Providing location privacy for online services in vehicular ad hoc networks

Hesiri Weerasinghe*

Department of Computer Systems Engineering,
University of Kelaniya, Sri Lanka
Email: hesiri@kln.ac.lk
*Corresponding author

Huirong Fu

Department of Computer Science and Engineering,
Oakland University,
Rochester, MI, USA
Email: fu@kln.ac.lk

Abstract: Communications through road side units in vehicular ad hoc networks (VANETs) can be used to track the location of vehicles, which makes serious threat on users' privacy. In this paper, we address the problem of location tracking for online service access and the privacy enhancement in VANETs. Firstly, by considering the unique characteristics of VANETs, we propose an anonymous online service access (AOSA) protocol. Secondly, we analytically evaluate the anonymity and the unlinkability of the proposed protocol. Finally, a series of simulation studies are conducted to evaluate the performance of our protocol in the real VANET environments such as Manhattan and urban scenarios. According to analytical evaluation and simulations, our protocol provides higher level of anonymity and location privacy by providing larger anonymity set and smaller tracking probability for online service access applications. Simulation results further show that our protocol is feasible and produce better performance in real VANET environments by producing higher success ratio and smaller delay.

Keywords: vehicular ad hoc network; VANET; privacy; anonymity; pseudonyms; certificate authority.

Reference to this paper should be made as follows: Weerasinghe, H. and Fu, H. (2019) 'Providing location privacy for online services in vehicular ad hoc networks', *Int. J. Forensic Software Engineering*, Vol. 1, No. 1, pp.91–114.

Biographical notes: Hesiri Weerasinghe is currently a Senior Lecturer in Computer Science at Department of Computer Systems Engineering, University of Kelaniya, Sri Lanka. He received his PhD and MSc in Computer Science and Engineering from Oakland University, Michigan, USA in 2011 and 2007, respectively and his BSc in Mathematics from University of Kelaniya of Sri Lanka in 2000. His research interests include security and privacy of vehicular networks, network security, mobile ad-hoc networks and communication networks.

Huirong Fu is a Professor in the Department of Computer Science and Engineering, Oakland University, USA. She joined Oakland University as an Assistant Professor in 2005. Previously, she has been working as an Assistant Professor at North Dakota State University for three years and as a Post-Doctoral Research Fellow at Rice University for more than two years. As a lead Professor and the principal investigator in several projects funded by the NSF, she has been actively conducting research in the area of information security. Her primary research interests are in information assurance and security, networks, internet data centres, and multimedia system and services.

1 Introduction

Vehicular ad hoc networks (VANETs) were proposed to enhance vehicular safety, improve traffic managements and facilitate other online service access from vehicles. These VANETs consists of vehicles with on board units (OBUs), road side units (RSUs) and administrative and service providing servers that are connected to RSUs with wired channels. By using vehicle to vehicle (V2V) communication and vehicle to infrastructure (V2I) communication, vehicles and service providers exchange required data and information for safety management, traffic management and other online service applications. In spite of the tremendous ongoing academic and industrial research efforts on VANETs, there are a lot of open issues on security and privacy to be addressed (Zarki et al., 2002; Hubaux et al., 2004; Raya and Hubaux, 2005a, 2005b, 2007; Dotzer, 2005).

Recently, researchers are working to develop security protocols for VANETs. Several security and privacy issues in VANETs are studied in Zarki et al. (2002). Architecture to handle the security and privacy of VANETs was presented in Hubaux et al. (2004) and Raya and Hubaux (2005a). Raya and Hubaux (2005b) suggested changing pseudonym identifiers frequently to provide anonymous communication in VANETs, and changing these pseudonyms upon the change of vehicle's direction. Further, the effect of frequently changing keys and pseudonyms as well as other security issues are analysed in Dotzer (2005) and Schoch et al. (2006). Li et al. (in press) and Lin et al. (2007) specifically proposed privacy preserving key management protocols for VANET to provide anonymous communication. However, none of the above works studies the location privacy when vehicles access other online services.

If an intruder can track a vehicle's location continuously for some time, he/she can collect a lot of information about the vehicle or the users such as travelling behaviours, frequently visiting places, etc. Particularly, if the driving history of the vehicle associates with other regional information such as maps, an adversary can simply find out the personal interests of the users. Furthermore, this private information can be abused for lots of illegal activities such as kidnappings or vehicle hijackings (Raya and Hubaux, 2007; Dotzer, 2005). Location tracking of vehicles is also helpful to find out the applications or other online services that are accessed by the vehicles. To improve the unlinkability between travelling locations of vehicles, the randomly changing pseudonym identifiers and keys are proposed in Raya and Hubaux (2005b, 2007).

The use of online services or sending data through RSUs can directly affect the privacy and anonymity of users. An entity has to be authenticated through online authorities and other network entities when it accesses any services. Further, some online

services may require accurate information of current location of the vehicle to provide their services successfully. Therefore, off-the-road entities such as service providers, authorities, even adversaries can trace back to the sender, and consequently, they can find out the location that may expose the identity of the vehicle with its consecutive locations. Most of the drivers do not want to expose their privacy information even to the authorities although these authorities are trusted (Raya and Hubaux, 2007). Location information should not be exposed to registration authority (RA) since it can be used to find the real identities of a pseudonym identifier. Any protocol should not allow RA to find out the real identifiers of the message sender except to solve the liability issues like an accident.

Based on the k-anonymity in which any entity in a system is indistinguishable from $k - 1$ other entities, the protocols proposed in Gruteser and Grunwald (2003) and Gedik and Lu (2005) preserve the privacy of probe data collection in mobile networks. Since those applications significantly modified the temporal and spatial information at the gateway, these protocols do not meet the accuracy requirements of the VANETs. Further, the protocols in Gruteser and Grunwald (2003), Gedik and Lu (2005) and Hoh et al. (2007) do not consider the sender authentication, and gateway can access all the real information from users. The protocol proposed in Hoh and Gruteser (2005) and Beresford and Stajano (2003) provide higher accuracy of collected data but it cannot provide higher level of privacy in a network with low user densities. The protocol in Li et al. (in press) performs anonymous communication for VANETs, however it does not prevent location tracking when vehicle access online services, since service provider can link two requests from the same vehicle. With the protocol in Lin et al. (2007), all vehicles have the same level of rights and the personalised services cannot be used for different vehicles. The service access protocol proposed by Sampigethaya et al. (2005) intends to prevent location linking uses online RA for authorising all the service access sessions. The online RA has to verify all service requests and a session key will be issued for each application session. Moreover, this gives the RA an ability of tracking all the service users all the time.

The major contribution of this paper is threefold. First, we propose an anonymous service access protocol that is based on the concept of forming groups among neighbouring vehicles. Second, we analytically evaluate the anonymity and unlinkability of the proposed protocols. Finally, a series of simulation studies are conducted to evaluate the performance of the proposed anonymous online service access (AOSA) protocols in the real VANET environments, such as Manhattan and urban scenarios.

