ISSN:0975-9646

Public Key Infrastructure (PKI) using Symmetric Key Cryptography (SC) in VANETs

Sumegha Sakhreliya[#1], Neha Pandya[*2]

[#]IT Department, Parul Institute of Engineering and Technology, GTU
Vadodara, India

[*]Asst.Professor, IT Department, Parul Institute of Engineering and Technology, GTU
Vadodara, India

***Abstract*— Vehicular Ad-Hoc Network (VANETs) provides the vehicle to vehicle (V2V) communication for the safety application. There are many security requirements in VANETs. ECDSA algorithm fulfils all the security requirements but it's come with the processing overhead and there is a chance of computation based DoS attack. However the VANETs are the time constrained each safety message should be reached at a time to other vehicles. TESLA uses the symmetric key cryptography that is MAC algorithm but it is not that much scalable as compared to ECDSA because of multi-hop communication is not possible in TESLA and also it uses the delay key disclosure so till that the message and MAC has to be stored in the memory so there is chances of memory based DoS attack in TESLA. So if we use the MAC algorithm in the classical PKI system in place of ECDSA algorithm than it can reduce the processing overhead associated with ECDSA so time will be low for each message authentication and it also mitigate the problem of memory based and computation based DoS attacks that can be useful for the VANETs safety related applications as safety applications are time constraint.**

***Keywords*— OBU, TPM, PKI, Group Signature, ECDSA, TESLA, MAC.**

I. Introduction

In 2007 , road accidents have cost 110 deaths ,4600 injuries and €438 millions daily in the European Union. The damage is similarly devastating in the United States with 102 deaths, 7900 injuries and $630 millions [1] daily therefore Vehicular ad hoc networks (VANETs) have appealed to many research interest now a days from academic, from research scholar and deployment efforts from industries [2].VANET applications can be divided in to three types 1) safety-related 2) traffic optimization and 3) infotainment [1].

VANETs are a subset of MANETs (Mobile Ad-hoc Networks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes, eventually dispersed in different roads[16].In the vehicular ad-hoc networks (VANETs) intelligent vehicles can communicate among themselves (Vehicle-to-vehicle(V2V) communication) and with the road-side infrastructure (Vehicle-to-Infrastructure (V2I) communication) as shown in the below Fig.1.Moreover, a large number of Certificate Authorities (CAs) or Trust Authority (TAs) will also exits ,where each CA is responsible for the identity management of all vehicles registered in its region (e.g. National territory ,district ,country) [6][20].

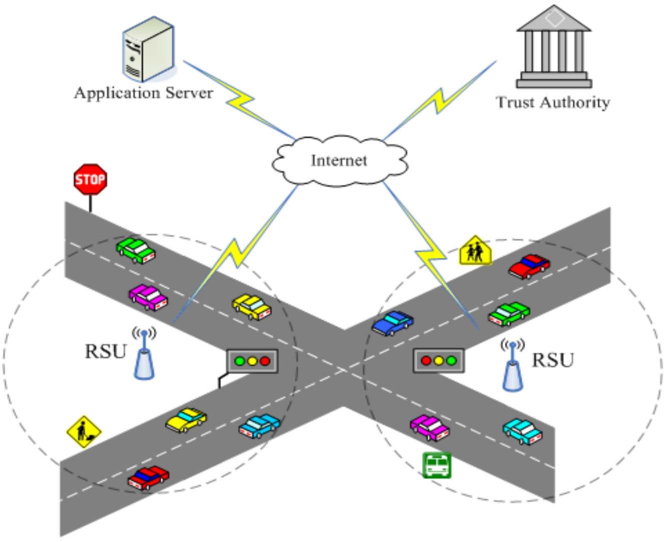

Fig 1.VANETs Example

It is anticipated that vehicles equipped with the wireless communication devices can communicate with each other and the roadside units (RSUs) located at critical points such as intersections. Vehicles are expected to communicate by means of the Dedicated Short-Range Communication Protocol (DSRC) standard, which applies the IEEE 802.11p standard for wireless communication. To offer communication with participants out of radio range, the messages could be forwarded by other vehicles (Multihop Communication)[2][3][18].

Trusted Platform Modules (TPMs) or Tamper Proof Devices (TPDs) is often mounted on vehicles. These devices are especially interesting for security purposes, as they offer reliable storage and computation. They usually have a reliable internal clock and are supposed to be tamper-resistant or at least tamper-evident. In this way, sensitive information (e.g. user credentials or pre-crash information) can be reliably stored [15][16].The organization of this paper is as follows: In section II survey of related work, section III contains the brief of proposed work, section IV contains simulation results and section V conclusion.

