Anonymity Framework for Vehicular Adhoc Networks Based on Pseudonyms

S. Nagavalli[1], Dr. G. Ramachandran[2], Dr. R. Saminathan[3]

[1]*Research Scholar,* [2,3]*Assistant Professor*

[1,2,3]*Department of Computer and Information Sciences, Annamalai University Annamalainagar – 608 002, Tamil Nadu, India.*

Abstract: - In this paper, propose a framework for providing anonymity to communicating cars in VANETs. The anonymity is accomplished based on a system of pseudonym generation, distribution, and replenishing. The Road Side Units (RSUs) play a key role in the framework by receiving the originally generated pseudonyms from the trusted authority, and then distributing pseudonym sets to cars while shuffling the sets amongst themselves to maximize anonymity. The pseudonym distribution process among the RSUs and to the vehicles is highly adaptive to accommodate the needs of the vehicles. Develop a distributed optimization algorithm for the shuffling process and a novel mechanism for cars to change their pseudonyms. Experimental evaluations based on ns2 simulations demonstrate the effectiveness of the framework through showing relatively high values of the used metric, namely the anonymity set.

Keywords: VANET, RSU, WAVE, CCH, DOT, TA, OBU.

I. INTRODUCTION

Vehicular Networks have been given considerable attention for the past decade and several standards have been developed to render such networks more organized and realizable. The primary goal of vehicular networks was to increase safety and transportation efficiency in applications that include emergency-response operations, adaptive cruise control, lane keeping, and assisted braking. One of the first steps was the adoption of the IEEE 802.11 technologies and modifying them to develop a suitable version for vehicular environments, namely 802.11p that provided lower MAC and PHY layer specifications for granting vehicles wireless access [1]. Moreover, the IEEE 1609 family of standards, known as the Wireless Access for Vehicular Networks (WAVE) protocol, were developed to provide specifications for the higher layers for offering vehicles multi-channel capabilities to enable them to access infotainment services in addition to the safety ones. More specifically, vehicles are able to access 6 other service channels (SCH) in addition to the control channel (CCH). Besides the safety-related messages (e.g., BSM in the US and CAM/DENM in Europe) broadcasted on the CCH, vehicles can send non-safety-related message on an SCH (e.g., POI and traffic jam notifications). Vehicles synchronously tune to the CCH for 50 ms to receive all periodic and event-driven messages, and then switch to any SCH of their choice for another 50 ms. For now, the only cars with vehicle- to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication capability are in test fleets. However, the Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) in the U.S. announced in February of 2014 that it will begin taking steps to enable V2V communication technology for light vehicles [16] [18]. Even though cars might start having such technology in 2017, it would take another 10 years before most of the on-road fleet to have it [17]. On the other hand, it is also anticipated that vehicles which do not come with the technology, could get aftermarket devices with much of the capability, such as those being tested in the UMTRI project that is led by the University of Michigan, and includes a consortium of car makers: General Motors, Ford Motor, Toyota, Hyundai/Kia, Honda, Volkswagen, Mercedes-Benz, and Nissan [17].

Despite the promises of vehicular communication, it is agreed that vehicular networks are subject to many privacy and security challenges which, if not addressed, will hinder the development and acceptance of services by users [2][3][19]. A major premise of vehicular safety applications is the need for vehicles to broadcast messages about their current location, speed and direction. Even though the latter provides great benefits to the safety applications, it also raises great privacy concerns. Malicious possession of this information might allow malicious entities to track individuals easily and possibly blackmail them. Such lack of privacy might deter drivers from participating in VANETs, which would greatly hinder the potentials of improving traffic safety. Therefore, there is a great necessity for hiding vehicles' identities to make tracking them a non-simple task. One of the most popular solutions for privacy is the use of pseudonyms, which are fake identifiers used by vehicles instead of fixed original identities. Cars use these pseudonyms as a source address for their beacons and their communications with other cars. Hence, information inside messages, whether location, speed, or direction will not be linked to a physical car, and the privacy of users will be kept safe. The solution of pseudonyms is not that direct though and simple, as it faces several challenges to be an effective scheme.

