International Journal of Future Generation Communication and Networking
Vol. 3, No. 1, March , 2010

Privacy Issues of Vehicular Ad-Hoc Networks

Hang Dok[1], Huirong Fu[1], Ruben Echevarria[2], and Hesiri Weerasinghe[1]

[1] *Department of Computer Science and Engineering, Oakland University, Rochester, MI 48309, USA.*
[2] *University of Illinois at Chicago, Chicago, IL, USA.*
{htdok, fu@oakland.edu, rechev2@uic.edu, hdweeras@oakland.edu}

Abstract

Vehicular Ad-Hoc Networks are networks of communication between vehicles and roadside units. These networks have the potential to increase safety and provide many services to drivers, but they also present risks to privacy. Researching mechanism to protect privacy requires two key ingredients: 1. a precise definition of privacy that reflects citizens' concern and perceptions, and 2. an upstanding of the type of attacks in VANETs. In this research, we formulate a workable definition of privacy, and focus on tracking attacks, which we found to lacking. Although considerable research has been performed in tracking none of the published solutions ensures full protection. We propose to combine a set of published solutions, namely: Mix Zones, Silent Periods, and Group Signatures in order to improve the privacy of drivers. Vehicles enters a region where, vehicles change their pseudonyms (Mix Zone) as well as network addresses; next enter the silent period, and then use one group key for communication. It could help make tracking more difficult and increase the safety and confidence of drivers using VANET.

Keywords: *Privacy, VANET, Security, Mix Zones, Silent Periods, and Group Signature.*

1. Introduction

The Vehicular Ad-Hoc Network, better known as VANET, is a network devoted to communication between vehicles and roadside units. With such technology, vehicle owners could increase safety and provide many services to drivers [1]. One of the safety increasing features includes warning messages of oncoming accident sites in real time. One of the simplifying features includes messages with traffic updates to warn about possible traffic congestions on a desired route [2]. To better understand the relationship, one could look at the relationship between computers and the internet and connect it to the relationship between vehicles and VANET. Privacy is an important aspect for VANET to be successful and accepted by the majority in this paper.

We proposed a combination of existed solutions to provide security in the vehicular network. This solution consists of Mix Zones, Silent Periods, and Group Navigation. In our theoretical analyzes, we measured silent period's anonymity and entropy of the identifying vehicles within the proposed solution. We then found that the numbers were high in anonymity so that it would make it difficult for trackers to identify any one vehicle.

The remainder of this paper is organized as follows. In the next section we discuss the difficulties of defining privacy from the American perspective, followed by our proposed definition of privacy. Then we took our proposed definition of privacy to discuss information

that should be kept private, followed by how anonymity endangers VANET. Next, we introduce some of the previously proposed solutions to retain privacy. In Section III, previously researched tracking attacks on privacy and solutions are discussed. In Section IV, our proposed solution for research is discussed, which uses a combination of the previous proposed solutions discuss in Section IV. In Section V, our solution is evaluated through theoretical works. After the evaluation, simulation is displayed in Section VI. Section VII, concluded by discussing the advantages of our solution over some of the known researched solutions and our future works.

2. Privacy

Globally there is no set definition for privacy, causing some difficulties to study what should be kept private. According to the Leading Surveillance Societies in EU (European Union) and the World 2007 proves that the United States has little privacy and is under secure surveillance [3]. There are laws to protect human rights, but nothing of the sort to define privacy.

The definition of privacy used for this research is from Dr. Standler. He defined privacy as "the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities [4]." With an addition, from the US Code Collection from Cornell University Law School, personal information that can be used as identification should be kept private as well [5].

With a working definition of privacy, we will discuss what should be kept private relating to VANET. The privacy information is categorized into two groups: motor vehicle records and personal information. Motor vehicle records are defined as any record that pertains to a motor vehicle operator's permit [5]. A few examples of motor vehicles records include, but not limited to: motor vehicle title, motor vehicle registration, and identification card issued by a department of motor vehicles. Personal information is defined as information used as identification. A few examples of personal information include, but not limited to: photograph, full name, routine routes and time of travel, bills, and private keys.

Some may think to have VANET with anonymity, but in reality the network would fail if anonymity was introduced to the whole network for every vehicle all the time. First, it would compromise the entire idea of a secure network. False messages could be sent, such as "some pranksters might send bogus warning messages to other cars, pretending that there are dangerous road conditions ahead. This might lead to cars slowing down or breaking, resulting in traffic jams or even accidents [6]." VANET would only be a success if users feel it can be trusted and utilized it for what is was made for. Second anonymity, would not allow law enforcement to track vehicles. The law enforcement may need to track vehicles using VANET as an aid in an investigation of a stolen car or hit-and-run accidents [7].

Therefore, VANET must have a way to validate transmissions and keep security while retaining privacy, ruling out anonymity. Some researched ways to help keep privacy are pseudonyms and keys. Pseudonyms are fictitious names given to vehicles to prevent tracking. There is research to have a "vehicle generate its own pseudonyms, in order to eliminate the need of pre-loading, storing and refilling pseudonyms... [8]."