The main advantages of our work are:

1 vehicles can anonymously access any services without exposing its real identity

2 forming groups and accessing services through group leader prevents trace backs to the sender

3 because of the use of common group identifiers within a group, this method enhances the location privacy and unlinkability of online service access

4 verification and vehicle authentication in online service access can be done without involving any authorities

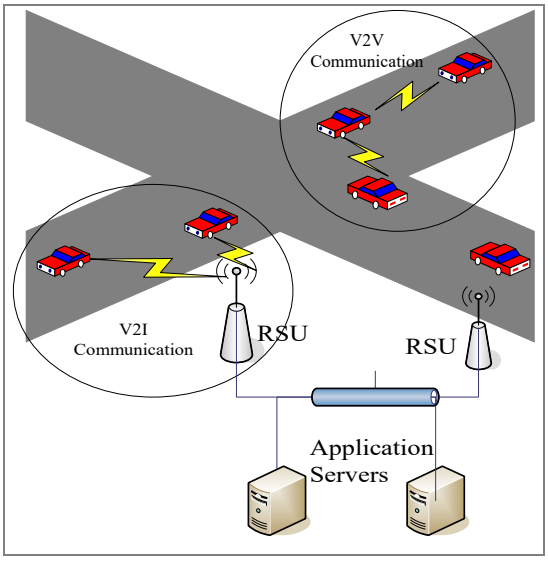
5 since group members use group public key to communicate with other vehicles, our group method can also be used in safety related V2V applications.

The rest of the paper is organised as follows. Section 2 introduces the system model. Section 3 presents the proposed AOSA protocol. Section 4 discusses the security and privacy of AOSA. Section 5 describes the performance evaluation metrics for anonymity and unlinkability in VANETs. Then, Section 6 develops an analytical method for evaluating the anonymity and unlinkability of the proposed methods. Section 7 presents the simulation experiments and performance analysis. Finally, Section 8 concludes this paper.

2 System model

As shown in Figure 1, vehicles in a VANET are equipped with an OBU for all the data processing, radio equipments for the communication with other OBUs and RSUs, sensors and other data collecting devices and storage devices. All the V2V communications are happening directly among OBUs and all V2I communications are going through the RSUs. RSUs are physically connected to other VANET components such as administrative servers, location servers and other application servers by a wired network. Further, RA provides registration services for both vehicles and service providers. All the security related credentials and processing such as certification, authentication, and authorisation services are handled by this trusted RA.

Figure 1 V2V and V2I communication scenarios (see online version for colours)



A suitable public key infrastructure (PKI) needs to be implemented in the VANET and the RA may also work as a certification authority (CA) for the PKI. All the vehicles and service providers need to contact the RA in a secure channel (offline) and register before entering the VANET operations. During the offline registration, each vehicle is assigned a unique identification number and a unique public/private key pair with a public key certificate signed by the RA/CA. In addition, each vehicle should be facilitated for

frequently changing pseudonym identifiers and keys. This can be done by using an offline pre-loaded set of certified pseudonym identifiers and keys (Raya and Hubaux, 2005b, 2007). With this method, each vehicle is pre-loaded with a large set of pseudonym identifiers, public/private key pair and a public key certificate for each pseudonym identifier. CA keeps a record for each vehicle with the set of all pseudonym identifiers. Each vehicle is able to change its pseudonym credentials by using the above method. Furthermore, each vehicle has the ability to verify the certificates and the signatures signed by other vehicles or any authority.

Our protocol can be used with all typical VANET applications and services such as safety messages distribution, vehicle data dissemination applications, traffic management and other online services. The first type of applications uses V2V communications while the others use V2I communications. Data dissemination applications are used by the authorities or other service providers to collect road and traffic related information to distribute this information to people who may require or have interest in the information. Vehicles send collected information to specific application servers through RSUs periodically or with the request of the service providers. Other online services may be any of the road services that can be accessed through RSUs while vehicles driving. In each of these applications, all messages should include necessary information for sender authentication such as signatures, public keys and certificates.

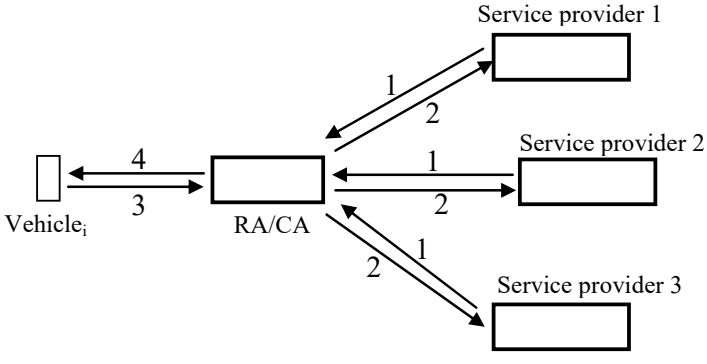
3 AOSA protocol

In this section, we propose the AOSA protocol to enhance location privacy in VANETs. The main goal of this proposed protocol is to mitigate the location tracking of vehicles by the adversaries, service providers or the authorities when the vehicles access online services through RSU. To protect the location privacy of vehicles that are accessing online services through RSUs, some kind of unlinkability between vehicles and the accessed applications has to be provided. (Here, the unlinkability is defined as the zero relationship between the applications and the sender). To achieve this goal, the vehicle should be able to anonymously access applications through RSUs, and no one is able to find any relationship between two service access communications from the same vehicle with different locations. This protocol applies the system model described in Section 2. Each vehicle registers with the RA and obtains pseudonym identities.

3.1 The procedure of AOSA

Figure 2 shows the procedure of the AOSA protocol, which consists of two phases. As shown in Figure 2(a), in the first phase, all service providers need to register with the RA. The vehicles that want to use online services should also register for the services through RA. Except for the pseudonym information, the information of registered vehicles for each service is forwarded to the service provider. When the RA/CA issues pseudonym public/private keys, the public key certificates should include the information about all the registered services and the blind signatures from service providers that the vehicle is currently registered. Each service information is encrypted with the service provider's public key. Consequently, each service provider can only access to its own information.

Figure 2 Aosa protocol, (a) phase 1: service provider and vehicle registration (b) phase 2: online service access protocol



(a)

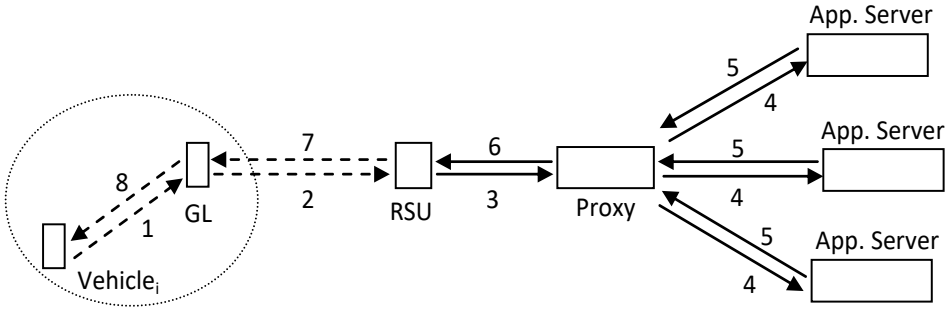
Notes: (a) Steps:

1 Service providers send their credentials to the RA/CA for registration (registration request).
2 RA/CA issues public/private keys and public key certificate to the service providers.
3 Each vehicle sends its credentials to RA/CA for registration. This request includes all other service requests from third party service providers.
4 RA issues a set of anonymous public/private key pairs with certificate for each public key. The RA signs these certificates including all service information that the vehicle registered/authorised.