Theoretically, if well implemented, the use of pseudonyms has two main ultimate aims. The first being anonymity, where a sent packet cannot be linked to a

physical vehicle as its sender. The second goal is unlinkability [6], where a new pseudonym cannot be directly linked to a previously used one of the same car. However, achieving anonymity and un-likability is subject to several challenges [20]. To begin with, there is a trade-off between privacy and the cost of applying pseudonyms to achieve it.

Due to the nature of wireless networks, nodes in proximity of the sending node can receive these encrypted packets, but without the corresponding session key, those neighbors will not be able to recover the packet. The investigation of pseudonyms from the perspective of how often they should be changed to achieve the highest level of privacy, and have been oblivious to face the challenges is an important task.

While the aforementioned works focus on the importance of determining the optimal approach in utilizing pseudonyms, they do not do a good job in addressing other essential factors, such as the origin of these pseudonyms, their generation, and the layer they are used. These key notions are, however, touched upon by other researchers, namely the authors of [12] who propose the frequent changing of MAC addresses, which are disposable addresses created based on a forward chain of MD5 hashes started with an unpredictable random seed. They do not however specify details about the frequency of changing pseudonyms and how the change occurs. The authors in [13] also worked to achieve privacy at the link layer. Every time a node needs to send a packet it encrypts its MAC address with the session key. The access point, having all the keys, will try all keys to find out which one decrypts the MAC address. Since the encryption of the same plaintext with the same key will result in the same Ciphertext, the authors suggest padding the MAC address with a sequence number that is changed every time. Due to the nature of wireless networks, nodes in proximity of the sending node can receive these encrypted packets, but without the corresponding session key, those neighbors will not be able to recover the packet. Nevertheless, this approach is gullible as it does not consider the consequences of compromising the session key which will result in the disclosure of all previously sent packets.

In this proposed model, consider a system of vehicles each having an onboard unit (OBU) equipped with wireless technology based on the IEEE 802.11p/WAVE standard, allowing them to communicate with each other and with road-side units (RSUs). The RSUs are equipped with the same technology and are fixed infrastructure connected to each other and to the backbone network through wired connections.

OBUs communicate with each other directly, if within transmission range, or use multi-hop communication, where nodes collaborate to forward packets from source to destination. Due to high mobility and frequent disconnections that occur in VANETs, we assume the existence of a routing protocol that enables nodes to build optimal paths between source and destination nodes. We also assume the existence of a Trusted Authority (TA) that registers OBUs and RSUs by providing them with public and private keys.

Our model assumes that the TA can be used for the pseudonym management of the system as well. We suppose the TA is aware of the existence of all RSUs and has a communication link with them. Hence, it is responsible for the generation of the pool of pseudonyms to be used by all vehicles and for the management of their distribution across the RSUs, which in turn manage the allocation of the pseudo-nyms to the vehicles. It goes without saying that the distribution of the pseudonyms should not be haphazard, as it is mandatory that no duplication, no session disconnections, and minimal message link ability occur. Moreover, frequent pseudonym changing on one protocol layer is not sufficient, since it does not prevent the attacker from linking messages to a sender by making use of the fixed addresses on another layer. Hence, it is required that the pseudonym framework supports pseudonymity on several protocol layers.

In our system, OBUs uses IPv6 data services to communicate with the TA, and so an issue is the compatibility with WAVE. Although the WAVE standard supports IPv6 data services, the recommendations for the operation of IPv6 over WAVE in the standard are rather minimal. There are operational issues for providing access to infrastructure-to-vehicle (I2V) IP-based applications in 802.11p/WAVE networks, like the fact that IPv6 works under certain assumptions for the link model which do not necessarily hold in WAVE. For instance, IPv6 assumes symmetry in the connectivity among neighboring interfaces, but interference and different levels of transmission power may cause unidirectional links to appear in WAVE. On the other hand, there are solutions that have appeared in the literature for providing I2V/V2I IP-based communications in 802.11p/WAVE networks, like the VIP-WAVE framework. We assume the existence of such a solution that enables IP-based communications between the TA and the OBUs, or alternatively, the OBUs may use the cellular network to connect to the TA.