Keys are types of pseudonyms that secure the communication between the sender and receiver. There are two ways to encrypt and decrypt messages. First is the Asymmetric

key consisting of a private and public pair of keys that correlate with one another. Public keys can represent mailbox addresses that everyone in the network can see. Private keys are like a key that can open the mailbox mentioned above. This key can open any messages that are encrypted with the corresponding public key. To encrypt a message, one needs the public key of the person that is being sent the message. To decrypt the message, the private key is used to decrypt and corresponds to the public key. The advantage of public and private keys is the ability to authenticate messages. The disadvantages are: high security overhead [9] [10] [11] and computationally costly storing large number of key pairs and keys must be changed frequently [12]. Another type of key is the Symmetric key that consists of a key to encrypt and decrypt messages. This key can only be seen by certain individuals with some sort of mutual agreement. The advantages to asymmetric keys are: more efficiency over asymmetric keys, less computational effort, and less vulnerable cryptanalytic advance [10] [11] [13]. The disadvantage is the key distribution process is currently unknown.

3. Related Works

However, VANET is vulnerable to attacks such as tracking. By emphasizing on definition of tracking, we're able to understand the tracking attacks in VANET. According to the *WordNet*, tracking is defined as "the pursuit of a person by following tracks or marks they left behind [14]."

3.1. Attacks

The following attacks use VANET as assistance to an attacker and breach privacy, such as pseudonyms, location and time. There are many attacks in other VANET papers, but we narrowed it to a few that related to the proposed solution. The first attack involves receiver that are connected to a central database, which stores the pseudonyms, location, and time stamp [16]. The second attack discussed is the use of third-trusted parties' application (payment methods, loyalty cards, and chat application) [16]. By using these applications, users are risking their privacy by exchanging personal information that may help trackers link previous or future pseudonyms. By accessing web applications, malware can be installed which records location of the vehicles [16] and attackers will be able to hack into the vehicle system.

3.1.1. Linking Pseudonyms: A skillful and knowledgeable attacker can intercept radio waves to and from a vehicle using some type of compatible transmitter/ receiver [15]. With the intercepted data, an attacker could use the information a number of ways. An attacker could steal identities; steal private keys, track past/future routes, and link pseudonyms. Although pseudonyms were introduced to VANET to help drivers feel safe and comfortable that their true identity would be safe, pseudonyms do not completely prevent tracking. A determined attacker can link pre-existing pseudonyms to present pseudonyms, which will then aid to future pseudonyms [16].

3.1.2. Solutions to linking of pseudonyms: Random Silent Periods are randomly chosen periods which vehicles are forced to remain silent. During silent periods, vehicles have no incoming or outgoing messages using VANET and cannot access location base servers. Silent periods should be placed after the process of updating pseudonyms and occur areas with heavier traffic. The disadvantages to this are: vehicles

can still be tracked due to time and space relations. If the silent period range longer that some x amount of feet could affect the safety and liability of drivers given there was an emergency that needed to be reported [17] [18].

Another solution is mix zones which are predetermined regions where vehicles are required to change pseudonym addresses. These regions should be placed in areas such as intersections to prevent tracking vehicles. Mix Zones are dependent on RSU due to the changing of pseudonyms. Unfortunately, the demand for RSU depends on the traffic flow of that region. It would be very costly for regions with extremely busy intersections, which is a disadvantage to Mix Zones. Another disadvantage is that the RSUs are fixed, which in return allows to easily identify the location of Mix Zones and work to intercept information [19] [20], unless there is some randomizing algorithm that allows some intersections to have mix zones at certain times. Vehicle's pseudonym will changed once within this region, but receiver will be able to record this and location and time stamp. There's a possibility of linking two pseudonyms to one vehicle.

Mix Zones can be easily determined and linking of pseudonym can happen. Therefore another solution was proposed that would ensure authenticity of messages and decrease linking pseudonyms. CMixes are an extension of the Mix Zone; it consists of the Mix Zone (inner region) and the extended Mix Zone (outer region) of the road intersection. Vehicles are able to change pseudonyms and receive a symmetric key used to secure the messages within the Mix Zone. Vehicles can request a key from another vehicle within the extended Mix Zone, when unable to communicate with the RSU, but will not be able to use the key until it reaches the Mix Zone. The RSU must have a key update mechanism to secure regions from eavesdroppers. The disadvantages include the ease of tracking a vehicle if traffic is low and updating symmetric keys can produce overhead, which could cause low delay [20].

Group navigation preserves group identity and reduces pseudonyms. This solution may consist of a group leader, group members, and a group key. Group members and leaders travel in a general direction and velocity. If vehicles request to join the group, the group leader sends the group key and private key. Group keys allow members to encrypt and decrypt messages, while messages received would be untraceable. A private key for each vehicle allows the group leader to authenticate members and identify the vehicles. Members are able to communicate amongst themselves while group leaders can communicate outside the group as with Road Aide Units. All the messages group members send will have to be approved by the leader and then the leader would be able to access servers and message other group leaders. The disadvantage to group navigation is that there is no known protocol to appoint a vehicle to the position of leader and the group's leader's identity could be revealed [11] [12] [17] [18].

3.1.2. Malware: Accessing applications such chatting, paying toll fees and connecting with the RSU can danger users of VANET. Since this network is a computer based, it is vulnerable to software attacks [16]. It can range from manipulating messages to crashing and hacking on-board units. Manipulating messages invades privacy and creates security issues to the unknown victim. A victim could receive a false accident report and be forced to travel on an unfamiliar road. A victim could also send an alert message, but have it never successfully be sent or have the message altered. An attacker could crash the on-board unit in the vehicle which would be more of an inconvenience and cost to the owner. On the other hand if an attacker could crash the system, an attacker could hack into the system. This makes drivers in VANET vulnerable to

tracking, impersonation attacks; steal private keys, track past/future routes, and link pseudonyms.