(b) Steps:

1 Vehicle sends service request signed using current pseudonym. The whole request message is encrypted with service provider's public key and then encrypted with the group secret key.
2 Group leader decrypts the message with the group secret key. The request is signed with group private key, and then it is forwarded with leader's certificate issued by RA to RSU.
3 RSU forwards the message to the proxy server.
4 Proxy server verifies the group leader's credentials and forwards the service request to the desired application server.
5 Service provider decrypts the message with its private key, then it verifies the vehicle's credentials using vehicle's certificate and RA's public key. Service provider verifies the vehicle's authority for the service by using vehicles certificate and service providers private key. Then service provider sends required parameters for session key establishment between the vehicle and service provider. This message is first encrypted with vehicles pseudonymous public key and then encrypted with group leader's public key.
6 Proxy server verifies the service provider's credentials and forwards the message to the RSU.
7 RSU forwards the reply message to the group leader.
8 Group leader decrypts the message and forwards it to the vehicle encrypted with group secret key. Vehicle decrypts the data from service provider and generates session key for the application session.

Figure 2 AOSA protocol, (a) phase 1: service provider and vehicle registration (b) phase 2: online service access protocol (continued)



(b)

Notes: (a) Steps:

1 Service providers send their credentials to the RA/CA for registration (registration request).
2 RA/CA issues public/private keys and public key certificate to the service providers.
3 Each vehicle sends its credentials to RA/CA for registration. This request includes all other service requests from third party service providers.
4 RA issues a set of anonymous public/private key pairs with certificate for each public key. The RA signs these certificates including all service information that the vehicle registered/authorised.

(b) Steps:

1 Vehicle sends service request signed using current pseudonym. The whole request message is encrypted with service provider's public key and then encrypted with the group secret key.
2 Group leader decrypts the message with the group secret key. The request is signed with group private key, and then it is forwarded with leader's certificate issued by RA to RSU.
3 RSU forwards the message to the proxy server.
4 Proxy server verifies the group leader's credentials and forwards the service request to the desired application server.
5 Service provider decrypts the message with its private key, then it verifies the vehicle's credentials using vehicle's certificate and RA's public key. Service provider verifies the vehicle's authority for the service by using vehicles certificate and service providers private key. Then service provider sends required parameters for session key establishment between the vehicle and service provider. This message is first encrypted with vehicles pseudonymous public key and then encrypted with group leader's public key.
6 Proxy server verifies the service provider's credentials and forwards the message to the RSU.
7 RSU forwards the reply message to the group leader.
8 Group leader decrypts the message and forwards it to the vehicle encrypted with group secret key. Vehicle decrypts the data from service provider and generates session key for the application session.

In our protocol, vehicles dynamically form groups by using a similar method like Sampigethaya et al. (2005) and use short group signature method (Boneh et al., 2004) to handle all the group keys and signatures. The detailed descriptions of group forming and group management are out of focus of this work. All the non-member vehicles listen to group leader notifications in the neighbourhood. If there is an existing group in the vicinity, the vehicle joins the group as a new member after verifying the validity of the group leader. Otherwise, the vehicle can initiate forming a new group and become the leader of the newly formed group. Further, the leader of the new group should provide its security credentials to authenticate itself to new members. All group members share a common group public key, and each member vehicle has a unique secret key that can be used with the common group public key. Further, all members share a set of common temporary identifiers. Two signatures from a same vehicle cannot be linked together (Boneh et al., 2004). However, the group leader and the RA can collaborate to find out the real identity of the signer. Member vehicles except group leader do not use real identification or pseudonym identifications and relevant public/private keys to sign broadcast messages. All the notations used in the following section are given in Table 1.

Table 1 Notations used in this paper

Symbol	*Notation*
V_i	Arbitrary vehicle
RA	Registration authority
CA	Certification authority
RSU_i	Arbitrary road side unit
PuK_E	Public key of the entity E
PvK_E	Private key of the entity E
GsK_E	Group secret key of the entity E
PuK_{GP}	Group public key
$Sig_E()$	Signature produced by E
$Cert_E()$	Certificate issued by entity E
PID_i	i^{th} pseudonym identifier
SID	Service provider's identity
$SK_{A,B}$	Session key between A and B
$SerREQ$	Service request

Basic steps of the second phase of the AOSA protocol are described in Figure 2(b). When a vehicle needs to access the service, it sends a service request, *SerREQ*, through the group leader. In step 1, the request message should be signed by the vehicle using its current pseudonym identifier and includes the public key certificate, $Cert_{CA}(PuK_V)$, issued by the CA. This request message is first encrypted with the service provider's public key, PuK_{SP}, then it is encrypted with the group secret key, GsK_V, by the source vehicle. This message M is constructed as follows:

$$M = Enc_{GsK_V}(SID \mid REQ)$$

where

$$REQ = Enc_{PuK_{SP}}\left(SerREQ, Sig_{PvK_V}(SerREQ), PID, PuK_V, Cert_{CA}(PuK_V)\right).$$

Then the message M is forwarded to the group leader.

In step 2, group leader decrypts the message and adds its signature $Sig_{GsK_{GL}}(REQ)$ and the group public key certificate $Cert_{CA}(PuK_{GP})$ to the new message M' and forwards it to the proxy through RSU after mixing with other requests. The massage M' is constructed as follows:

$$M' = \left(REQ, SID, Sig_{GsK_{GL}}(REQ), Cert_{CA}\left(PuK_{GP}\right), Loc_{GL}\right)$$

where Loc_{GL} is the location of the group leader.

In step 3, the RSU forwards the message to the proxy server. In step 4, the proxy server verifies the group leader's certificate and forwards the request, REQ, to the requested service provider. Proxy also keeps a record of the forwarded RSU's location for reply purposes. Only if the request is sent for location-based service, the location information of the RSU is forwarded to the service provider. Because the real identifier of the vehicle is concealed to the service provider and the pseudonym is used only once, this information is not a threat to the location privacy.

After receiving the service request, service provider decrypts the message with its private key, PvK_{SP}, then it verifies the vehicles pseudo credentials using vehicles certificate, $Cert_{CA}(PuK_V)$ and CA's public key, PuK_{CA}. Finally service provider verifies the vehicles authorisation for the service using the vehicle's certificate and service provider's private key.

In step 5, the service provider sends the session key, $SK_{SP,V}$ to share between the vehicle and service provider for new service session. This message is first encrypted with the vehicle's pseudonymous public key and then encrypted with the group leader's public key. The response message R is constructed as follows:

$$R = \left(Enc_{PuK\ GP}(REP) \mid GID\right)$$

where

$$REP = Enc_{PuK_V}\left(SK_{SP,V}, ts, Sig_{PvK_{SP}}(SK \mid ts)\right).$$

In step 6, proxy server forwards the reply message, $Enc_{PuK_{GP}}(REP)$ to the RSU. In step 7, the RSU forwards the reply message to the group leader. Then in step 8, the group leader forwards this response message to the vehicle. Only the specified vehicle is able to read the service provider's response by using its pseudo private key. Then the rest of the communications between service provider and the vehicle are encrypted with the shared session key, $SK_{SP,V}$, and all the messages are going through the group leader.

