ISSN 2348 – 9928
IJAICT Volume 1, Issue 1, May 2014 doi:01.0401/ijaict.2014.01.02 Published Online 05 (05) 2014

# A STUDY OF SIGNCRIPTION WITH GROUP SIGNATURE BASED AUTHENTICATION IN VEHICULAR AD-HOC NETWORK

*A. M. Arul Raj*
*Associate Professor,*
*Dhaanish Ahmed College of Engineering,*
*Tamilnadu, India*

*Dr. Naganathan*
*Professor & Head, Department of CSE,*
*Hindustan University,*
*Tamilnadu , India*

***Abstract*— Vehicular ad hoc networks are emerging as an effective technology for providing a wide range of safety applications to by-vehicle passengers. VANET is a special class of Mobile ADHOC Networks (MANET), in which the nodes are the vehicles which communicate with other vehicles or with the base station which acts as a roadside infrastructure for using security and services application. The most favorable target is the more useful, efficient and safer roads will built through vehicular networks by informing to basic authorities and drivers in time in the future. If a vehicle changes its certificate between two observation points controlled by an attacker while moving in the same lane and with the same speed on the road, an attacker can correlate the certificates used by that vehicle and hence track the vehicle. The proposed system overcomes the location privacy with the Signcryption is a new paradigm in public key cryptography. A remarkable property of a signcryption scheme is that it fulfills both the functions of public key encryption and digital signature, with a cost significantly smaller than that required by signature-then-encryption. The purposes of this paper are to demonstrate how to specify signcryption schemes and to examine the efficiency of such schemes. A signcryption is a primitive that provides private and authenticated delivery of messages between two parties. Proxy signature schemes are variations of ordinary digital signature schemes and have been shown to be useful in many applications. We proposed an identity-based signcryption scheme from the group signatures. Also we analyze the proposed scheme from efficiency and security points of view. Group signature is given for those security properties. We have shown that the signcryption scheme is as efficient as ordinary identity-based signcryption schemes under certain circumstances.***

***Keywords — Authentication , group signature, Signcryption.***

## I. INTRODUCTION

### *1.1 Vehicular ad-hoc network (VANET)*

***a) Definition :*** In VANETs, authentication with privacy preservation is any process by which a system verifies the approved identity of a vehicle that wishes to access it, whereas the confidential private information will not be disclosed, when that disclosure would cause either embarrassment or distress to the vehicle of reasonable sensitivities.

***b). Objectives****:* We endeavor to construct an authentication framework with privacy preservation using ID-based key management for different kinds of communication in VANETs. For authentication, the RTA preloads an ID pool of regional RSUs into a vehicle, and the RSU ID pool does not need to update/replenish unless the RSU ID changes or increases. For the vehicle privacy, we utilize a form of self-defined pseudonyms as real-world IDs without exposing privacy. Therefore, a vehicle can change its pseudonym anytime it wants for privacy preservation. The goal of the proposed authentication framework is to guarantee the privacy-preserving authentication in VANETs.

A special class of Mobile Ad-Hoc Networks (MANETs) is vehicular ad-hoc network (VANET) in which, nodes self-organize and self-manage information in a distributed fashion [1]. A vehicular ad-hoc network (VANET) is a type of network which is formed by combination of vehicles and infrastructure points [2]. Infrastructure points are called road side units (RSUs). RSUs are positioned at definite space on the road, alike an access point in conventional wireless ad hoc networks for providing compulsory infrastructure support for network setup and communications. There is no need of fixed infrastructure, like base station or, mobile switching center in VANET [3]. In vehicular ad-hoc network (VANET) the communication can either be among vehicle (vehicle-to-vehicle) or between vehicle and infrastructure (vehicle-to-infrastructure) [1] [2] [3] [4].

### *1.2 Importance of authentication in VANET*

In general, a secure network should have the following attributes: authentication, non-repudiation, confidentiality, data integrity, Access Control and availability. Authentication is the verification of a user identity prior to granting access to the network. It can be considered as the first line of defense against intruders. Non-repudiation is the verification that the data was sent with a user credentials so that without denial or repute the data can be associated to the sender. Confidentiality is the assurance that the data could not have been accessed by any other user than the designated recipient for whom it was meant; thus insuring that the data was untouched until reception. Confidentiality is generally achieved by cryptography techniques. Data integrity is the assurance that the content of the data was not modified while in transit. It differs from confidentiality in the sense that it allows for detection of data modifications. Availability is the proportion of time that a system is in a functioning state. Each of these attributes brings its network requirements whose balance and compromises make network security challenging.