II. Related Work

Many research work has been done related to security issues in the VANETs safety related applications. There are various security requirements in VANETs. When we talks about all this security requirement than PKI is the most suitable and old technique to achieve all this goals that are given by the authors in papers [1][4][14].In paper [12] Raya and Hubaux proposed PKI system with it advantages and disadvantages. In 2007 Raya and Hubaux proposed PKI system with multiple certificates that are preloaded in the vehicle to provide privacy with classical PKI system [15].The disadvantage of the scheme is that there is need to change certificate at the time interval which is time consuming. In ABAKA scheme [2] the authors had consider the conditional privacy and also provided the use of the pseudoidentity to hide the actual identity of the vehicle. In AMOEBA [10] scheme authors had considered the privacy issue and proposed the group signature scheme to provide privacy. However in AMOEBA the real identity is with group manager. The selection of group manager done randomly so there are chances that malicious vehicle can be selected as group manager and thus the real identity of all vehicles can leak. In the paper [1] authors proposed the overhead of ECDSA algorithm for providing the security in VANETs and also there are chances of computation based DoS attack [3].In TESLA scheme authors use MAC algorithm in place of ECDSA thus reduce the complexity but, still there is need to store MAC and Message in memory till the key disclose and thus chances of memory based DoS attack[13].In paper [3] authors proposed the VAST scheme that is the combination of MAC and Signature but, still in this there is need to store key and self-generated MAC in memory till key discloses.

III.Proposed Work

A. System Preliminaries

For the proposed scheme that is PKI-SC we have taken the classical PKI system. In the PKI system there is one certificate authority that is CA is used for the credential management and authentication of the vehicles and after registration process it provides the certificate and the pair of the public and private key to the vehicle. After that this private key and certificate it can use for the communication with the other vehicles within the VANETs [16].The vehicles communicate with the CA via RSU (Road Side Unit) which is known as the online registration else it can directly communicate with CA that is known as the offline registration [16].

We assume that each vehicle will be equipped with the tamper proof device, which is secure against any compromise attempt in any circumstances [2][12][15]. Note that the use of tamper proof device is recommended by current VANET Security standards to reduce the risk of vehicle compromised by adversaries. Due to tamper proof device no adversary can steal data that is stored in the device [2].Here we used the MAC algorithm that is the symmetric key cryptography algorithm in place of the ECDSA algorithm that is the asymmetric key cryptography algorithm in classical PKI system so; it can provide the benefit of PKI system and reduce the time overhead associated with ECDSA algorithm.

B. System Model

The below detail shows the how the authentication of the vehicle done with the CA, and how the one vehicles will authenticate the other vehicle.

1. *Registration of New Vehicle to CA*

The below procedure show authentication of the new vehicle to CA and, generation of pseudoidentity and secret key. For the privacy preservation the CA is responsible for generating random pseudoidentity and corresponding secret key. Fig. 2 shows registration of new vehicle to CA.

I. *Authentication Module: OBU*

This step is required to ensure that the car user is the valid user and is not a malicious vehicle so any other person will not be able to get access of the vehicle's OBU.A user inputs its password in activate the OBU to pass the verification process. Password PWVi that is in form of the bits. If the password is valid than only RVIDi (Registration Number) is delivered to the Certificate Authority (CA)[2] ; otherwise the taper-proof device will not be activated that is attach with OBU to store the sensitive data for OBU so, an adversary cannot get any information. Each vehicle have the Registration Number is stored within the OBU's Tamper -Proof device that cannot be changed by attacker [2][5][15].

Table 1
Notations Used for Proposed System

Notation	Description
Vi	Vehicle Vi
RVIDi	Registration Number of vehicle Vi
PWDi	Password of the Tamper Proof device for vehicle Vi
Ti	Time Stamp of vehicle Vi
SKVi	Secret Key or Secret Number for vehicle Vi sent by CA
PUVi	Public Key of vehicle Vi sent by CA and store in certificate
TCA_Ti	Current Time Stamp of CA

II. *Authentication Request Procedure of the Vehicle to CA*

If the password of the tamper proof device is correct than only the tamper proof device will be activated and the RVIDi (Registration Number) is delivered to the certificate authority (CA).Certificate authority which registers the vehicles before they are allowed to operate on the road and that cannot be compromised.