3.2 Implementation specific details

When a vehicle starts to drive, it starts to broadcast beacon messages continuously in every *beacon interval*. At the same time, it is participating in all the safety and other cooperative driving applications as required. All of these messages are signed using pseudo keys and the certificate of the public key is attached. All the group leaders also broadcast the leader notification messages in every *beacon interval*. If a non-member

vehicle receives a leader notification from its neighbourhood, it replies with a join request only if the distance from the leader is less than the *group radius*. This request should include all the credentials to authenticate the vehicle to the leader. Upon receiving a join request, a vehicle will be authenticated by the leader and the acceptance notice will be sent to the new member with all group parameters encrypted with the member's current keys. Then the new member starts to use common group parameters that are shared by all the group members. All the service access and probe data messages are sent through the group leader. All the safety and other cooperative driving messages are broadcasted using group credentials and vehicles not in the same group can also authenticate the sender using group public key and its certificate.

If any new vehicle does not receive leader notification message for a *threshold* time, the new vehicle forms a group as a group leader and provides its current pseudo credentials to the RA to acquire required group credentials. Then it starts to broadcast leader notification messages in the neighbourhood.

After joining a group, a member always updates the leader notification from the leader and if the member does not hear from the leader for a *threshold* time the leader is considered as out of range and then the member vehicle removes all group parameters and starts to function as an individual vehicle. Group leader also updates the member beacon. If the leader does not hear from the member for a *threshold* time, the member is considered as out of range and all the information about this member will be removed.

4 Security and privacy of AOSA

In the proposed protocol, vehicles will join an existing group only after the group leader is verified by using the group leader's public key certificate issued by the CA. Hence, any malicious vehicle that does not have valid public key certificates could not form a group as a group leader. Moreover, malicious vehicle cannot join an existing group without having a valid certificate from the CA.

Further, since the service request message is encrypted with service provider's public key, none of the details are exposed to others except the intended service provider. Group leader and the proxy are only forwarding the original service request. No one else can impersonate the vehicle or change the original message since the digital signature of the sender is included in each request message. This means the proposed AOSA protocol provides confidentiality, authentication, message integrity and non-repudiation for online service access.

Since the service provider encrypts the reply message with the vehicles' pseudo public key, the shred session key is only available for the intended vehicle. Consequently, the secure shared session key provides confidential communication for the entire session. The proposed protocol does not use online authorities for service authorisation verification to prevent location exposes of the drivers to authorities. More importantly, since RA/CA contains the real identities for the pseudonyms of all vehicles, exposing the location to RA/CA is not recommended.

Since all the group members use common pool of identifiers and same group public key, outsiders cannot differentiate different messages from different vehicle, thus it preserves the *k*-anonymity. Furthermore, since all the service messages are going through

the group leader and the group leader mixes all request messages before forwarding them, our protocol prevents the ability of trace-backs to the sender by any adversary.

Since the vehicle's pseudo public key certificate issued by RA/CA contains all the information about the level of service authorisation, the actual identity of the vehicle is not exposed to the service provider. Hence, it prevents any type of possible location tracking by the service providers. Further, the proxy server only identifies the group leader's location, but not the location or the identification details of the source vehicle. The service provider only identifies the pseudonym of the sender, but not the location information of the sender or the group leader.

5 Performance evaluation metrics

Adversaries can use the relationships among a sequence of messages from the same pseudonym identifier to track a vehicle's movement. According to Huang et al. (2005), trajectory T_i for pseudo identifier i can be defined as a series of actions with the same sender identity i. These trajectories are associated with each pseudonym identifier but not with each vehicle. Since each vehicle uses different pseudo identifiers over time, actions of a vehicle belong to several trajectories according to pseudo identifiers. With the AOSA protocol, since all the member vehicles in a group share the group number as its identity, all actions executed by group members belong to the same trajectory with the group number.

Let $p(i, j) \in P$ be the probability of correlating two trajectories T_i and T_j on the source of actions (Huang et al., 2005). Then for each pseudonym identifier i, we have.

$$\sum_{j \in ID} p(i, j) = 1$$

To evaluate the proposed protocol, we define five performance metrics as follows.

Definition 5.1 (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:

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

It means that AS_i includes all pseudonym identifiers whose trajectory may be equivalent to T_i. Then we define the size of AS_i, as $|AS_i|$, which is a measure of location privacy for pseudonym identifier i (Huang et al., 2005).

Definition 5.2 (Entropy of an anonymity set): The entropy H_i of the anonymity set AS_i, can be defined as:

$$H_i = -\sum_{j \in AS_i} p(i, j) \log_2 \left(p(i, j) \right) \tag{2}$$

This represents the level of uncertainty of the relationship between two trajectories T_i and T_j (Huang et al., 2005).

Definition 5.3 (Tracking probability): The tracking probability Pt_i of a target i can be defined as:

$$Pt_i = P\left(\left|AS_i\right| = 1\right) \tag{3}$$

This is the probability of the size of the anonymity set is equal to one, which means that the anonymity set of an target only contains the target itself.

Definition 5.4 (Average service response time): To measure the protocol overhead of the anonymous service access protocol, we will measure the average service response time *Ds*. This is the round trip delay between the time when a group member sends its service request and the time when the group member receives the first reply from the service provider. This round trip time includes all the delays introduced by the new protocol such as processing at the group leader. By measuring the average service access time, we can evaluate the delay overhead introduced by the protocol, i.e.,

$$Ds = \frac{1}{|G|}\sum_{i=1}^{|G|}\left(\frac{1}{Nr_i}\sum_{j=1}^{Nr_i} RTT_{i,j}\right)$$

where $|G|$ is the number of group members, Nr_i is the number of service requests sent by member i, and $RTT_{i,j}$ is the round trip time of the j^{th} request made by vehicle i.

Definition 5.5 (Success ratio of service access): Due to high mobility of VANETs, continuous availability of the services may not be possible. Sometimes, a vehicle may not be available when the reply comes from the service provider if the round trip time is high. To evaluate the availability of the proposed protocol, success ratio of the service access Sr can be measured. This is defined as the ratio of the number of received service replies over the total number of service requests, i.e.,

$$\text{Sr} = \frac{\text{Total number of received service replies}}{\text{Total number of service requests}}$$

6 Theoretical analysis

In the online service access scenario, the target of an adversary is the sender (source) of an application message. The main goals of our AOSA protocol are:

1 to hide the real identity of the sender of a message when vehicles access the authorised services

2 to unlink the vehicles and the ongoing messages from the group leader.

To evaluate the level of anonymity and the unlinkability of the anonymous service access protocol, we use the performance evaluation metrics in terms of tracking success ratio, the size of the anonymity set and the entropy of the anonymity set. Additionally, to evaluate the performance of the anonymous service access protocol, we introduce other metrics such as average service response time, service access success ratio.