II. LITERATURE SURVEY

In order to achieve unlinkability between two beacons, a vehicle updates its pseudonym regularly. However, according to despite the pseudonym update, a mobile node can still be tracked. The temporal and spatial relation between the new and old locations of the mobile node maintains the link ability between the new and old pseudonyms. As a solution to this problem, the authors in [7] propose the use of a silent period where a car is

enforced to remain silent for a randomly chosen period. During this period, the vehicle is not allowed to disclose neither its old pseudonym nor its new one, which introduces ambiguity and masks the temporal and spatial correlations. The authors do not address the issue of the number of pseudonyms available and any management mechanism for their renewal. Furthermore, they change pseudonyms at the MAC layer (i.e., MAC addresses), and do not perceive the need to change addresses on all layers. But, if the MAC address is changed and the IP address is the same in packets, nodes can then be tracked by their IP addresses.

The authors in [8] state that even when changing pseudonyms at random intervals, the attacker could still identify nodes using several approaches that could depend on the direction of mobile nodes, their density, or beacon frequency. They propose the use of context information such as the number of neighbors, their directions, and speed for initiating a pseudonym change rather than changing them haphazardly. In this approach, nodes change their pseudonym when they are surrounded by nodes that provide a good camouflage for changing. Basically, a node waits for the pseudonym it holds to expire, and until its "context" is suitable for changing them. To assess how suitable the mix context is, the nodes should monitor the surroundings to find a point where the entropy after the change will be sufficiently high. At such a point the node finds several other nearby nodes with similar status, and changes its pseudonym. That work however only focuses on the effectiveness of changing pseudonyms, and does not provide mechanisms for the management of pseudonym generation and refilling.

The authors in [9] also state that status information (position, speed and direction) found in the beacons sent by vehicles facilitate attacks on vehicles. They propose a pseudonym change algorithm to provide a high probability for two vehicles of same status to change their pseudonyms simultaneously. The vehicle adds a change flag to its beacon, and sets it to 1 when the time of its current pseudonym expires. When a node receives beacons from k vehicles with similar status and change flags equal to 1, the node changes its pseudonym. In that work, the authors however assume that the pseudonyms are installed in advance and do not mention how the vehicles are supplied with them and what number of pseudonyms is sufficient. They also fail to mention any mechanism that supplies the vehicle with new pseudonyms after their depletion, and hence they presumably assume the reuse of the pseudonyms by the same vehicle.

Similarly, the authors in [10] propose a synchronized pseudonym changing protocol, which aims to increase the number of close by vehicles that change their pseudonyms simultaneously. In this protocol, vehicles form groups, where each group has a leader that is given by the TA a group secret key, a public key certificate, and a group identifier. Each member in the group also has a secret key known by the group leader. For pseudonym changing, the leader randomly chooses a time to change the pseudonyms and informs all members, prompting them and itself to change pseudonyms simultaneously. The authors then propose an analytical model to evaluate their protocol and compare it to other suggested protocols. However, and similar to other works, they do not provide a mechanism to update the pseudonyms given to vehicles to avoid their depletion or reuse.

Similar to the concept of mix zone, the work in [14] proposes to change pseudonyms at social spots, which are usually crowded with cars. They state that when cars change their pseudonyms at those points, their next beacons will be indistinguishable as they will include the same information, i.e., same location and a zero velocity. Unlike the previously discussed approaches, the authors propose a method to provide cars with pseudonyms, suggesting for the TA to provide users rather than cars with anonymous keys to be saved by the users, but not in their vehicles. When on the move, the user self-generates the pseudonyms from the key for use with upcoming messages. The authors use the anonymity set metric to evaluate their scheme in large and small social spots, but assume the continuous availability of social spots, which is not always the case, like on long highways with a low density of cars.