- There are many ways to check the reply attack. Here we choose the use of time stamp because each OBU can perform time synchronization using the tamper-proof device [2][12].To mitigate with the reply attack the Vi first generate the Ti that is the current timestamp.

- Now by using the tamper proof device the Vi will pass its RVIDi and the time stamp to the Certificate Authority. Other vehicles can also know the real identity of other vehicles by using the other things like camera etc. But, we are not considering that because it is out of scope. Here the real identity of the vehicle RVIDi will be passed to the Certificate Authority (CA) so it can store and can track the vehicle if there is some misbehaviour done by the vehicle so here we are considering the conditional privacy preservation.

III. *Vehicle Credential Verification by CA*

- When the CA will get the message then it will first check weather $\Delta T \geq TCA\_Ti - Ti$ is valid, where ΔT is the transmission delay for the network and that is predefined and the TCA_Ti is the current time of the Certificate Authority (CA).If it is valid, then go to next step; otherwise, the CA will ceases this connection because it might be a reply attack [2].
- Pass RVIDi of that vehicle to the next module that is the Pseudoidentity & Secret key Generation Module.

IV. *Registration Procedure Done By CA*

The below shows the registration procedure that is done by Certificate Authority (CA) to authenticate the vehicle and provide it public key and secret key.

- **Secret Key Generation:** To generate the secret key the CA will choose a random number.
- **Public Key Generation :** To generate the public key (PUVi) the (RVIDi)⊕(SKVi) operation will be done that will generate the public key for that vehicle.Here the Registration Number is stored in the Tamper Proof device and cannot change by the vehicle itself and if vehicle want to change registration number it has to go for the customer service centre and have to change so it is unique and unchanged for the vehicle so here we used registration number as the private key for vehicle for the authentication requirement.
- **Pseudoidentity Generation:** To provide the privacy to the vehicle the real identity of the vehicle that is RVIDi is only known to the Certificate Authority (CA) and we will use the pseudoidentity generation using the random number to provide the identity of the vehicle which will hide the real identity of the vehicle and will provide the privacy. Pseudoidentity will be generated by the (PUVi)⊕(Random Number) operation.

V. *Pass Secret Key and Certificate to Vehicle by CA*

After the successful registration of the vehicle to Certificate Authority (CA) the Certificate Authority (CA) will pass the secret key SKVi and Certificate to the vehicle Vi.The secret key will used by the vehicle to generate its private key.Certificate Authority (CA) will pass the secret key to the vehicle. Now the registration number is stored in the vehicle's Tamper Proof Device so the vehicle will perform same operation with its RVIDi and secret key that is performed by the CA to generate the private key for that vehicle.As the registration number cannot change by vehicle by its own so no other vehicle can generate the same key that the CA has for that vehicle though other vehicle will get the secret key.

The vehicle will do the operation between its own RVIDi and the secret key which it gets and will generate the same key as the generated by the CA and passed in the Certificate to use that key to encrypt the message so other vehicle can authenticate it. That Key and the certificate will be stored in the tamper proof device of that vehicle Vi so that it cannot be misused by anyone else without password. Here we assume that the vehicle will change the secret key and pseudoidentity of itself periodically to provide privacy as per the requirement so certificates will not be preloaded in the vehicle.