### *1.3 The illustration of VANET architecture*

A VANET with guaranteed security basically consists of three network components as shown in Figure 1: Road Side Units (RSUs), vehicles (users) and a Regional Trusted Authority (RTA). The figure show VANET consisting of a RTA, finite numbered registered RSUs along roads, and a large number of vehicles on or by the roads. We suppose that, the RSUs are always reliable, while vehicles are vulnerable to being compromised by attackers. The wireless communication in VANETs can be classified mainly into three types, Vehicle-to-Roadside (V2R) communication, Roadside-to-Vehicle (R2V) communication, and Vehicle-to- Vehicle (V2V) communication. Other communications are through secure channels, such as inter-RSU communication and RSU-to-RTA communication.

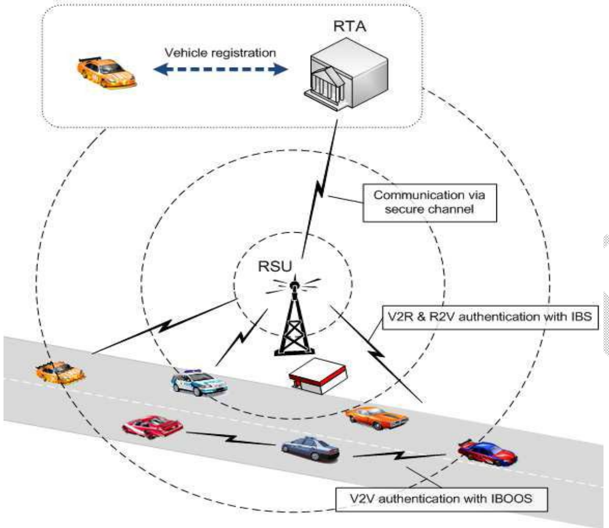
RTA
Vehicle registration
Communication via secure channel
RSU
V2R & R2V authentication with IBS
V2V authentication with IBOOS

*Fig- 1. The network structure and component in VANET*

### *1.4 Attacks in VANET*

#### *i. Impersonation attack:*

The attacker pretends to be another entity. It can be performed by stealing other entity's credential. As a consequence, some warnings sent to a specific entity would be sent to an undesired one.

#### *ii. Sybil attack:*

The attacker uses different identities at the same time. In this way, e.g., a single attacker could pretend vehicles to report the existence of a false bottleneck in traffic.

#### *iii. Attacks on privacy:*

Attacks on privacy over VANETs are mainly related to illegally gathering sensitive information about vehicles. As there is a relation between a vehicle and its driver, exposure of vehicle's situation could affect its driver privacy

#### *iv. Identity revealing attack:*

Getting the owner's identity of a given vehicle could put its privacy at risk. Usually, a vehicle's owner is also its driver, so it would simplify getting personal data about that person.

#### *v. Location tracking attack:*

The location of a vehicle in a given moment, or the path followed during a period of time is considered as personal data. It allows building that vehicle's profile and, therefore, tracking its driver. Mechanisms resisting the attacks on both authentication and privacy are required in VANETs. They must satisfy the tradeoff between privacy and utility.

### *1.5 Attackers in VANET*

Attacker create problem in the network by getting full access of communication medium. Here we are discussing some properties and capability of the attackers

#### *a) Insider*

This type of attackers who is an authentic user of the network and have detail knowledge of network. Insider attacker might have access to insider knowledge and this knowledge will be used for understanding the design and configuration of network. When they have all information about the configuration then it's easy for them to launch attacks and create more problem as compare to outsider attacker. It can create problem in the network by changing the certificate keys. We can simply say that insider attacker is the right man doing the wrong job in the network.

#### *b) Outsider*

The outsider attacker is considered as an authentic user of the network. It is a kind of intruder which aims to misuse the protocols of the network and the range of such attacks are limited. Outsider attacker also has a limited diversity for launching different kind of attacks as compare to insider attacker.