3.1.3. Solution to malware: Malware is another way to track pseudonyms by accessing the web applications. We considered two solutions, Silent period and Group Navigation. This first attack is disabling vehicles transmission so no vehicle can access the network. Therefore no malware would be able to trace the pseudonyms for that region. However the rest of the region is at risk of tracing pseudonyms. Another solution we consider is group navigation, it allows vehicle to access applications and hides vehicle pseudonym.

4. Proposed Solution

Prior to the proposal we first assume that we are dealing with attacks consists of listening to transmissions. In addition, we propose that users within the network are reliable and have no bad intention. During vehicle registration, private keys are distributed to valid members of the network. In order to avoid or minimize tracking attacks such as listening to beacons and stealing information by hacking into third party applications, we consider the combination of earlier proposed solutions from above. This solution contains of a combination of Mix Zones [19] [20] [21], Silent Period [17] [18], and Group Signature [11] [12] [17] [18]. Many proposals rely on road intersection as a way to lower chances of tracking. In this proposal we considered road intersection as the basis of the solution to privacy.

4.1. Entering mix zone

In this scenario we will have two types of protocols of traveling vehicles, group key and pseudonyms. Each vehicle will be assigned a new pseudonym (mix zone) before entering intersection region. In figure 1, we see that there are groups key 13, 41, and 12 entering the region changing their pseudonym. In this process the identifiers changes for each vehicle. For example one of the cars in group key 13 may have pseudonym with 1234 but changed to 2345. This current pseudonym allows for communication among other vehicle in case of accident within the silent period region.

4.2. Entering silent period

After exiting the mix zone, vehicles will enter a region where transmission is disabled and enter the intersection. In fig. 2, group key 13 and 41 enters the silent period, therefore their group key or pseudonym is not revealed. This will lower chances of identifying vehicles directions due to high traffic.

4.3. Group keys

When vehicles leave the silent period region, users are forced to change pseudonyms address once again. By using the same example in entering mix zone, a vehicle in group key 13 will change pseudonym from 2345 to 5678. At the same time the vehicle will be assigned to a group key 55, fig. 3. Vehicles will be assigned to encrypted group key distributed by RSU. Group key is obtained; vehicles may or may not form group navigating depending on the surrounding environment. After leaving the Mix Zone,

general public are advised to become group members, while authority vehicles are group mangers. Algorithms for group navigation should be able to switch from independent traveling to group members to group managers. Group keys should change frequently after some time interval - key mixes. All group keys allow communication with a different group key. Group keys should not have any connection with identifier.

Group navigation allows member to remain anonymous among other members and possible attackers. There will be many groups navigating using the same group key depending on the road intersection traveled through. Therefore different groups can communicate with a group key. A fixed location compromises the solutions intent to protect against privacy attacks. Therefore the areas of Mix Zones and Silent Periods need to be randomly generated with an algorithm to place the combination of zones at the highest traffic intersections, preferably traffic in commercial and highway.

4.3.1. Members navigation: For the first batch of vehicles receiving the group key will be the first group navigating using group key xxxx. To have group navigation, this batch of vehicles must have a similar velocity and direction. Group members holds a group key and are able to send and receive messages to each other as a group and will not be able to know the sender of the message [12]. When a members access the RSU or application server, attacks may be hack into these application but cannot distinguish vehicles because the usage of the group key. Group key therefore cannot have any connection to unique pseudonym of the member. Since there are many users of this group key, no one attack will be able to identify one person in the group.

4.3.2. Members diverging paths: However, if vehicles diverge different path or velocity then if will travel by sending its pseudonym address. These users will be able to listen to all the activities surrounding them but will not be able to reply to any of the messages; transmission is cut off until a group is detected nearby. Group key given during key mixes will be allowed to join other available groups as long there are a similar velocity.

4.3.3. Manger and members: Authorities vehicle are group managers provided that there are not corrupted. Manager maintains authenticity of group members and allows member to access applications servers and RSU. The duties of the manager consist of recording all the data and pseudonym of each member. Therefore managers can look up the identities of its members to ensure authenticity in any give case. Managers should beacon out public key letting members know it is a group manager. Only group manager can communicate beyond the group, like servers and applications. Messages received by the manager from the application servers are beaconed among the members.

5. Theoretical analysis

The paper is based on mix zones, silent periods, and group concept. The purpose of this section is to measure the level of privacy for each vehicle within this region. In doing so, we theoretically analyze the silent period and ignore other purposed solution due to its analytical perplexity.

We will be analyzing the silent period that contains an intersection with a heavy flow-rate. Vehicles are to send beacons every millisecond however within the silent period no vehicles are to send or receive messages due to the failure of the transmission

in this region. After exiting, vehicles automatically continue sending beacons. The measurement of the privacy levels is crucial in determining the question of usage. We use two performance metrics: anonymity set and entropy level.