In [15] the concept of silent periods and synchronized pseudonym changing were combined with a basic idea that vehicles do not transmit beacons when their speed is less than some threshold, but they change pseudonyms during such periods. This, reportedly ensures that vehicles stopping at traffic lights or moving slowly in a traffic jam will refrain from transmitting heartbeats and change their pseudonyms nearly at the same time and location. Interestingly, the authors criticize their own approach by stating that refraining from sending beacons is in contradiction with safety, which is the initial and main objective of vehicular communication.

In other words, a system achieves more privacy if pseudonyms have a shorter lifetime, but a frequent changing of pseudonyms can be costly [11]. This is a result of getting the pseudonym from an external authority, in addition to the packet loss that could occur after the node changes its pseudonym and then receives a packet on its old pseudonym. Second comes the issue of addressing, where the use of a pseudonym in one layer allows the attacker to link fixed addresses of other layers [3], and therefore, identify physical vehicles as the senders of particular messages, and all information in the messages will be exposed.

Another challenge is the negative correlation between privacy and security [3]. The more privacy achieved, the harder it is to provide services such as non-repudiation and accountability [4]. Non-repudiation is preventing a node from denying an action it performed or a message it sent, while accountability is the ability of tracking back a malicious behavior and knowing who was behind it. Anonymity, on the other hand, ensures that a vehicle is not identifiable. Thus, it seems to contradict with non-repudiation and accountability. An anonymity providing architecture designed for vehicular networks should then provide mechanisms in which nodes can be tracked and held accountable for malicious behavior. Last but not least are the complications pseudonyms create on geographic routing, which relies on fixed identifiers of neighboring nodes. Frequent pseudonym changes disturb proper routing functionality, decreases routing efficiency, and increases packet loss, as analyzed and described in [5].

III. NS2 – NETWORK SIMULATOR TOOL

NS2 [21] is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. It implements network protocols TCP and UDP, traffic source behavior of FTP, Telnet, Web, CBR and VBR, router queue management mechanism of Drop Tail, RED and CBQ, routing algorithms Dijkstra and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. NS2 has gained popularity in the networking research community since its birth in 1989.

The Fig.1 shows the simplified user's view of NS. NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler, network component object libraries and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). To setup and run a simulation network, an user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library and instructs traffic sources when to start and stop transmitting packets through the event scheduler. When an user wants to make a new network object, he or she can easily make an object either by writing a new object or by making a compound object from the object library and plumb the data path through the object.

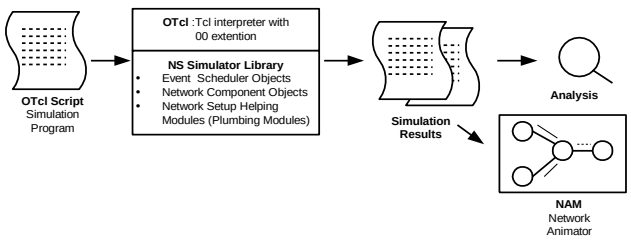

Fig. 1 Simplified User's View of NS

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). C++ is used to define the internal mechanism of the simulation objects, OTcl is used to set up simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and OTcl are linked together using TclCL. NS2 provides a large number of built-in C++ objects. It is advisable to use these C++ objects to set up a simulation using Tcl simulation script. After simulation, NS2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used. NS2 supports multiple protocols which is a positive factor in demand and popularity of the simulator. Due to this feature of NS2, it is an appropriate simulator for many networks. NS2 supports protocols of TCP/IP at different OSI layers. Some of the protocols such as TCP, UDP, CBR, and FTP are application layer of OSI model protocols.

IV. PROPOSED WORK

Fig. 2 shows the RSUs an additional role in the proposed privacy framework, where they will work together and with the TA to distribute pseudonyms to passing vehicles. The use of RSUs to assist in privacy preservation in VANETs, as several frameworks has exploited this aspect to use them for distribution of pseudonyms, keys, and tokens. The number of pseudonyms available for use is directly related to the privacy achieved since a larger number allows for a higher frequency of pseudonym changing and hence more privacy. The RSUs, on the other hand, have a larger amount of resources, specifically storage capacity, and can hold a huge number of pseudonyms as compared to OBUs.