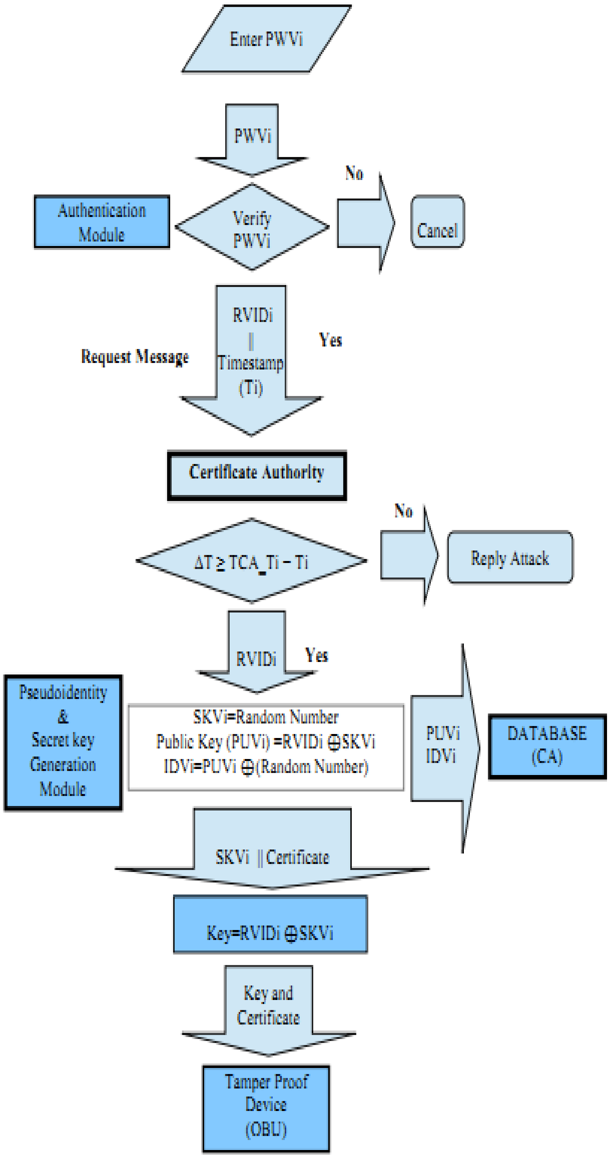

Fig. 2 Flow of Secret Key and Public Key Generation by CA

2. ***Vehicle-to-Vehicle (V2V) Communication***

The below procedure shows how the other vehicle will authenticate the message, that is send by the sender vehicle from the message of the sender vehicle.

I. Message Generation By the Vehicle

When the Vehicle Vi wants to send the message to the other vehicle than it will use its key and MAC algorithm to generate the MAC of the message and will attach the Certificate with it and will send this message to other vehicles. The format of message is shown in below Fig. 3.Here we are generating our private key by the same operation the Certificate Authority (CA) does to generate the public key so both key are the same so its provides the symmetrical cryptography and we can use MAC algorithm to send the message to other vehicle which provide less processing and communication overhead.

The Secret Key is provided by the Certificate Authority (CA) and that is only known to that vehicle Vi and the Certificate Authority (CA).After registration process the CA will send RVIDi and secret key SKVi to the vehicle. At the vehicle side they both will be stored in the tamper proof device of the vehicle. So, they cannot be steal by any other vehicle or user and it cannot be changed by the vehicle itself because the tamper proof devices are the tamper resistance or the tamper evidence [12][16].The example of the tamper proof device is the smart card that store all the sensitive information on the chip within it.

Certificate
Message
MAC, MAC Key

Fig. 3 Message Format Used By Proposed System

We can compare the communication overhead of the traditional PKI scheme and our PKI-SC scheme as from the below Table 2.

Table 2
Comparison of Communication Overhead

Scheme	**Message Size (Byte)**
PKI	262 B
PKI-SC	232 B

II. Message Authentication by the Other Vehicles

When the other vehicle Vi will get the message than it will again produce the MAC of the message by using the public key that is stored in the certificate that is attached with the message send by the sender vehicle. If the both of the MAC matches than the message will be accepted otherwise the message will be dropped. The whole verification process is shown in below Fig. 4.

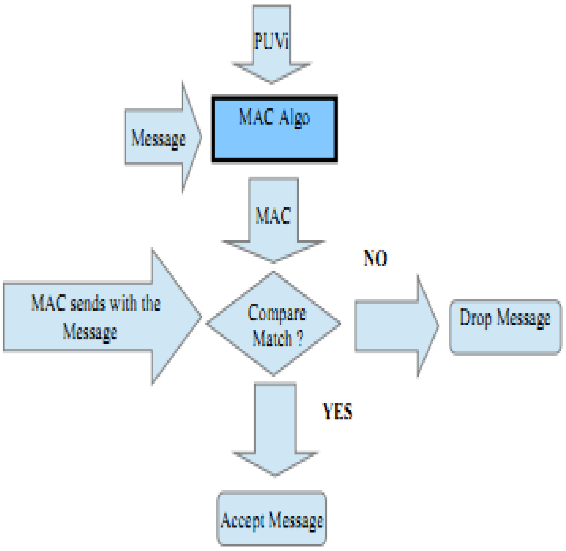

Fig. 4 Flow of Message Verification Process Done by Other Vehicles

IV.Simulation Results

VANET relies on the two simulators for its smooth functioning that are the Traffic Simulators and the Network Simulators [19].These both the simulators work independently but to fulfill the need of the VANETs solution required to use these both simulators together. Here as a network simulator NS2 has been used and as a traffic simulator the MOVE and simulators are used. The traces that are generated by the SUMO cannot be used by NS2 directly because it is the traffic simulator that's why MOVE works as a parser for parsing that traces for NS2[19].Here the highway of 3 lanes has been used for the simulation purpose. The communication range used is the 250 meter. The below table shows the simulation parameters that are used for simulation of our system and comparison with the existing system.