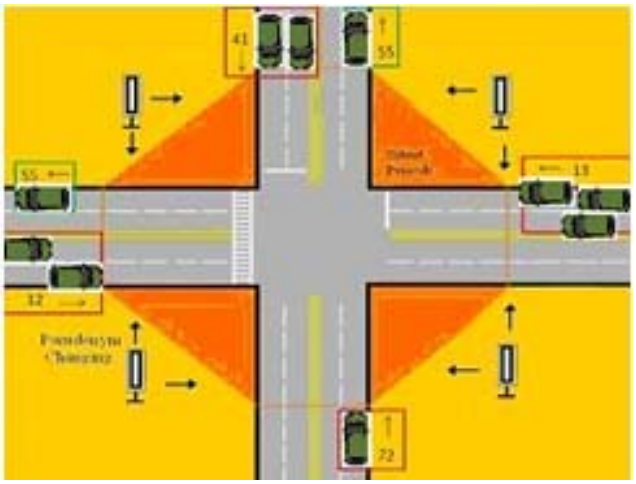


Figure 1. Group key 13, 12, 72, 41 enter Mix Zone

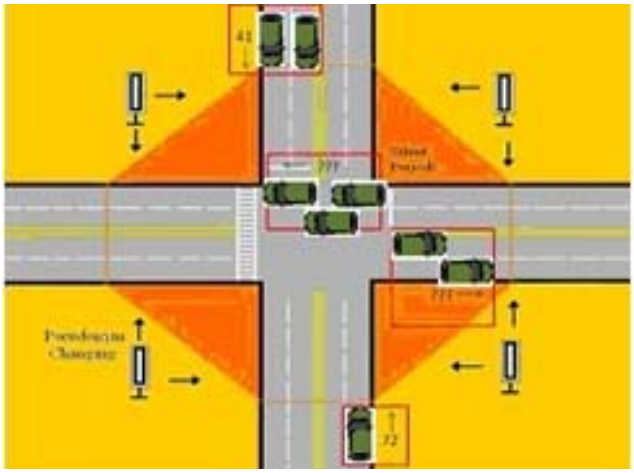


Figure 2. Group key 13, 12 enter Silent Period

An anonymity set is the number of possibilities for an attacker to track a vehicle. The higher the anonymity set, the lower the probability for tracking of a vehicle. In the proposed solution, the number of vehicles exiting the combination of zones between a reasonable minimum and maximum time for one vehicle to exit is the anonymity set. There are numbers of parameter that are affected by the anonymity set as a vehicle enters the combination of zones: 1. Number of lanes for vehicle to exit assuming that there is no U turns 2. Rate of number of vehicles per given time exits the region for each lane 3. Minimum and maximum time for each vehicle to travel within silent period

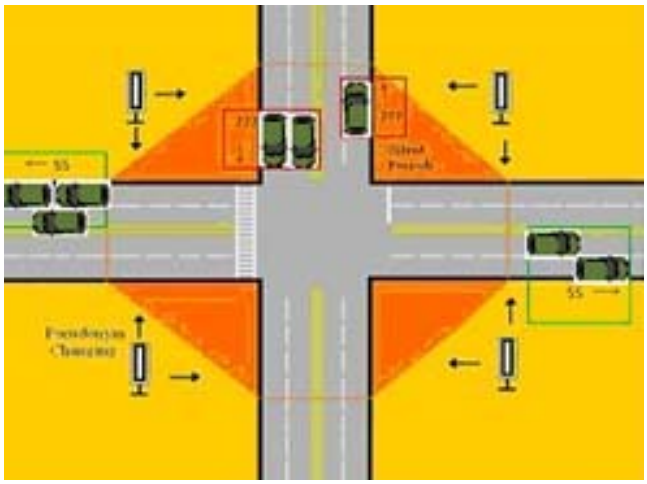


Figure 3. Group key 13, 12 are assigned group key 55. Group key 72 and 41 enter Silent Period

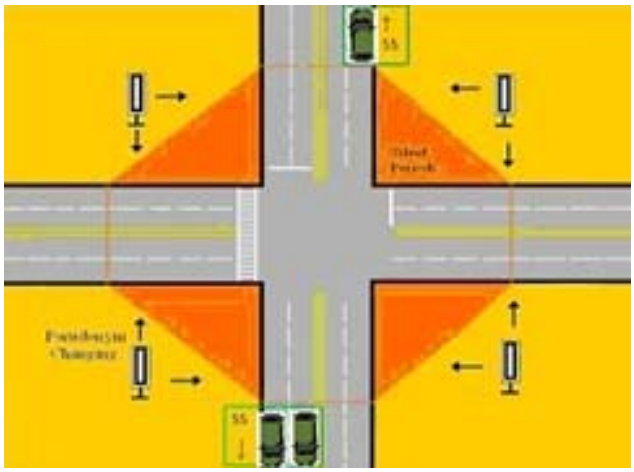


Figure 4. Group key 72 and 41 are assigned group key 55

After determining the parameter, the function that will define the anonymity set is

$$S_A = \sum_{i=1}^{N} RL_i * t \cdot \quad (1)$$

Entropy is a measure of the content of a message evaluated with respect to its probability of occurrence, or uncertainty of occurrences. In this case we are measuring the solution we proposed to see whether high anonymity set is probable. Given that the attacks are unknown, the probabilities for all the anonymity sets are equal. If the entropy is high then privacy is high as well.

$$E = -\sum_{i=1}^{SA} P_i (\log_2 P_i) \cdot \quad (2)$$

P_i Stands for probability for anonymity set

$$P_i = \frac{1}{S_A}$$

Now that we know the definition of each metrics we can illustrate a traffic scenario, with the assumption of these properties from Table I. Next consider these parameters: size of Silent Periods which affects the duration of vehicles within the region given the average speed of vehicles in the scenario, flow-rate and the number of lanes for each scenario.