#### *c) Coverage area*

Coverage area is the main property of attacker when they launch any kind of attacks. Attacker could cover the main area of road, and it depends on the nature of the attacks. Basic level attacker has controlled and covers the range of at most 100 meters but the extended level attackers are more organized and cover more area using of hundred channels.

#### *d) Technical Expertise*

Technical expertise of the attacker makes them stronger for creating attacks in the network. It is difficult for attacker to mount attacks on cryptographic algorithms. Chance is low for attacker to compromise the infrastructure network and data capture from restricted area of network. Attacker having ability to extracts the program code.

## II OVERVIEW OF SIGNCRYPTION

In this paper, we present a new concept called signcryption scheme (SS).This is an important cryptographic primitive that must be used to protect privacy and authenticity of a collection of users who are connected through an ad-hoc network, such as Bluetooth. We also present an efficient Signcryption scheme based on secure delivery of data. As a regular signcryption scheme, this scheme combines the functionality of signature and encryption schemes. However, the idea is to have an identity based system. In our scheme, a user can anonymously sign-crypts a message on behalf of the group. This shows that our scheme outperforms a traditional identity based scheme that is obtained by a standard sign-then-encrypt mechanism, in terms of the length of the cipher text. We also provide a formal proof of our scheme with the chosen cipher-text security under the assumption.

### *2.1 Security and authentication in signcryption*

Secure and authenticated message delivery and storage is the major aims of computer and communication security research. The current standard method to achieve this is to have signature followed by encryption. The cost of secure and authenticated message delivery and storage is possible to transport or store messages of varying length in a secure and authenticated way with an expense less than that required by signature followed by encryption.

To avoid forgery and ensure confidentiality of the contents of a message , for centuries it has been a common practice for the originator of the message to authenticate on it and ten send to the deliverer. A signcryption scheme is a cryptographic method that fulfills both the functions of secure encryption and group signature, but with a cost smaller than that required by signature then encryption. Using the terminology in cryptography, it consists of a pair of algorithms (S,U), where S is called the signcryption algorithm, while U the unsigncryption algorithm. S in eneral is probabilistic, but U is most likely to be deterministic. (S,U) satisfy the following conditions.

- ***Unique unsigncryptability –*** given a message m, the algorithm S signcrypts m and outputs a signcrypted text c. on input c, the algorithm U unsigncrypts c and recovers the original message UN – ambiguously.
- ***Security –*** (S,U) fulfill, simultaneously, the properties of a secure encryption scheme and those of a secure group signature scheme. These properties mainly include: confidentiality of message contents, enforceability, and non-repudiation.
- ***Efficiency –*** The computational cost, which includes the computational time involved both in signcryption and unsigncryption, and the communication overhead or added redundant bits, of the scheme is smaller than that required by the best currently known signature-then-encryption scheme with comparable parameters.

A direct consequence of having to satisfy both the second and third requirements is that signcryption is not equal to signature-then-encryption. These two requirements also justify our decision to introduce the new word signcryption which clearly indicated the ability for the new approach to achieve both the functions of signatures and secure encryption in a logically single operation.

### *2.2 Applications of signcryption*

As discussed in the introduction, a major motivation of this work is to search for a more economical method for secure and authenticated transactions/message delivery. If digital signcryptions are applied in this area, the resulting benefits are potentially significant: for every single secure and authenticated electronic transaction, we may save 40% in computational cost and 75% in communication overhead.

Some signcryption schemes are compact and particularly suitable for smart card based applications. They will find innovative applications in many areas including digital cash payment systems and personal health cards. Of particular importance is the fact that signcryption may be used to design more efficient digital cash transaction protocols that are often required to provide with both the functionality of digital signature and encryption .

## III. COMMUNICATION THROUGH SIGNATURES

### *3.1 Digital Signature*

Cryptographic digital signatures are applied to messages or hashes over messages to provide authenticity, integrity protection and non- repudiation. Digital message signatures are commonly using public-private key cryptography. Messages or hashes over the respective messages are signed with the message originators private keys.

By using private key, it is guaranteed that the messages originate from nodes holding the required cryptographic key material and the messages have not been altered by intermediate forwarding nodes. The message receiver verifies the integrity and authenticity of the messages, by using the corresponding public keys. The node cannot be impersonated because the node only knows private key. In any message sent by a vehicle should be digitally signed specially safety messages or warning messages. Furthermore, messages that serve as input or triggers to the safety system could also be signed. The main advantage is the requirements for digitally signature are very small i.e. the nodes need a possibility to receive or create and store cryptographic key pairs. They need the processing power for creating and verifying message signatures. Main disadvantage is Message forging and denial of service (DoS) attacks are possible.