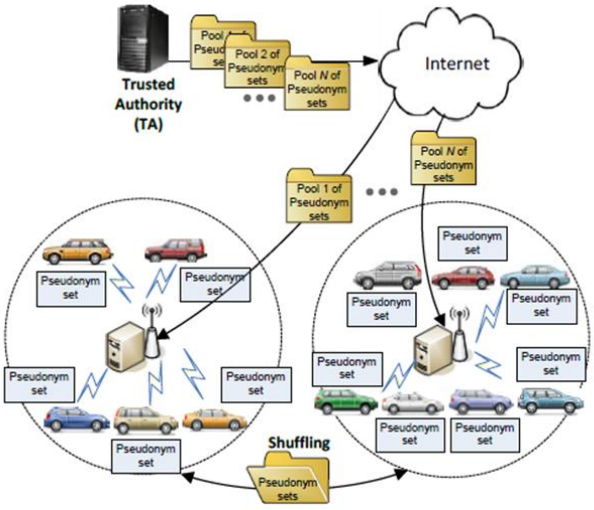

Fig. 2 System Architecture

The proposed system is divided into four modules namely Vehicles Registration, Generating Address for Vehicles, Pseudonym Management and Performance Evaluation.

Vehicles Registration

In this module the vehicles are registered if it's entered first time. Travelling Agent is aware of the existence of all RSUs and has a communication link with them. Hence, it is responsible for the generation of the pool of pseudonyms to be used by all vehicles and for the management of their distribution across the RSUs, which in turn manage the allocation of the pseudonyms to the vehicles. To achieve this, a car needs to announce the upcoming SCH that it is going to switch to. This opens the door for privacy violations, as it would allow an eavesdropping attacker to link conversing cars together, and also learn about their interests, given that a car's next service channel is a clear indicator of its interests. This issue is worsened by the fact that such information is transmitted as routine "HELLO" messages periodically during the CCH. Additionally, due to the wireless nature of VANETs, all messages sent by a car are heard by other nodes that are within its transmission range.

Generating Address for Vehicles

Similar to other networked hosts, a vehicle uses two addresses: the MAC address, which is a 48-bit address that uniquely identifies a node at the link layer, and the 128-bit IPv6 address that is used for communications within the network. Hence, using one fake address on one layer of the protocol stack is not sufficient as messages with the same address at the other layers can be linked to the same vehicle. Cryptographically generated addresses (CGAs) are IPv6 addresses generated by computing a hash function using public key and additional parameters. The OBU then generates a set of pseudonyms together with appropriate certificates. Those addresses are then distributed to the vehicles through the RSUs. The CGA algorithm uses a 128-bit random number and a public key to generate the interface identifier which is then concatenated with a subnet prefix to form the IPv6 address.

Pseudonym Management

This pseudonym will be used by the car to communicate with the first RSU and request a set of pseudonyms. The TA then sends the public keys of all registered cars to all the RSUs to be used for authenticating the cars, as describe later. After generating N pseudonyms, the TA distributes the pseudonym sets to the RSUs, where the number of sets given to an RSU is determined based on the density of traffic surrounding it. Hence, during registration, the RSU informs the TA of the average flow rate λ of cars in its locations which is assumed to be known and determined by traffic engineers. Obviously, an RSU with a higher traffic flow rate is given a larger pool of pseudonyms than RSUs with lower λ. When the RSU receives the pool, it updates its POOLSIZE value which indicates its needs at the moment. However, this value might not be reflective of the number of cars the RSU is servicing at all times. For this, the RSU monitors λ by counting the number of pseudonym requests it is receiving per hour as shown in Fig. 3.