Table 1. Define each scenario through various speed and number of lanes.

	Speed (mph)	Lanes
Downtown	25-30	1, 2
Local	35-45	2, 3
Highway	60-70	3, 4

For each scenario, flow-rate increase over time and number of vehicles exit increases as well, known as the anonymity set. Results may affect the average speed at which vehicles are moving and due to the assumption's size of the scenario. Varying numbers are adjusted to improve the anonymity set by increasing number of lanes, time duration or flow-rate. Figure 5, illustrates that 3-lane local and 2-lane downtown has a greater anonymity set due to average time measures respectively at 5.70 s and 3.92 s. However, increasing the time duration to 10-20seconds, highway scenario obviously has higher anonymity set. Therefore it takes vehicles longer to travel within this scenario due to higher velocity and size of the region. For the next measurement, entropy set uses Figure 5 to determine the probability. Figure 6 illustrates that 3-lane local and 2-lane downtown has the preeminent results compared to other four scenarios due to particular traffic scenarios.

By determining better results, we took the measurements at higher time duration of 20 seconds. However we questioned why highway traffic scenario had the least anonymity set so we then compared to another anonymity set for a longer time duration, which resulted in highest anonymity set compared to other 4 traffic scenario. As a result, concluded that traffic scenarios with higher velocity must travel in a larger size region for a longer time within the silent period. If more factors came into this simulation, the theoretical part would be more realistic. However, traffic lights and the path of directions vehicles were ignored. Next section we considered traffic lights and vehicle's destination path and prove that flow-rate will increase the anonymity set.

Table 2. Define each multiple scenario by an average speed and number of lane.

	Speed (mph)	Lanes
Downtown	27.5	1
Local	27.5	2
Local	40	3
Highway	72.5	3
Highway	65	4

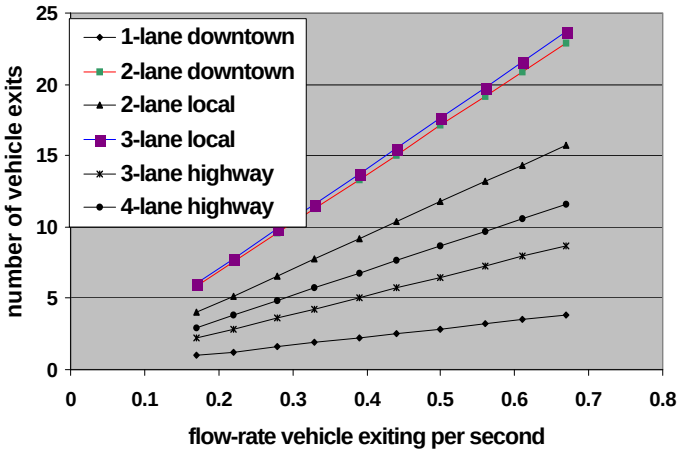


Figure 5. Illustrate flow-rate is dependent on the anonymity set for each scenario. Assume that downtown areas should be one lane or two lanes and traveling around 27.5 mph; local area should be two or three lanes and traveling around 40mph; and highway areas should be three or four lanes and traveling around 72.5mph.

6. Simulations

Matlab is used to simulate the process of vehicles moving into and out of the silent period, in order to imitate, exponentially random times in seconds were produced. Next we ordered the random times in ascending order and summed the time before and current time to give us the exact times of each vehicle entering the region. Finally we had to find the parameters that will affect the timing of vehicles inside the region: Destination, Speed, Flow-rate, Size, Traffic Lights of silent period depending on different scenarios.

Each traffic scenario has different speeds. By comparing to real life traffic (mph): downtown areas range from 20-30, local areas range from 35-45, commercial area range from 45-55, and highway may range from 60-70. The definition of flow-rate is how many vehicles will enter the region per second ranges from 0-1.0 vehicle per second (vps). Size of silent period is dependent on types of scenarios, downtown and local assumes vehicle will be traveling in range of 20-45 mph; therefore size should be 60.96-91.44m (~200-300 ft). Commercial and highway assume vehicles will be traveling in range of 45-70mph; therefore size should be 300-450 ft, so that vehicles have some decent time to traveling in the region. Traffic Lights are considered since we are dealing with busy road intersections, how long it will take to change from red and green lights, we used 10 seconds since the time we are measuring is only 20-30 seconds. Destination is for vehicles to take; either straight, right, or left. Timing will be different whether going straight (3s), right (2s), and left (4s).

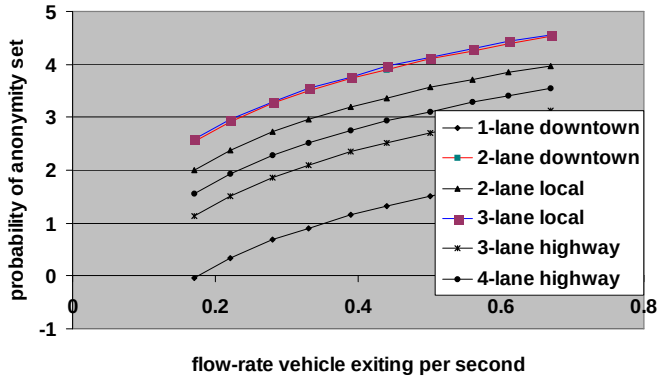


Figure 6. Measure probability of the anonymity set in Fig. 5. 3-Lane local traffic scenario measures time duration at 3.92 seconds traveling velocity at 40mph while 2-lane downtown measures time duration at 5.70 seconds traveling velocity at 27.5mph. 3-lane and 2-lane of local and downtown, respectively have the highest probability.

