions of the vehicles that significantly reduce the ability to linking two successive pseudonym identifiers by the adversary. Since this method does not use any kind of silent periods, it can be applied in both safety communication and online service access scenarios without affecting the required level of safety. Performance evaluation and comparison showed that the proposed method provides significantly higher level of privacy over the silent period approach. Furthermore, it showed that the proposed protocol can be used with different mobility scenarios and different vehicular densities. The evaluation results further indicate that this protocol can be efficiently used with a wide range of parameters, such as group radius and group lifetime.

REFERENCES

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

[2] 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.

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

[4] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc neworks," in Proc. of the ACM Workshop on Security of Ad hoc and Sensor Networks (SASN), 2005, pp. 11– 21.

[5] M. Raya and J-P. Hubaux. "Securing Vehicular Ad Hoc Networks", *Journal of Computer Security*, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, No. 1, pp. 39 - 68, 2007.

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

[7] 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, pp. 31–42, 2003,

[8] 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, Sep 2002.

[9] 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, 2003.

[10] ITS probe vehicle techniques.[Online]. Available:http://tti.tamu.edu/documents/FHWA-PL-98-035 c5.pdf.

[11] 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 (ESASpp. pp.43–57,), 2006,

[12] M. Raya, A. Aziz and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in Proc. of the 3rd international workshop on Vehicular Ad hoc Networks (VANET), pp. 67–75, 2006.

[13] Chun-Ta Li, Min-Shiang Hwang and Yen-Ping Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Journal of computer Communication*, article in press.

[14] X. Lin, X. Sun, P.-H. Ho and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE Transactions on Vehicular Technology*," Vol. 56, No. 6, pp. 3442-3456, 2007.

[15] A. R. Beresford, "Location privacy in ubiquitous computing," Ph.D. dissertation, University of Cambridge, 2004.

[16] 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), pp. 1187–1192, 2005.

[17] L. Huang, K. Matsuura, H. Yamane and K. Sezaki, "Towards modeling wireless location privacy," in Proc. of the Workshop on Privacy Enhancing Technologies (PET), pp. 59–77, 2005.

[18] J. Freudiger, M. Raya and M. Felegyhazi, "Mix-Zones for location privacy in vehicular networks", WiN-ITS 2007, Vancouver, Canada.

[19] 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.

[20] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET", IEEE Journal on *Selected Areas in communications* Vol. 25, No. 8, pp. 1569-1589, 2007.