Since all the vehicles use group parameters as their identifications, the attacker can only find the number of ongoing application requests from the groups. Hence, according to equation (1), the anonymity set for a target i, the sender of an application request in the anonymous service access protocol, include all the members of the group that the vehicle i belongs. So, the size of the anonymity set, $|AS_i|$, is defined as:

$|AS_i|$ = Number of group members who send application requests through group leader with the source i

The attacker can find the number of application requests going through group leader, but they are unable to find who sends the application request. If the number of vehicles requesting application is k, then the probability of choosing k member vehicles from the group is binomially distributed over the total member vehicles in the group. Since all the member vehicles in the group have equal probabilities to be a sender, if the total members in the group $|G|$ are n, then the probability of selecting one member vehicle as a sender is $1/n$.

6.1 Tracking probability

Theorem 6.1 (Tracking probability of a vehicle): Tracking probability Pt_i of a vehicle i of an application request in the anonymous service access protocol is:

$$Pt_i = 1 - \sum_{k=1}^{N} \left(\sum_{n=k}^{N} \binom{n}{k} \left(\frac{1}{n}\right)^k \left(1 - \frac{1}{n}\right)^{(n-k)} \times p_n \right) \tag{4}$$

where k is the number of pseudonym identifiers in the anonymity set, and n is the number of vehicles in the group. The probability p_n is the probability of having n member vehicles in the group. N is the maximum possible vehicles in a group.

Proof: The tracking probability Pt_i of a sender i of a request in anonymous service access can be defined as:

$$\begin{aligned} Pt_i &= P(|AS_i| = 1) \\ &= 1 - P(|AS_i| > 1) \\ &= 1 - \sum_{k=2}^{N} P(|AS_i| = k) \end{aligned}$$

If only k number of vehicles send the service requests, then the anonymity set of any target contains only k vehicles. The probability of having k vehicles in the anonymity set given that the group has n members is:

$$P(|AS_i| = k) = P(|AS_i| = k \,\|\, G_i \,| = n) \times p_n$$

where $|G_i|$ is the total number of group members in the group that sender i belong to. Also, n varies from k to N. Then we have:

$$\begin{aligned} Pt_i &= 1 - \sum_{k=2}^{N} \left(\sum_{n=k}^{N} P(|AS_i| = k \| G_i| = n) \times p_n \right) \\ &= 1 - \sum_{k=2}^{N} \left(\sum_{n=k}^{N} \binom{n}{k} \left(\frac{1}{n}\right)^k \left(1 - \frac{1}{n}\right)^{(n-k)} \times p_n \right). \end{aligned}$$

□

6.2 Size of the anonymity set

Theorem 6.2 (Expected size of the anonymity set): The expected size of the anonymity set of a sender i of an application request in the anonymous service access protocol is:

$$E\left(|AS_i|\right) = \sum_{k=1}^{N} k \left(\sum_{n=k}^{N} \binom{n}{k} \left(\frac{1}{n}\right)^k \left(1-\frac{1}{n}\right)^{(n-k)} \times p_n \right) \tag{5}$$

where all the parameters are same as those defined in Theorem 5.1.

Proof: The expected value of the size of the anonymity set for the anonymous service access can be defined as:

$$E\left(|AS_i|\right) = \sum_{k=1}^{N} k \times P\left(|AS_i| = k\right).$$

With the probability of having k vehicles in the anonymity set when the group has n members, we have:

$$\begin{aligned} E\left(|AS_i|\right) &= \sum_{k=1}^{N} k \left(\sum_{n=k}^{N} P\left(|AS_i| = k \,\|G_i| = n\right) \times p_n \right) \\ &= \sum_{k=1}^{N} k \left(\sum_{n=k}^{N} \binom{n}{k} \left(\frac{1}{n}\right)^k \left(1-\frac{1}{n}\right)^{(n-k)} \times p_n \right). \end{aligned}$$ □

6.3 Entropy of the anonymity set

Theorem 6.3 (Entropy of the anonymity set): Entropy H_i of the anonymity set of a sender i of a request in the anonymous service access protocol is:

$$H_i = \log_2 \left(\sum_{k=1}^{N} k \left(\sum_{n=k}^{N} \binom{n}{k} \left(\frac{1}{n}\right)^k \left(1-\frac{1}{n}\right)^{(n-k)} \times p_n \right) \right) \tag{6}$$

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

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

where $p(i, j)$ is the probability of matching identifier j in the anonymity set with the sender i of the request. With this method all identifiers in the anonymity set have equal possibility to match with the sender. Thus,

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

Then we have:

$$H_i = -\sum_{j \in AS_i} \frac{1}{E\{|AS_i|\}} \log_2 \frac{1}{E\{|AS_i|\}}$$
$$= \log_2 E\{|AS_i|\}$$

$E\{|AS_i|\}$ can be replaced with equation (5). Then we have

$$H_i = \log_2 \left(\sum_{k=1}^{N} k \left(\sum_{n=k}^{N} \binom{n}{k} \left(\frac{1}{n}\right)^k \left(1-\frac{1}{n}\right)^{(n-k)} \times p_n \right) \right). \quad \square$$

7 Simulations and analysis

A series of simulations are made to validate the theoretical models developed in previous sections as well as the feasibility of the proposed AOSA protocol. The network simulator NS-2 (The Network Simulator – NS-2, http://www.isi.edu/nsnam/ns/) is used as the simulation tool. The latest version NS-2.33 already includes the modified versions of MAC and physical layer protocols defined in IEEE 802.11p standard which is used for inter-vehicular communications.

7.1 Experimental settings

In these simulations we measure five performance evaluation metrics, i.e., the size of the anonymity set, the entropy of the anonymity set, tracking probability (tracking success ratio), average service response time and service access success ratio. We measure these metrics by varying the number of vehicles, group radius, and group lifetime.

For each case, we evaluate these metrics with the urban and Manhattan vehicle scenarios by using Mobile Generator Framework (http://gmsf.hypert.net/). This scenario generator uses geographical road maps to create vehicles route and follows the traffic light and car following models to generate the mobility patterns for vehicles. The urban scenario contains 250 vehicles and Manhattan scenario contains 400 vehicles driving within 3,000 × 3,000 m^2 area, unless we explicitly state the different number of vehicles. For each case, the simulation is run for 500 s and the average values of each measurement are taken from 100 simulation runs with different seed values. Unless specifically states, general parameter values for the all simulation scenarios are listed in Table 2.