### *3.2 Digital Signatures with Digital Certificates*

The signatures can be combined with digital certificates provided by a trusted third party. The basic assumption with certificates is that nodes, which include certificates in their messages, are trusted by other nodes that are able to verify the certificates. Certificates are provided by trusted third party and Digital Signature provides Data integrity also.

The distribution of certificates is limited to valid VANET nodes, for example communication systems inside vehicles or roadside equipment. Since nodes having obtained a valid certificate can only create new valid active safety messages, this excludes outside attackers. Obviously, this statement holds only, if we can assume that those attackers have no certified keys and if they are unable to extract any from valid nodes. Owner identification might also be used for other legal aspects, not directly linked to active safety application, which is out of scope for this document. The advantages of the digital signature with certificate are:

The possibility to exclude external attackers from the system, the ability to remove malicious or defective nodes.

### *3.3 Group signature*

In our system, after receiving a secret member key from an RSU, each vehicle can anonymously send messages on behalf of the group maintained by this RSU, by using a group signature scheme. Group signatures allow the members of a group to sign on behalf of the group. Everyone can verify the signature with a group public key while no one can know the identity of the signer except the group manager. Further, it is computationally hard to decide whether two different signatures were issued by the same member. In this In case of a dispute, a designated group manager can reveal the actual identity of the signer; we employ a group signature scheme to secure V2V communication.

Due to the security requirements of VANETs, the group signature scheme employed should satisfy the following properties:

- ***Unforgeability.*** Only the group members can sign messages on behalf of the group. This fulfills the "*message authentication*" requirement in VANETs.
- ***Unlinkability.*** Deciding whether two different valid signatures were computed by the same group member is computationally hard for anyone except the group manager. This can deal with the "*privacy protection*" requirement in VANETs.
- ***Traceability.*** The group manager is always able to open a valid signature and identify the signer. In this paper, the TM acts as the group manager, and it can use this property to address the "*anonymity revocability*"

## IV. SYSTEM MODEL

We consider a typical VANET, which consists of a top trusted authority (TA), some stationary RSUs deployed at the roadsides, and a large number of vehicles equipped with moving on the road, as shown in the following figure

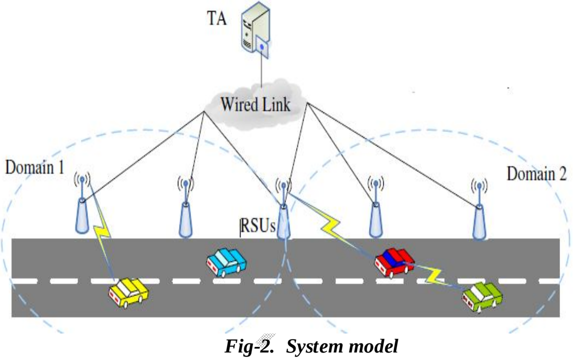

***Fig-2. System model***

### *4.1 Trusted Authority (TA):*

TA is fully trusted by all parties in the system and in charge of the registration of RSUs and vehicles. The TA can divide its huge precinct into several domains and deploy RSUs at the boundary between these domains. The domain information is available to all entities. As usual, TA is assumed powered with sufficient storage capability and infeasible for any adversary to compromise.

### *4.2 RSUs:*

RSUs act as the infrastructure of VANET and connect with the TA by wired links in the system. They provide service for information dissemination and certificate updating. In general, the density of RSU varies in different domains. Without loss of generality, the cantonal domains are supposed to have the similar RSU density while the domains in suburb may have a small number of RSUs. The pseudonymous certificates issued by an RSU can only be used in the domain where the RSU locates. As a distributed unit deployed on the roadside, an RSU has risk to be compromised. Although TA can detect a compromised RSU and take action to recover it, the records stored in the RSU maybe have been leaked.

### *4.3 Vehicle:*

Vehicles equipped mainly communicate with each other for sharing local traffic information and improving the driving experience. A vehicle frequently requests the certificate service from an RSU and obtains enough certificates for the following period until passing by another RSU. Obviously, the number of the updated pseudonymous certificates depends on the RSU density. The vehicle changes the pseudonymous certificates periodically to sign routine traffic messages.