[21] D. Chaum, “The dining cryptographers problem: Unconditional sender and recipient untraceability,” *Journal of Cryptology*, Vol. 1, pp. 65–75, 1988.
[22] A. Pfitzmann and M. Waidner, “Networks without user observability – design options,” in Advances in Cryptology – EUROCRYPT’85. Springer-Verlag, LNCS 219, pp. 245–253.
[23] A. Serjantov and G. Danezis, “Towards an information theoretic metric for anonymity,” in Proc. of the Workshop on Privacy Enhancing Technologies (PET), pp. 41–53, 2002.
[24] F.L Mannering, W. P. Kilareski and S. S. Washburn, “Principles of Highway Engineering and Traffic Analysis, 3rd Ed, Wiley Publishers, 2004.
[25] A. M. Mathai, An Introduction to Geometrical Probability: Distributional Aspects with Applications. CRC Press, 1999.
[26] The Network Simulator - NS-2. [Online], Available: http://www.isi.edu/nsnam/ns/.
[27] Mobility Generator Framework [Online], Available: http://gmsf.hypert.net/
[28] D. Boneh, X. Boyen and H. Shacham, “Short group signature” in Proc.*Advances in Cryptography* – Crypto’04, ser. LNCS, Vol. 3152, Springer-Verlag, pp. 41-55.
[29] IEEE 1609.2: Trial-Use Standards for Wireless Access in Vehicular Environments (WAVE)-Security, 2016.
[30] R. Lu, X. Lin, H. Zhu, P. -H. Ho and X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications”, in proceedings *of the IEEE* INFOCOM *2008.*
[31] C. Zhang, X. Lin, R. Lu, P. -H. Ho and X. Shen, “An Efficient Message Authentication Scheme for Vehicular Communications”, *IEEE transactions on vehicular technology*, Vol. 57, No. 6, Nov 2008.
[32] A. Wasef and X. Shen, “REP: Location Privacy for VANETs using random encryption periods”, *Springer-Mobile Networks and Applications*, Vol. 15, No. 1, pp. 172-185, Feb. 2010.
[33] J. H. Song, V. W. S. Wong and V. C. M, Leung, “Wireless location privacy protection in vehicular ad hoc networks”, *Springer-Mobile Networks and Applications*, Vol. 15, No. 1, pp. 160-171, Feb. 2010.
[34] G. Yvonne, W. Bernhard and G. H. Peter, “Medium Access Concept for VANETs Based on Clustering”, in the 66th IEEE VTC, pp. 2189-2193, 2007.
[35] P. Fan, “Improving Broadcasting Performance by Clustering with Stability for Inter-vehicle Communication”, in Proceedings of the 65th IEEE VTC, Dublin, Ireland, 2007.
[36] W. Zhiagang, L. Lichuan, Z. MengChu and A. Nirwan, “A Position-Based Clustering Technique for Ad Hoc Intervehicle Communication,” *IEEE transactions on Man and Cybernetics*, Vol.38, No.2, Mar 2008.
[37] Z. Y. Rawashdeh and S. M. Mahmud, “Toward Strongly Connected Clustering Structure in Vehicular Ad Hoc Networks”, in Proceedings of the 70th IEEE VTC, Alaska, USA, 2009.
[38] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” In *Proceedings of the ACM* VANET '07 Montreal, Canada, 2007.
[39] S. Ahren, E. Shi, F. Bai and A. Perrig. "TACKing Together Efficient Authentication Revocation, and Privacy in VANETs," in Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009, Rome, Italy.
[40] E. Fonseca, A. Festag, R. Baldessari and R. Aguiar, “Support of annonymity in VANETs- Putting pseudonymity into practice”, In Proc of IEEE WCNC, Hong Kong, 2007.
[41] L. Buttyan and T. Holczer and I. Vajda, “On the effectiveness of changing pseudonyms to provide location privacy in VANETs”, InProc of European workshop on security and privacy in ad hoc and sensor networks (ESAS), Cambridge, 2007.
[42] L. Buttyán, T. Holczer, A. Weimerskirch and W. Whyte, “SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs,” IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 2009.
[43] IEEE P802.11p TM/D3.0 Draft Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and metropolitan area networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
[44] Intellidriveusa [Online], Available: http://www.intellidriveusa.org/documents/052009-Technical Description.pdf
[45] B. Wiedersheim, Z. Ma, F. Kargl and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in Proc. 7th International Conference on wireless On-demand Network Systems and Services (WONS'10), pp. 176-183, 2010.
[46] M. Gruteser and B. Hoh. “On the anonymity of periodic location samples In Security,” in Pervasive Computing 2005, pp. 179–192.
[47] L. Fischer, S. Katzenbeisser and C. Eckert, ‘‘Measuring unlinkability revisited,” In WPES ’08: Proc. ACM workshop on Privacy in the electronic society, October 2008.
[48] Z. Ma, F. Kargl and M. Weber, ,‘‘A location privacy metric for v2x communication systems,” In IEEE Sarnoff Symposium, Princeton, USA, Mar 2009.
[49] Hesiri Weerasinghe, Huirong Fu, “ESAP: Efficient and Scalable Authentication Protocol for Vehicular Ad hoc Networks,” in Proceedings of the IEEE Globecom 2010, pp. 1786-1791, Miami, Florida, Dec 2010.