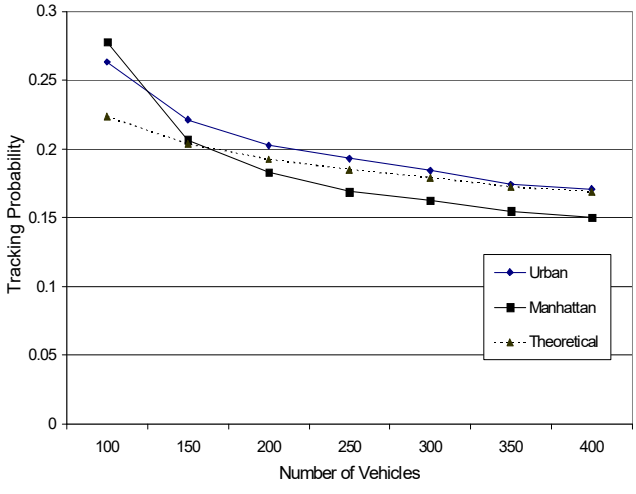
Table 2 Simulation parameters

Group lifetime	100 s
Group radius	300 m
Leader/member beacon interval	5 s
Leader/member update interval	15 s
Terrain area	3,000 m × 3,000 m
Simulation time	500 s

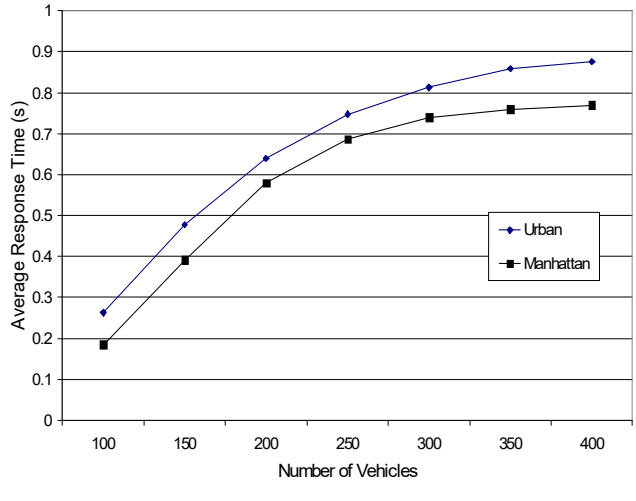
7.2 Impact of number of vehicles

We first study the performance of our protocol by varying the number of vehicles in both urban and Manhattan scenarios. The number of vehicles varies from 100 to 400 with the increment of 50. Figure 3 shows the impact of the number of vehicles in the network on the protocol performance.

Figure 3 Effect of the number of vehicles, (a) size of the anonymity set vs. number of vehicles (b) tracking probability vs. number of vehicles (c) average response time vs. number of vehicles (d) access success ratio vs. number of vehicles (see online version for colours)

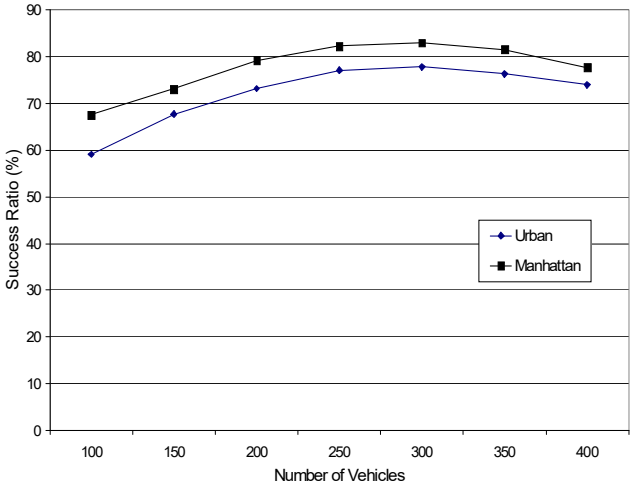


(a)



(b)

Figure 3 Effect of the number of vehicles, (a) size of the anonymity set vs. number of vehicles (b) tracking probability vs. number of vehicles (c) average response time vs. number of vehicles (d) access success ratio vs. number of vehicles (continued) (see online version for colours)



(c)

When the number of vehicles varies, both urban and Manhattan scenarios have the same number of vehicles but with different road infrastructures. With variable number of vehicles, both scenarios are behaving in a very similar manner. But Manhattan scenario always shows slightly better performance than urban scenario in all of the four parameters. Further, our theoretical results nearly match with the simulation results, which validate our analytical evaluation of the proposed protocol.

Figure 3(a) shows the impact of number of vehicles on the size of the anonymity set. In this proposed AOSA protocol, anonymity set (AS) of a message sender is defined as the number of group members in the group which the sender is reside. When the number of vehicles in the network increases, the number of vehicles in a group leader's perimeter also increases. Then higher number of vehicles in the network makes larger anonymity set size. So, this makes the higher level of anonymity.

Figure 3(b) shows how the tracking probability is affected by the number of vehicles. The average size of the anonymity set is not reduced to one, but for each scenario, there is a very little probability that the actual size of the anonymity set becomes one. It means that there is a small possibility that only one member vehicle is in the group when that member is sending a service request through the group leader. In this situation, whoever listens to the ongoing communication from the group leader has very little possibility to exactly find out the sender of the application messages. Since higher number of vehicles makes more group members, the probability of having single member group decreases with the increase of the number of vehicles.

The vehicle density in roads directly affects the number of vehicles in the group. Higher vehicle density always causes more communication traffic than the lower vehicle densities. In Figure 3(c), we plot the average response time for individual service access through the group leader. When the density of vehicles increases, the average response time also increases since the higher vehicular traffic makes higher communication traffic in the wireless networks. Even if all service access communications are going through group leader and the group leader performs some mixing among incoming packets, the average response time is still within 1 second. This means that our new anonymous service access protocol can maintain feasible response time while providing location privacy for the service users.

Figure 3(d) shows the impact of the number of vehicles on success ratio of service access. The number of vehicles does not heavily affect on the success ratio. When the number of vehicles increases from 100, the success ratio is slightly increasing since the higher number of vehicles increases the availability of more groups and group leaders. Nevertheless, when the number of vehicles further increases the success ratio is going down since higher communication traffic introduces message delays in the networks.

7.3 Impact of group lifetimes

We study the performance of our protocol by varying group lifetime in both urban and Manhattan scenarios. The group lifetime varies from 20 s to 200 s with the increment of 30 s. Figure 4 shows the impact of group lifetime on the proposed anonymous service access protocol.

In this case, when the lifetime of the group varies, Manhattan scenario always provides higher level of privacy than urban scenario. One of the main possible reasons is that Manhattan scenario always contains more vehicles than urban scenarios. Higher vehicular density always provides higher level of privacy and anonymity. However, due to higher communication traffic, Manhattan scenario also requires slightly higher response time than urban scenario. Further, these results validate our analytical evaluation since the theoretical results match with the simulation results.

Figure 4(a) shows the impact of group's lifetime on the size of the anonymity set. With the increase of lifetime, more and more vehicles are becoming members of the group. So, long live groups always have more members than the groups with shorter lifetime. Then longer lifetime makes larger anonymity set size for each service access. Therefore, it always increases the privacy of the sender of the service request.