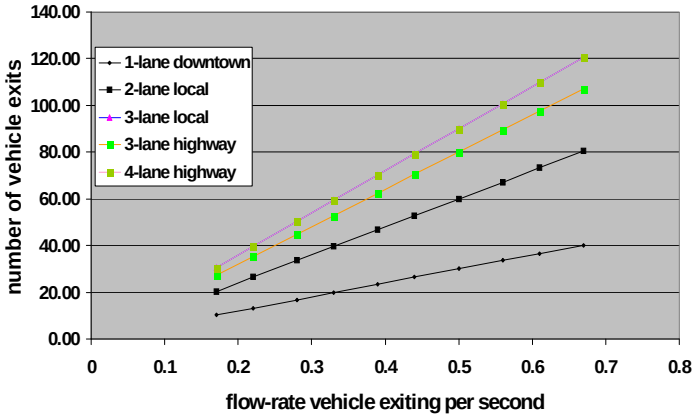


Figure 7. Measure the time duration for max of 20 seconds. 3-lane local and 4-lane highway has the greatest anonymity set.

Next we calculated the time it takes for each vehicle to exit the silent period. During the simulation, queries of the silent period were made to see whether it would be effective enough for privacy solution in VANET. Therefore we measure the anonymity set for each vehicle at a time, which is a set of other vehicles exiting within same range of time, depending on how long it will take that one vehicle to exit. Basically anonymity set illustrates how vehicles are able to be anonymous within the region, due to other vehicles exiting at similar ranges of time so it will be hard for some tracker to identify a particular vehicle from a mass of other vehicles.

We then took the average of the anonymity set per direction: north, south, east, west roads and also the average for the entire silent period. Then graph different parameters that will affect the privacy of the users.

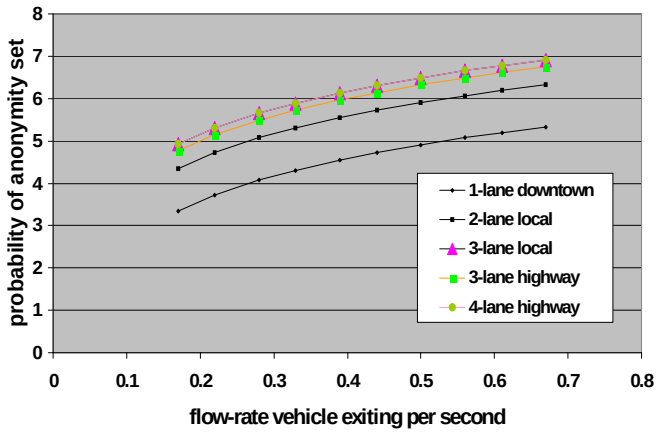


Figure 8. Measures the entropy of the anonymity set from Fig. 7 for each scenario.

Fig.9 measures the anonymity set due to varying flow-rates, where vehicles are in different scenarios (downtown, local, commercial, and highway). As you can see the local traffic scenario have a greater anonymity over the varying flow-rates set compared to the rest of the scenarios, which seem to be caused by the medium range of the velocity. Similar to previous, Fig.10 measures the anonymity set verse flow-rate depended on silent period size of 102.108 meter. As the size of the silent period increase, the anonymity set increased a bit, this does not seem to affect the anonymity set too much. However the local traffic scenario seems to have a greater anonymity set in both figures. Now let's look at the sizes of the silent period verses anonymity set. Fig.11 and 12 each shows this but since 2 regions are similar are group together. In fig.11 we see that local region have a better anonymity set since it has a higher flow-rate than downtown. Similarly in fig. 12, shows the silent period ranges from 85-110 meters where the highway has greater anonymity set compared to commercial regions. This may tell us that flow-rates ranging from 0-40mph has a greater and stable anonymity set compared to higher ranges.

After the simulation, we can expect that the parameters do affect the privacy levels of the silent period; if we were to increase the flow-rate or the size of the silent period. As one can see that different scenarios does better than others, which does not affect the silent period since our results for the anonymity set is fairly high..

One of the major issues for silent periods is that what if there was an accident inside the silent period. Since there will be others vehicles inside the region at same time, vehicles must be alert due to its surroundings and save the data of the accident onto the on-board-unit and execute message to authority, server, or other vehicles once out of the region. In doing this will increase the safety of the users in VANET.

In that situation, safety appears to be more important than privacy. Vehicles not inside the region automatically sends warnings and alerts constantly, so that some base unit nearby will disable the silent period. Some nearby authority will be able receive the message and to go the scene of the accident.