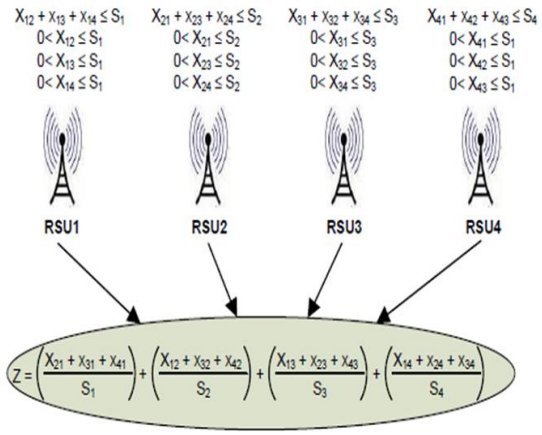

Fig. 3 Distributed Pseudonyms Shuffling Problem

Performance Evaluation

The performance of the network can be evaluated through (1) System Effectiveness, (2) Overhead, (3) Throughput.

1. System Effectiveness: To evaluate the efficiency of our system, we simulate a scenario using the network simulator ns2 that comprises a 10 km highway, with RSU's placed 500 m apart (consistent with rates). More specifically, the figure shows how higher car arrival rates increasingly offset the low communication activity in the network, which is justifiable since the total number of communicating vehicles, which may be approximated by the product of the arrival rate and the activity level.

2. Overhead: The main variables affecting the amount of overhead are the average car speed and the wireless transmission speed, as they both determine how often cars cross the boundaries of the RSU transmission ranges, thus triggering distribution of pseudonym sets and increasing the frequency of shuffling. The growth of wireless overhead traffic per RSU in response to increasing both the average car speed and the wireless transmission range of cars.

3. Throughput: The throughput can be measured by the simulations by choosing a random vehicle as a target and calculate the anonymity set to be the number of vehicles that change pseudonyms simultaneously with the tracked vehicle. Divide our results to scenarios where vehicles use only one pseudonym at a time and other scenarios where vehicles are allowed the simultaneous use of multiple pseudonyms for each active session.

V. RESULTS AND DISCUSSION

Fig. 4 shows the Vehicular Network Formation consists of Travelling Agent, Road Side Units, and vehicles are moved in roads for starts communication.

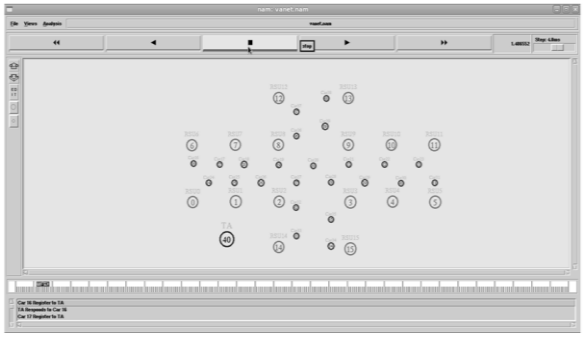

Fig. 4 Vehicular Network Formation

Fig. 5 shows the message transmission among road side units and vehicles to transmit packets from source to destination.

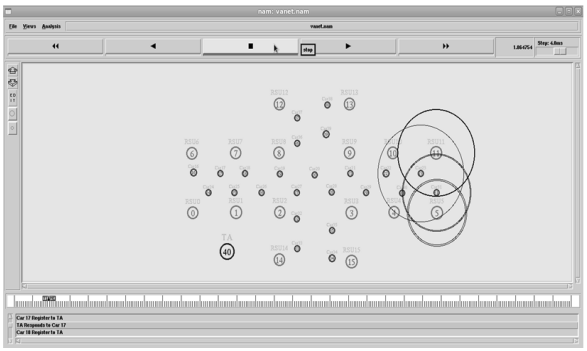

Fig .5 Message Transmission

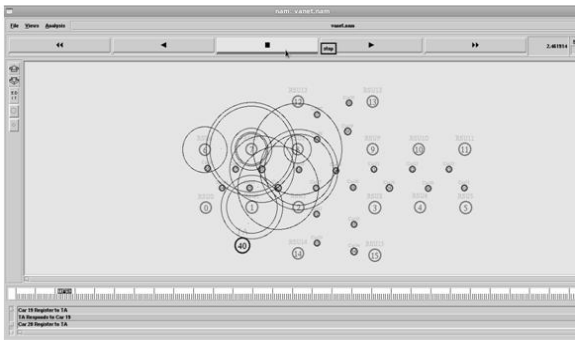

Fig. 6 Vehicle enters to Transmission

Fig. 6 shows when the new vehicle enters to transmission area first it's registered into travelling agent. The below Fig.7 represent the pseudonym transmission between the registered vehicles and the Transmitting agent.