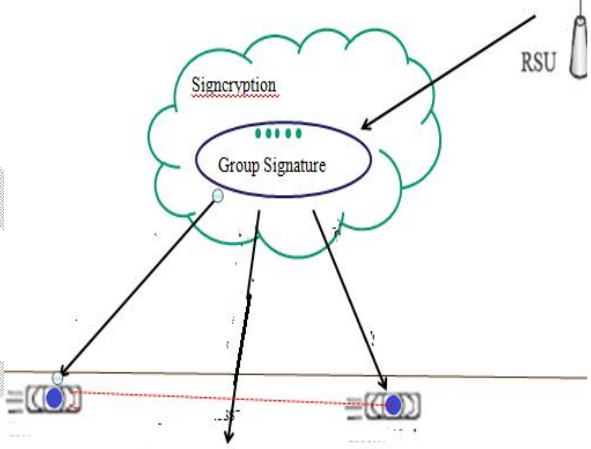

***Fig-3. Signcryption with group signature.***

### *4.4 Signature based authentication system:*

In this system an attack is detected if the data matched with malicious behaviors that are already registered. The system has a database behavior of confident attacks with which are evaluated the data collected. This technique may demonstrate low false positive rates, but at detecting earlier strange attacks it does not perform well [11] [12].

### *4.5 Group level authentication*

In Group level authentication the message is confirmed to instigate from a certain group of nodes. There are two techniques of authentication, which are: 1) group signature schemes and 2) pseudonyms. In signature scheme, a private key is given to each user, with which it signs the message. Pseudonyms also help in privacy protection [4].

The RSU assign a group signature to all the trusted nodes for authentication. This is a private key which is generated using Signcryption [17]. A group signature permits the members of a group to sign on behalf of the group. After receiving a private key from an RSU, each vehicle can secretly send messages on behalf of the group maintained by this RSU.

## V. CONCLUSION

Presence of the attacks in the network or misbehaving nodes in the network one of the major security issues for the VANET which is also affecting the performance of the vehicular ad hoc network. In this paper we discussed the infrastructure design for VANET security. Important parameters of VANET security framework designs along with the constraints of designing the security framework for VANET are discussed here. From this paper we want to clear that for the strong security of VANET communication we not only needs the strong cryptography algorithm but also one need the strong communication framework or strong routing algorithms those can easily detects the malicious vehicles from network and mitigate them.

The fundamental security functions in VC will consist in authenticating the origin of a data packet. Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities. Authentication helps also to control the authorization levels of vehicles. In this paper, requirements and methods of authentication in VANETS are discussed. Digital signatures and Digital Certificates have been discussed comprehensively. Working, advantages and disadvantages of digital signatures with digital certificates have been discussed. Then RSU assign a group signature to {TN} for authentication. This is a private key which is generated using Signcryption [17]. A group signature permits the members of a group to sign on behalf of the group. After receiving the private key from an RSU, each vehicle can secretly send messages on behalf of the group maintained by this RSU. Thus the attacks can be avoided.

## VI. **FUTURE DIRECTION**

The future work we will work on framework design based on new algorithm which can detect and mitigate the malicious vehicles from network and reduced the packet drops while maintaining the throughput. The future direction requires studying different possible authentication types for vehicular network. And Design an efficient, Reliable and cost-effective mechanism for authentication in vehicular ad-hoc.

### References

[1] Ayonija Pathre, Chetan Agrawal and Anurag Jain, "Identification of Malicious Vehicle in Vanet Environment from Ddos Attack", Journal of Global Research in Computer Science, Volume 4 No 6, 30-34, ISSN-2229-371X, June 2013

[2] [2] Brijesh Kumar Chaurasia and Shekhar Verma, "Infrastructure based Authentication in VANETs", International Journal of Multimedia and Ubiquitous Engineering, Vol. 6, No. 2, April, 2011

[3] [3] M.Erritali, B. EL Ouahidi, B.Hssina, B. Bouikhalene and A. Merbouha, "An Ontology-Based Intrusion Detection for Vehicular Ad Hoc Networks", Journal of Theoretical and Applied Information Technology, Vol. 53 No.3, and ISSN: 1992-8645, 31st July 2013.