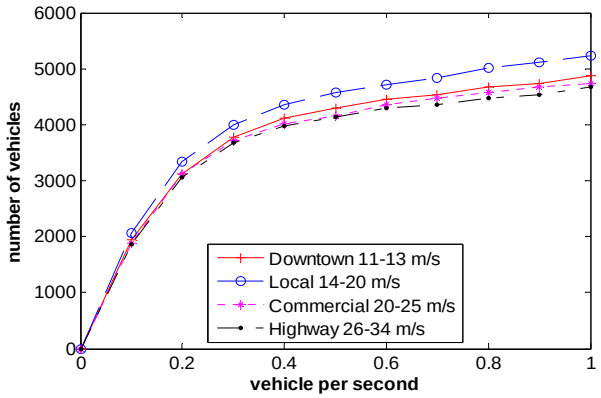


Figure 9. Anonymity set vs. Flow-rate graph sets size of region to 76.2 meters. Measure the number of vehicles with the given protocol over the variation of flow rate of the traveling vehicles.

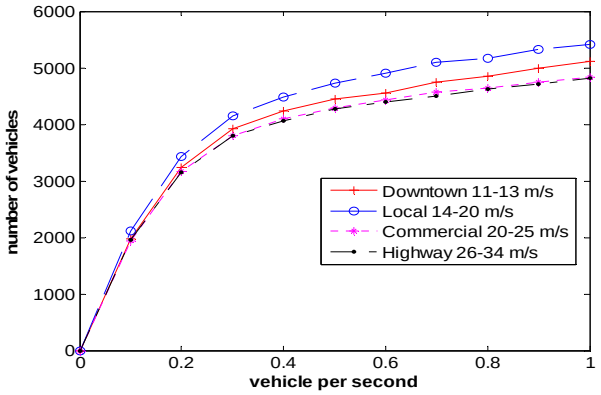


Figure 10. Anonymity set vs. Flow-rate graph sets size of region to 102.108 meters. Measure the number of vehicles with the given protocol over the variation of flow rate of the traveling vehicles.

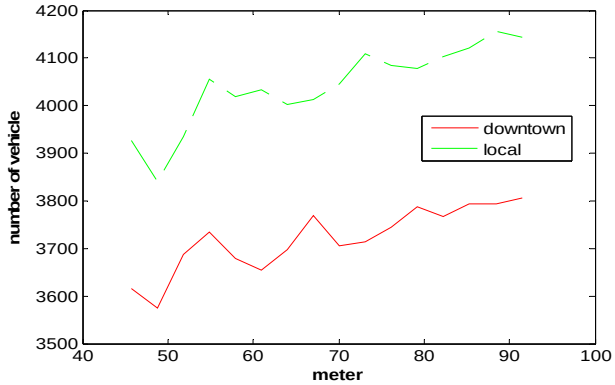


Figure 11. Measures the number of vehicles entering the silent period depended on the varying sizes of the silent period.

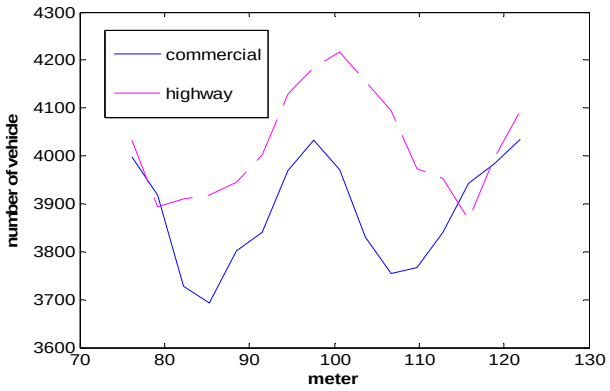


Figure 12. Measures the number of vehicles entering the silent period being depended on the size of the silent period.

Since our protocol is not based on only one silent period but several around the region, it should randomly generate another silent period /group navigation and by replacing into another intersection. Therefore one disable mix zone and silent period would not affect the privacy of other vehicles within the region. This proposed solution seems to be a potential solution used in VANET to prevent possible attacks in the future.

7. Conclusion and future work

This solution has many benefits for preserving privacy. The solution prevents attackers from linking transmission to a particular vehicle after an intersection. When vehicles enter the region, vehicles change their pseudonym address, and then enter the silent period, where vehicles can travel in different paths; as a result the attacker would have no choice, but to guess which path to continue following. Once in a group, vehicles are able to become anonymous, because every vehicle shares only one key to communicate. Since group keys are not related to pseudonyms, identities should not be linkable. By using one group key, security overhead is reduced opposed to asymmetric keys. Group keys reduce the number of key maintenance [12], and are more efficient. Messages encrypted with the group key can only be opened by the group key. Only group members and leaders know the group key, which was distributed by the Mix Zone. Having the Mix Zone in certain regions, congested road intersection, reduces the amount of pseudonyms that could possibly cause a delay from the RSUs. Opposed to Mix Contexts, which change pseudonyms frequently before and after places have been visited, but cause pseudonyms to be wasted [16]. For those reasons, forming groups helps vehicles retain privacy because an attacker would be challenged with the pseudonym change, network address change, Silent Periods and group navigation.

In conclusion, VANET could only be successful if vehicle owners trust the network to secure their privacy. With our proposed solution to combine a set of published solutions, namely: Mix Zones, Silent Periods, and Group Signatures to improve the protection of privacy of drivers. The more drivers using VANET, the more people will benefit from the network. The more people benefit, the more useful the information

shared. Along with our proposed solution to retaining privacy, VANET could be a more trusted and therefore accepted network for vehicle owners. With such technology, vehicle owners could increase safety and provide many services to drivers.