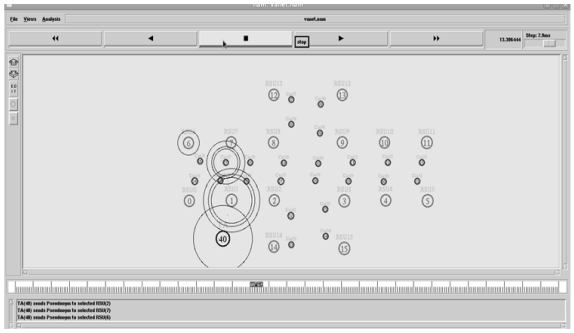

Fig. 7 Pseudonym Transmission

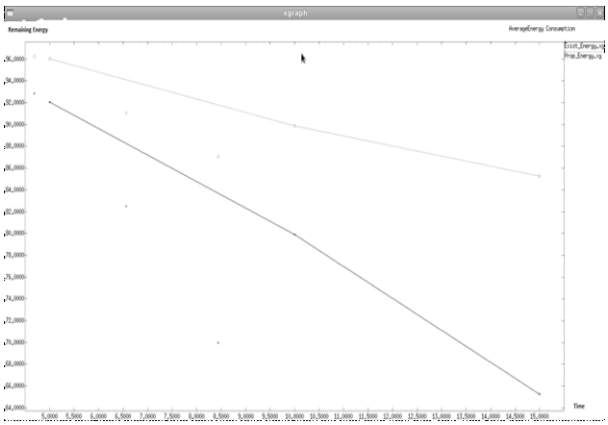

Fig. 8 Energy Conversation ranges between proposed VT and DSR approach

Fig. 8 represents the energy conversation ranges between proposed VT and DSR approach and VT saves more energy.

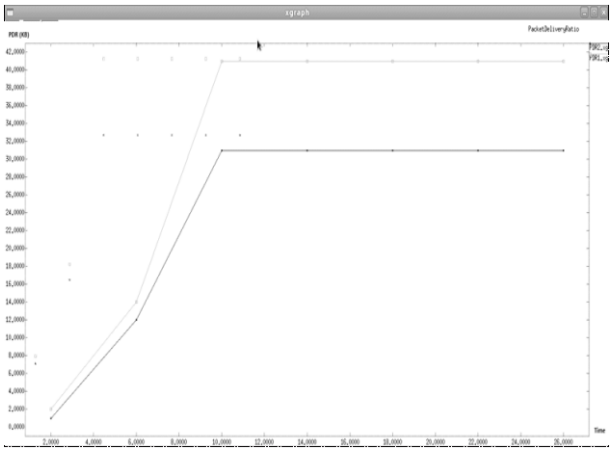

Fig. 9 Packet Delivery Ratio between proposed VT and DSR approach

Fig. 9 represents the packet delivery ratio between proposed VT and DSR approach and VT sends more number of packets with respective to time. The below Fig. 10 represents the packet drop ratio between proposed VT and DSR approach and VT shows less number of packet drops.