Table 3
Simulation Parameters for NS2

Packet size	232 , 262 byte
Packet Interval	100– 300 ms
Transmission Range	250 m

A. Generate the Highway Scenario

Fig. 5 Visualization of Vehicles on Highway in NAM Animator

For the simulation purpose the first requirement is to produce the proper traffic scenario. For that MOVE has been used to generate the configurable number of nodes for the proposed system with SUMO. The highway scenario generated by MOVE is shown in Fig. 5.

B. Comparison of Communication Delay

For comparison of the communication delay for PKI system and PKI-SC system we have used the packet size that is shown in Table 2.The results for the communication delay is shown in Fig. 6.

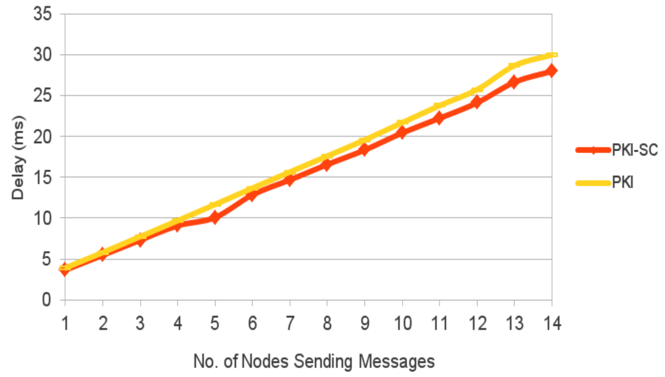

Fig. 6 Communication Delay Comparison

C. Comparison of Processing Delay

For comparison of the processing delay for PKI system and PKI-SC system we have used the processing time that we find by implementing ECDSA and MAC algorithms for PKI and PKI-SC system respectively on the sender and receiver nodes. The time we get by implementing that algorithms are shown in Table 3.

Table 3
Comparison of Processing Time

Scheme	Message Generation	Message Verification
PKI	2 ms	5 ms
PKI-SC	26 µs	26 µs

Fig. 7 shows the signature generation and verification delay using the ECDSA algorithm that is generated from Eq.1 [1] and the time we get for existing and proposed system in Table 3.

$$NTX = 2N_L\lambda pR \qquad (1)$$

Here, $\mathbf{N_L}$ is the number of lanes, **λp** is the density of vehicles (veh/km/lane), **R** is the communication Range. From the graph in Fig. 7 we can conclude that the processing time or authentication time for proposed system is very low compared to existing PKI system that is very near to message without security. So, authentication overhead is removed in proposed system and it will also provide the authentication which is required for VANETs safety related applications which are time constraint.

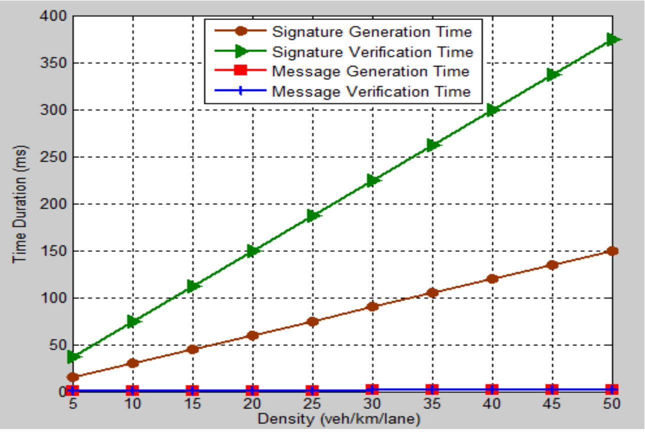

Fig. 7 Processing Delay Comparison

V. CONCLUSION

In this paper we have proposed the PKI-SC system that is Public Key Infrastructure (PKI) using Symmetric Key Cryptography (SC) in VANETs that use the symmetric key cryptography algorithm. Asymmetric key cryptography algorithms are more complex than, symmetric cryptography algorithm and takes more time. The problem with symmetric key cryptography is that we need to change the key else if someone will steal the key than message will be disclose but, here we are using the vehicle registration number that is store in OBU of vehicle as a key that is unique and cannot change by owner. From results we can conclude that it provides security and processing time is low for proposed system so, there is no issue of authentication overhead as in ECDSA. Communication delay is also reduced in proposed system. It also provides multi-hop communication that is not possible in TESLA. In future work we will find processing delay issue in the form of braking distance of vehicles.