Our solution has been tested analytically and theoretically. In future work, we intend to have our solution simulated to test efficiency, anonymity set, and entropy against other known solutions. We would also like to create the algorithm to randomly generate the areas of Mix Zones and Silent Periods for our solution.

Acknowledgement

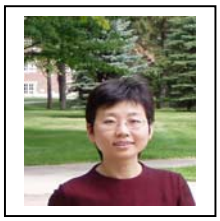
This work is supported by the U.S. National Science Foundation under Grants No.0716527 and No. 0736877, Michigan Space Grant Consortium Research Seed Grant, and Oakland University Faculty Research Fellowship.

References

[1] Atulya Mahaian, Niranjan Potris, Kartik Gopalan, Andy Wang, Lehman Brothers, “Modeling VANET Deployment in Urban Settings,” MSWIM’07, 22-26 October, Chania, Crete Island, Greece, (2007).
[2] Walaa El-Din M. Moustafa, “Privacy of location Information in Vehicular Ad Hoc Networks,” www.cs.umd.edu/class/spring2007/cmsc818z/present.ppt.
[3] Privacy International, http://www.privacyinternational.org/indexs.html, Clerkenwell, London, (1990).
[4] Ronald B. Standler, “Privacy Laws in the US,” http://www.rbs2.com/privacy.html, Massachusetts, (1997).
[5] Thomas R. Bruce, Emeritus Peter Martin, “US Code Collection,” Legal Information Institute, Cornell Law School, Myron Taylor Hall, Ithaca, NY, (1992).
[6] Frank Kargl, Zhendong Ma, and Elmar Schoch Ulm University, Institute of Media Informatics, “Security Engineering for VANETs,” http://medien.informatik.uni-ulm.de/forschung/publikationen/escar2006.pdf.
[7] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, ”The Security and Privacy of Smart Vehicles,” IEEE Security and Privacy, vol.4, no. 3, pp. 49-55, (2004).
[8] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux Antonio Lioy, “Efficient and Robust Pseudonymous Authentication in VANET,” VANET’07, 10 September, Montreal Quebec, Canada, (2007).
[9] Maxim Raya, Panos Papadimitratos, Jean-Pierre Hubaux, “Securing Vehicular Networks,” The 25th Conference on Computer Communications IEEE InFOCOM 2006, 23-29 April, Barcelona, Catalunya, Spain, (2006).
[10] Kewei Sha, Weisong Shi, Loren Schwiebert, Tao Zhang, “Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks,” ISADS Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, (2007).
[11] Maxim Raya, Jean-Pierre Hubaux, “Securing Vehicular ad hoc networks,” Journal of Computer Security 15 (2007) 39-68.
[12] Jinhua Guo, P. Baugh, and Shengquan Wang, “A Group Signature Based Secure and Privacy Preserving Vehicular Communication Framework,” 2007 Mobile Networking for Vehicular Environments vol.11,no.11,pp.103-108, May 2007.
[13] J. Choi, M. Jakobsson, S. Wetzel, “Balancing Auditability and Privacy in Vehicular Networks,” Q2SWinet, October 13, Montreal, Quebec, Canada, (2005).
[14] "tracking." WordNet® 3.0. Princeton University. 15 Jul. 2008. <Dictionary.com http://dictionary.reference.com/browse/tracking>.
[15] Jerry Werner, “Details of the vii initiative’s ’work in progress’ provided at public meeting,” http://www.ntoctalks.com/icdn/vii pubmtg v1.php.
[16] M. Gerlach, “Assessing and Improving Privacy in VANETs,” Published: In Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR), Hamburg, Germany, November (2006).
[17] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VANET,” IEEE Journal on Selected Areas in Communications (JSAC), Special issue on Vehicular Networks, (2007).
[18] Mingyan Li, Krishna Sampigethaya, Leping Huang, Radha Poovendran, “Caravan: Providing Location Privacy in VANET,” Workshops On Privacy in the Electronic Society, Proceedings of the 5th ACM workshop on Privacy in electronic society, Alexandria, VA, 30 Oct., (2005).

[19] Florian Dotzer, "Privacy issues in vehicular ad hoc networks," In proceedings of the Workshop on Privacy Enhancing Technologies, (2005).
[20] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos and J.P Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS) Vancouver, (2007).
[21] Alastaire R. Beresford, Frank Stajano, "Location Privacy in Pervasive Computing," Pervasive Computing, IEEE, Vol. 2, Issue 1, pp. 46-55, (2003).

Authors



Dr. Huirong Fu is an associate professor with the Department of Computer Science and Engineering at Oakland University (OU). Prior to her joining OU as an assistant professor in 2005, she has been working as an assistant professor at North Dakota State University (NDSU) for three years, and as a post-doctoral research associate at Rice University for more than two years. As a lead professor and the principal investigator in several projects funded by the NSF, Dr. Fu has been actively conducting research in the area of information security. Her primary research interests are in information assurance and security, networks, Internet data centers, and multimedia system and services.

Hesiri Weerasinghe is currently a Ph.D candidate in Department of Computer Science and Engineering at Oakland University, Michigan, USA. He received his B.Sc degree in Mathematics from University of Kelaniya of Sri Lanka in 2000 and his M.Sc degree in Computer Science and Engineering from Oakland University in 2006. His research interests include security and privacy of VANETs, Network Security, Mobile ad-hoc networks and Communication Networks.