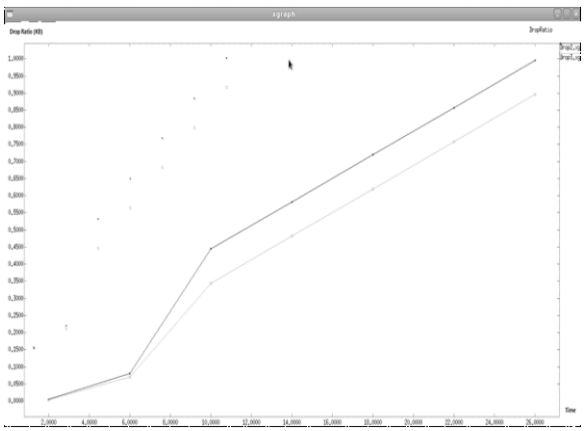

Fig. 10 Packet Drop Ratio between proposed VT and DSR approach

VI. CONCLUSION AND FUTURE WORK

The proposed work consists of an anonymity framework for vehicular ad hoc networks based on the use of pseudonyms. The framework comprises as main elements a Trusted Authority, the Road Side Units (RSU's), and the vehicles themselves. Introduced an innovative pseudonym management system that distributes pseudonym sets to vehicles in response to particular events that depend on vehicle speeds and how distant the RSU's are from each other. Our performance results show the ability of the system to maintain a sufficiently large anonymity set that is meant to confuse the attacker..

REFERENCES

[1] D. Jiang, L. Delgrossi, "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments", In IEEE Vehicular Technology Conference, pp. 2036-2040, 2008.

[2] M. Raya, J.P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, 2007,15(1),39-68.

[3] E. Fonseca, A. Festag, R. Baldessari, R. Aguiar, "Support of anonymity in vanets-putting pseudonymity into practice", In IEEE Wireless Communication and Networking Conference, pp. 3400-3405, 2007.

[4] H. Jayasree, A. Damodaram, "Anonymity and accountability in web-based transactions", Advanced Computing,3(2).

[5] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets", In Security and Privacy Ad-Hoc and Sensor Networks,Springer Berlin Heidelberg,pp. 43-57, 2006.

[6] A. Pfitzmann, M. Köhntopp, "Anonymity unobservability and pseudonymity - a proposal for terminology", In Designing Privacy Enhancing Technologies, Springer Berlin Heidelberg pp. 1-9, 2001.

[7] L. Huang, K. Matsuura, H. Yamane, K. Sezaki, "Enhancing wireless location privacy using silent period", In IEEE Wireless Communication and Networking Conference,2(2005),1187-1192.

[8] M. Gerlach, F. Guttler, "Privacy in VANETs using changing pseudonyms — ideal and real", In IEEE Vehicular Technology Conference, 2521-2525, 2007.

[9] J. Liao, J. Li, "Effectively changing pseudonyms for privacy protection in vanets", In 10th International Symposium on IEEE Pervasive Systems, Algorithms, and Networks, 648-652, 2009.

[10] H. Weerasinghe, H. Fu, S. Leng, Y. Zhu, "Enhancing unlinkability in vehicular ad hoc networks", In IEEE International Conference Intellingence and Security Informatics,161-166, 2011.

[11] J. Freudiger, H. Manshaei, J. Y. Le Boudec, J. P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks", IEEE INFOCOM, 1-9, 2010.

[12] M. Gruteser, D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis", Mobile Networks and Applications,10(3),315-325, 2005.

[13] F. Armknecht, J. Girao, A. Matos, R. L. Aguiar, "Who said that? privacy at link layer", Proc. IEEE INFOCOM, 2521-2525, 2007.

[14] R. Lu, X. Li, T.H. Luan, X. Liang, X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets", IEEE Transactions on Vehicular Technology,61(1), 86-96, Jan. 2012.

[15] L. Buttyán, T. Holczer, A. Weimerskirch, W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets", In IEEE Vehicular Networking Conference, 1-8, 2009.

[16] DOT Press Release, February 3,2014,http://www.dot.gov/press-release?tid_1=All&items_per_page=10&page=24.

[17] USA TODAY,"cars that 'talk' to each other move a step closer",july 2013,[online].Available:

[18] http://www.usatoday.com/story/money/cars/2013/07/01/connected-car-technology-dsrc-nhtsa-mandate/2439659/

[19] Automotive News,U.S. regulators pave way for vehicle-to-vehicle communications, safety technology,February,2014.Available:

[20] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks", IEEE Transactions on Vehicular Technology,(62)2,536-551,2013.

[21] The Network Simulator NS2", [Online]. Available: http://www.is.edu/nsnam/ns/.