[4] [4] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic, "Data-centric Misbehavior Detection in VANETs", Vehicular Technology Conference (VTC Fall),5-8 Sept, 2011, IEEE, ISSN : 1090-3038, Print ISBN: 978-1-4244-8328-0. doi>10.1109/VETECF.2011.6093096

[5] [5] Khalid Haseeb, Dr.Muhammad Arshad, Dr.Shazia Yasin and Naveed Abbas, "A Survey of VANET's Authentication", Liverpool John Moores University, ISBN: 978-1-902560-24-3 © 2010 PGNet, Jun 2010

[6] [6] Huang Lu, Jie Li and Mohsen Guizani, "A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs", Computing, Communications and Applications Conference (ComComAp) IEEE, 11-13 Jan. 2012, Print ISBN: 978-1-4577-1717-8, doi: 10.1109/ComComAp.2012.6154869

[7] [7] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah and Jamalul-lail bin Ab Manan, "Classes of Attacks in VANET", Electronics, Communications and Photonics Conference (SIECPC),Saudi International, IEEE, 24-26 April 2011, Print ISBN: 978-1-4577-0068-2, doi: 10.1109/SIECPC.2011.5876939

[8] [8] Mrs.Kadam Megha V, "Security Analysis in VANETs: A Survey", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012, ISSN: 2278-0181.

[9] Aikaterini Mitrokotsa, Manolis Tsagkaris and Christos Douligeris, "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms", IFIP International Federation for Information Processing Volume 265, 2008, pp 133-144

[10] Tim Leinm¨uller, Albert Held, G¨unter Sch¨afer and Adam Wolisz, "Intrusion Detection in VANETs", 12th IEEE International Conference on Network Protocols (ICNP 2004), Student Poster Session, Berlin, Germany, October 5th - 8th, 2004

[11] Mohammed ERRITALI, Bouabid El Ouahidi, "A Survey on VANET Intrusion Detection Systems", International Journal of Engineering and Technology (IJET) ISSN: 0975-4024 Vol 5 No 2 Apr-May 2013

[12] Paul Brutch and Calvin Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks", SAINT-W '03 Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), Page 368 , IEEE Computer Society Washington, DC, USA ©2003, ISBN:0-7695-1873-7

[13] Yongguang Zhang, Wenke Lee and Yi-An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, Volume 9 Issue 5, September 2003, Pages 545 - 556, ISSN: 1022-0038, doi>10.1023/A:1024600519144

[14] SANS Institute InfoSec Reading Room, "A Paper On Intrusion Detection System", © SANS Institute 2001, As part of the Information Security Reading Room.

[15] Cheng Tan, Hao Sun, Ning Cao, Lihui Sun, Cheng Li, "A Novel Grey Game-Theoretic Model for Intrusion Detection in Vehicular Ad Hoc Network", ICCSEE-13, Advances in Intelligent Systems Research, ISBN:978-90-78677-61-1, ISSN: 1951-6851, doi:10.2991/iccsee.2013.140, January 2013

[16] M. Mehdi, S. Zair, A. Anou and M. Bensebti, "A Bayesian Networks in Intrusion Detection Systems", Journal of Computer Science 3 (5): 259-265, 2007, ISSN 1549-3636 © 2007 Science Publications

[17] Lei Zhang, Qianhong Wu, Agusti Solanas and Josep Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications", Vehicular Technology, IEEE Transactions Volume: 59, Issue: 4, May 2010, ISSN: 0018-9545, INSPEC Accession Number: 11285973, doi: 10.1109/TVT.2009.2038222

[18] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen and Jinshu Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehic*ular Communications"*, Vehicular Technology, IEEE Transactions, Volume:59 , Issue: 7 , Sept. 2010, Pg3589 - 3603, ISSN : 0018-9545, INSPEC Accession Number: 11523632, doi : 10.1109/TVT.2010.2051468

[19] Hsu-Chun Hsiao, Ahren Studer, Fan Bai, Bhargav Bellur and Aravind Iyer, *"Flooding-Resilient Broadcast Authentication for VANETs"*, MobiCom '11, 17th annual international conference on Mobile computing and networking, Pages 193-204, ISBN: 978-1-4503-0492-4, doi>10.1145/2030613.2030635, 2011