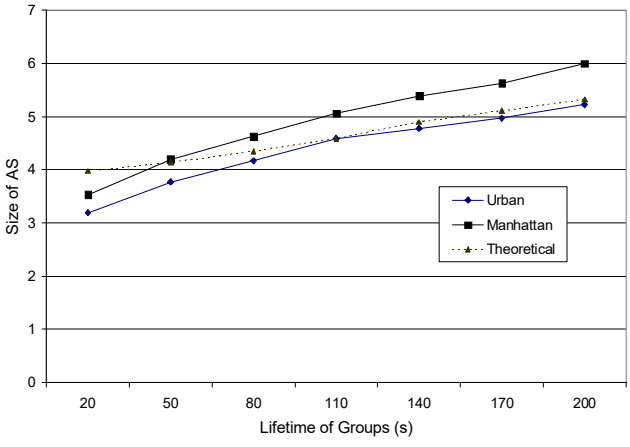
Figure 4(b) shows how the tracking probability is affected by the lifetime of groups. Group lifetime heavily affects on the number of group members in a group. Higher lifetime always causes higher number of members in any group, so it reduces the probability of having single member groups. Then, the tracking probability of service request sender can be reduced.

The lifetime of a group does not really affect on the response time of the service access. In Figure 4(c), we plot the average response time for individual service access through the group leader. When the lifetime increases from 20 s, the average response time increases very slightly, but the response time does not increase with the further

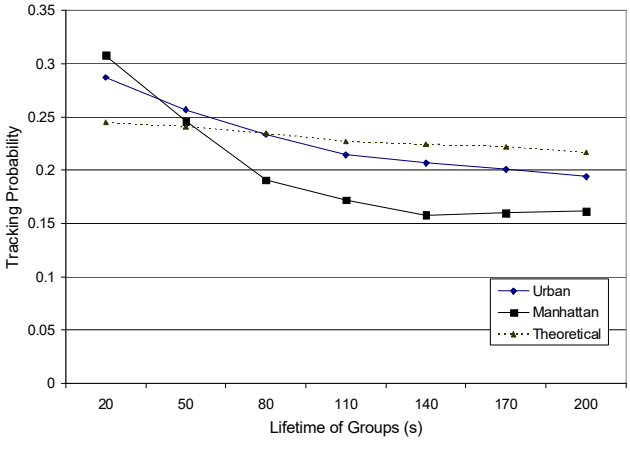
increase of the lifetime. The lifetime of groups does not change the availability or the communication traffic in the network, so that it does not affect the service response time considerably.

Figure 4(d) shows the impact of group's lifetime on success ratio of service access. The lifetime of groups does not heavily affect the success ratio. When the lifetime increases from 20 s, the success ratio significantly increases until 80 s. With short lifetimes, vehicles have to switch their groups frequently, which cause more unsuccessful service requests and provides lower success ratio.

Figure 4 Effect of group lifetime, (a) size of the anonymity set vs. group lifetime (b) tracking probability vs. group lifetime (c) average response time vs. group lifetime (d) access success ratio time vs. group lifetime
(see online version for colours)

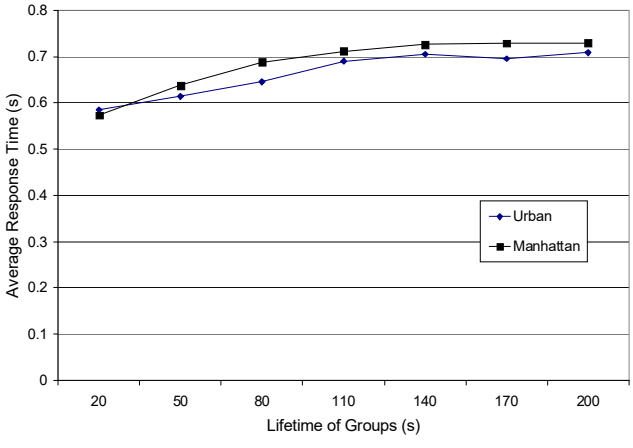


(a)

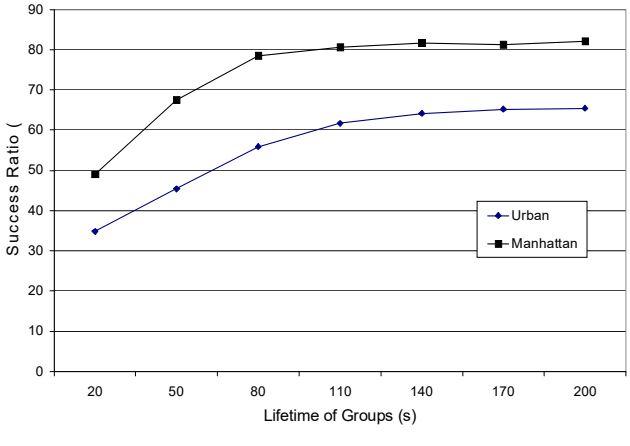


(b)

Figure 4 Effect of group lifetime, (a) size of the anonymity set vs. group lifetime (b) tracking probability vs. group lifetime (c) average response time vs. group lifetime (d) access success ratio time vs. group lifetime (continued) (see online version for colours)



(c)



(d)

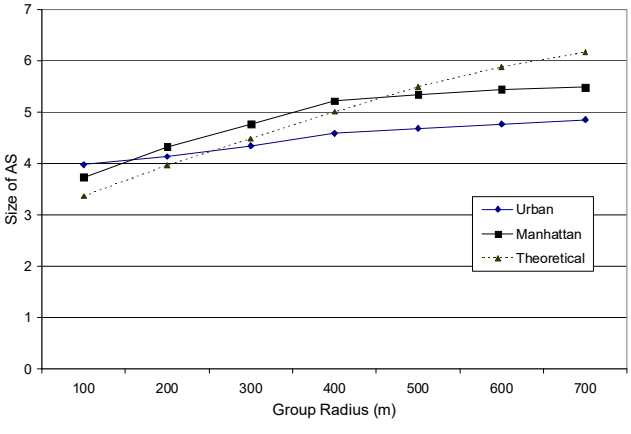
7.4 Impact of group radius

Figure 5 shows the impact of group radius on the proposed anonymous service access protocol. The group radius varies from 100 m to 700 m with the increment of 100 m. When the radius of the group varies, Manhattan scenario always provides higher level of privacy than urban scenario due to higher number of vehicles in Manhattan. Higher vehicular density always provides higher level of privacy and anonymity. But, due to higher communication traffic, Manhattan scenario also requires slightly higher response time than urban scenario. Further, these results validate our analytical evaluation since the theoretical results match with the simulation results.

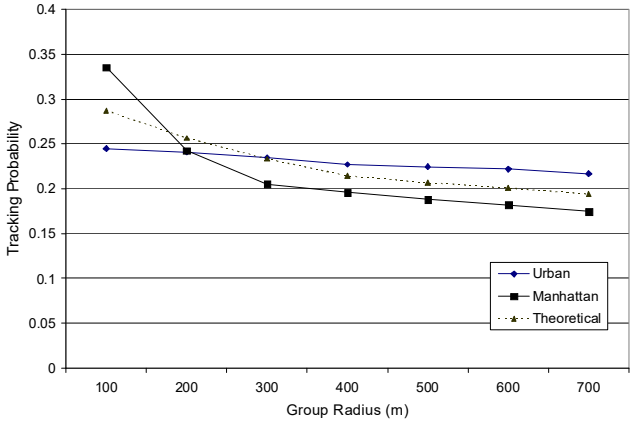
Figure 5(a) shows the impact of group radius on the size of the anonymity set. When the group radius increases, the number of vehicles, which can be stayed in a group leader's perimeter, also increases. Then, with the larger radius, groups always have more number of member vehicles than those with smaller radius group. Then larger group radius always makes larger anonymity set size.