ACKNOWLEDGMENT

Sumegha Sakhreliya – I would like to thanks my parents and my family for their support. I would also like to thanks my guide Neha Pandya for her guidance.

REFERENCES

[1] Jonathan Petit and Zoubir Mammeriautheticato,”Authentication and consensus overhead in vehicular ad hoc networks”,Published online: 24 August 2011 © Springer Science+Business Media, LLC 2011,Telecommun Syst (2013) 52:2699–2712 ,DOI 10.1007/s11235-011-9589-y, ISSN:1572-9451.

[2] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien,”ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks” in IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 60, NO. 1, JANUARY 2011,ISSN: 0018-9545.

[3] Ahren Studer, Fan Bai,Bhargav Bellur and Adrian Perrig,”Flexible, Extensible, and Efficient VANET Authentication”,IEEE JOURNAL ON SPECIAL ISSUE ON SECURE WIRELESS NETWORKING,VOL 11, NUMBER 6, DECEMBER 2009 ,ISSN 1229-2370.

[4] Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow,”EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks”,IEEE TRANSACTIONS ON MOBILE COMPUTING,VOL. 12,NO. 1,JANUARY 2013,ISSN 1536-1233.

[5] Chen Lyu, Dawu Gu, Xiaomei Zhang, Shifeng Sun, Yinqi Tang,”Efficient, Fast and Scalable Authentication for VANETs”,2013 IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS,ISSN:0018-9545.

[6] Ameneh Daeinabi and Akbar Ghaffarpour Rahbar,"Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks",Published online: 5 April 2011 © Springer Science+Business Media, LLC 2011,Multimed Tools Appl (2013) 66:325–338 DOI 10.1007/s11042-011-0789-y, ISSN:1572-9451.

[7] Yong Hao, Yu Cheng, Chi Zhou, Senior Member, and Wei Song,"A Distributed Key Management Framework with Cooperative Message Authentication in VANETs",IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011, ISSN:0018-9545.

[8] Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures,"Efficient Certificate Management in VANET",2nd International Conference on Future Computer and Communication,2010.

[9] Jason J. Haas, Yih-Chun Hu and Kenneth P. Laberteaux,"The impact of key assignment on VANET privacy",SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks. (2009) Published online in Wiley InterScience (www.interscience.wiley.com) DOI: 10.1002/sec.143.

[10] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran,"AMOEBA: Robust Location Privacy Scheme for VANET",IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 25, NO. 8, OCTOBER 2007, ISSN:0018-9545.

[11] Mark Hartong,Rajni Goel and Duminda Wijesekera,"Key Management Requirements for PTC Operations",IEEE VEHICULAR TECHNOLOGY MAGAZINE , JUNE 2007,ISSN:1556-6072.

[12] Maxim Raya and Jean-Pierre Hubaux, "The Security of Vehicular Ad Hoc Networks", Laboratory for computer Communications and Applications (LCA),2005.

[13] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “The TESLA broadcast authentication protocol,” in RSA CryptoBytes, 2002.

[14] Mrs. Arzoo Dahiya and Mr. Vaibhav Sharma"A survey on securing user authentication in vehicular ad hoc networks".

[15] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[16] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda,"Overview of security issues in Vehicular Ad-hoc Networks".IGI Global 2010 (www.igi-global.com).

[17] Don Johnson ,Alfred Menezes and Scott Vanstone,"The Elliptic Curve Digital Signature Algorithm (ECDSA)", Certicom Corporation 2001(www.certicom.com).

[18] “Communications in Vehicular Networks” ,Zaydoun Yahya Rawashdeh and Syed Masud Mahmud.

[19] Aamir Hassan,Master’s Thesis in Electrical Engineering,"VANET Simulation",School of Information Science, Computer and Electrical Engineering Halmstad University,2009.

[20] Sumegha Sakhreliya, Neha Pandya, "A Review on Security Issues and Its Solution's Overhead in VANETs", International Journal of Scientific and Research Publications,Nov-2013,ISSN 2250-3153.