Figure 5(b) shows how the tracking probability is affected by the group radius. There is a small possibility that only one member vehicle is in the group, when that member is sending a service request through the group leader. Since larger group radius makes more group members in a group, the probability of having single-member-groups decreases with the increase of group radius. So, the tracking probability is reduced significantly with the increase of group radius.

Figure 5 Effect of group radius, (a) size of the anonymity set vs. group radius (b) tracking probability vs. group radius (c) average response time vs. group radius (d) access success ratio vs. group radius (see online version for colours)

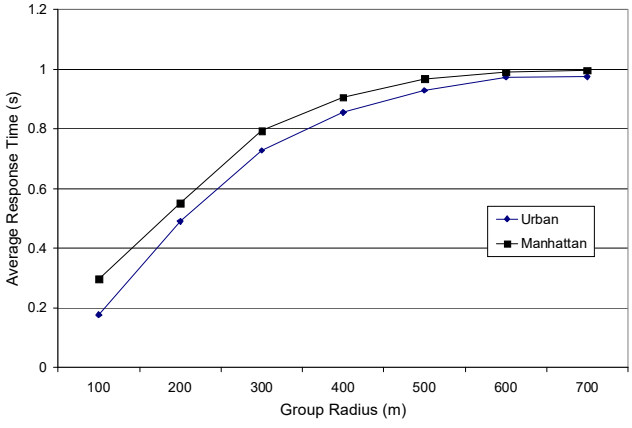


(a)

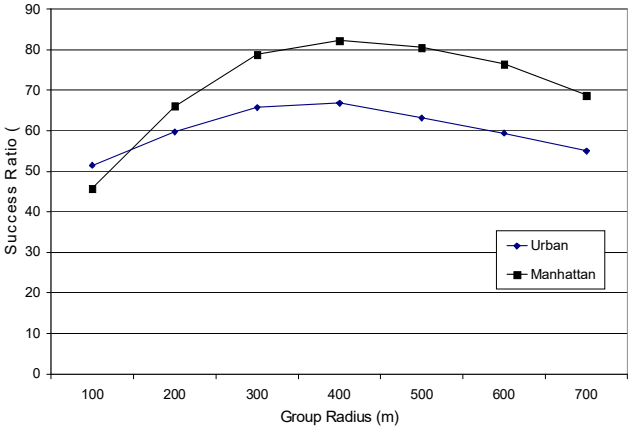


(b)

Figure 5 Effect of group radius, (a) size of the anonymity set vs. group radius (b) tracking probability vs. group radius (c) average response time vs. group radius (d) access success ratio vs. group radius (continued) (see online version for colours)



(c)



(d)

In Figure 5(c), we plot the average response time for individual service access through the group leader. When the radius of groups increases, the average response time also increases since the higher radius make higher average distance from the group leader to group members. Also, higher radius increases the number of group members in any group, consequently. The number of service requests that the group leader must handle is increasing with the higher radius. When the group radius further increases, response time also increases, but the rate of increase is decreasing. Furthermore, the average response time is still within 1 second. Therefore that our new anonymous service access protocol can maintain feasible response time with larger group radius which provides higher location privacy for the service users.

Figure 5(d) shows the impact of the group radius on success ratio of service access. When the group radius increases from 100, the success ratio is significantly increasing. When the group radius is small, vehicles have to switch their group frequently, so that

maintaining successful communication with group leaders is difficult. So, the smaller group radius always makes lower success ratio. With the increase of group radius, success ratio increases until around 400 m. But, with further increase of the group radius, success ratio is going down, because the distance between group leader and group member increase and the communication traffic going through the group leader also increases. This shows that the optimum group radius is around 400 m.

8 Conclusions

In this paper, we address the problem of location tracking in VANETs. By considering the unique characteristics of VANETs, we proposed the AOSA protocol to enhance the location privacy in VANETs. Simulation results showed that the new protocol give good performance by producing larger anonymity set, higher entropy as well as smaller tracking probability in different VANETs scenarios. We also evaluated the effect of number of vehicles, group radius, and group lifetime. Simulation results showed that:

1 higher vehicle densities give higher privacy level

2 group lifetime does not severely affect the performance but higher lifetime makes slightly better performance.

It can be concluded that the main advantages of the AOSA protocol include:

1 vehicles can anonymously access any services without exposing their real identity

2 grouping and accessing services through group leaders prevent tracing back to the sender

3 because of the use of common group identifiers within a group, this method enhances the location privacy and the unlinkability of service access

4 verification and vehicle authentication in online service access can be done without involving any authorities

5 since group members use group public key to communicate with other vehicles, our group method not only is capable for V2I communication, but also can be used in safety related V2V applications.

References

Beresford, A.R. and Stajano, F. (2003) 'Location privacy in pervasive computing', *IEEE Pervasive Computing*, Vol. 2, No. 1, pp.46–55.

Boneh, D., Boyen, X. and Shacham, H. (2004) 'Short group signature', in *Proc. Advances in Cryptography – Crypto'04, ser. LNCS*, Springer-Verlag, Vol. 3152, pp.41–55.

Dotzer, F. (2005) 'Privacy issues in vehicular ad hoc networks', in *Proc. of the Workshop on Privacy Enhancing Technologies (PET)*, June, pp.197–209.

Gedik, B. and Lu, L. (2005) 'Location privacy in mobile systems: a personalized anonymization model', in *Proceedings of the 25th IEEE ICDCS 2005*, Washington, DC, USA, pp.620–629.

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

Hoh, B. and Gruteser, M. (2005) 'Protecting location privacythrough path confusion', in *Proceedings of IEEE/Create-Net SecureComm*, Athens, Greece, September.

Hoh, B., Gruteser, M., Xiong, H. and Alrabady, A. (2007) 'Preserving privacy in GPS traces via uncertainty-aware
path cloaking', *ACM CCS'07*, Alexandria, Virginia, USA, 29 October–2 November.

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

Hubaux, J-P., Capkun, S. and Luo, J. (2004) 'The security and privacy of smart vehicles', *IEEE Security & Privacy*, Vol. 2, No. 3, pp.49–55.

Li, C-T., Hwang, M-S. and Chu, Y-P. (in press) 'A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks', *Journal of computer Communication*.

Lin, X., Sun, X., Ho, P-H. and Shen, X. (2007) 'GSIS: a secure and privacy-preserving protocol for vehicular communications', *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, pp.3442–3456.

Raya, M. and Hubaux, J-P. (2005a) 'Security aspects of inter-vehicle communications', in *Proc. of Swiss Transport Research Conference*, March.

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

Raya, M. and Hubaux, J-P. (2007) '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.

Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K. and Sezaki, K. (2005) 'CARAVAN: providing location privacy for VANET', in *Proc. of the Workshop on Embedded Security in Cars (ESCAR)*.

Schoch, E., Kargl, F., Leinmuller, T., Schlott, S. and Papadimitratos, P. (2006) '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, pp.43–57.

The Network Simulator – NS-2 [online] http://www.isi.edu/nsnam/ns/.

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