A Review on Security Issues and Its Solution's Overhead in VANETs

Sumegha Sakhreliya*, Neha Pandya**

*IT Department, Parul Institute of Engineering and Technology/GTU, India
**CE Department, Parul Institute of Engineering and Technology/GTU, India

Abstract: Vehicular Ad-hoc networks (VANETs) are very likely to be deployed in the coming years because of the safety requirements and thus become the most relevant form of mobile ad hoc networks. Security is the main issue in VANETs because of the main use of the VANETs is for safety related application and in that case the viability of the security may cause harm to human lives. In this paper, we address the security issues of this networks and the methods are used to solve the security issues and its consecuses overhead in VANETs.

Index Terms: OBU, TPM, PKI, Group Signature, ECDSA, TESLA

I. Introduction

In 2007 , road accidents have cost 110 deaths ,4600 injuries and €438 million daily in the European Union. The damage is similarly devastating in the United States with 102 deaths ,7900 injuries and $630 million[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[3].In the vehicular adhoc networks (VANETs) intelligent vehicles can communicate among themeselves (Vehicle-to-vehicle(V2V) communication) and with the road-side infrastructure (Vehicle-to-Ifrastructure (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 identiry management of all vehicles registered in its region (e.g. National territory ,district ,countary) [4][5].

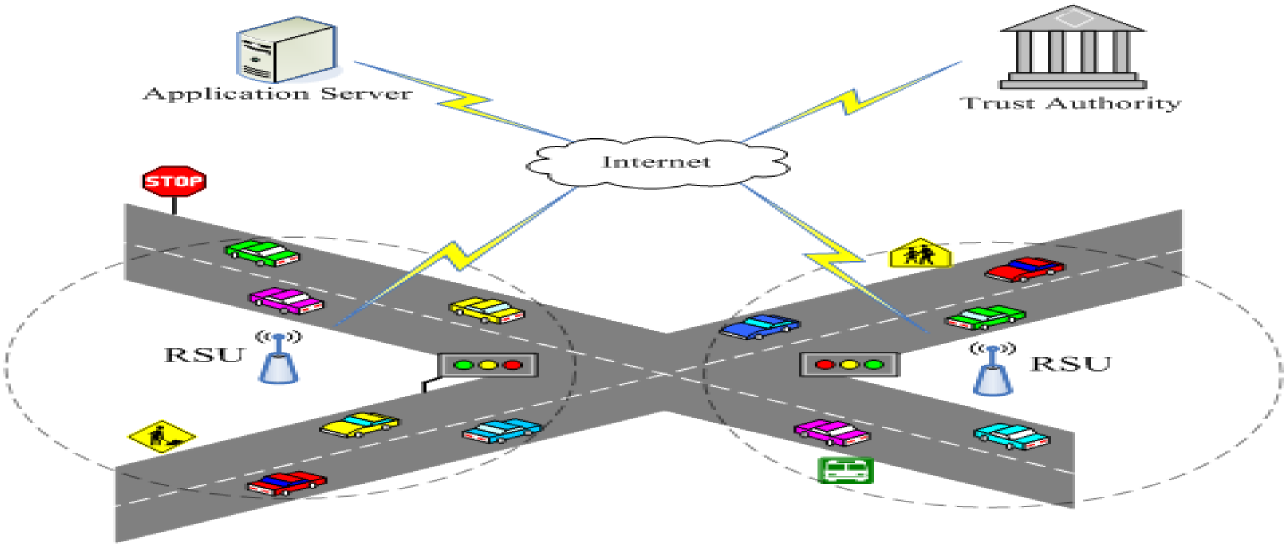

Figure 1.VANETs Example

It is anticipated that vehicles eqipped with the wirelss communication devices can communicate with each other and the roadside units(RSUs) located at critical points such as intersactions.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].

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[3].In this paper in section II we will see different VANET entities,in section III security requirements in VANET,in section IV different VANET schemes, in sectio V ECDSA ,in section VI TESLA and in section VII conclusion.

II. VANET ENTITIES

A. Common VANET Entities

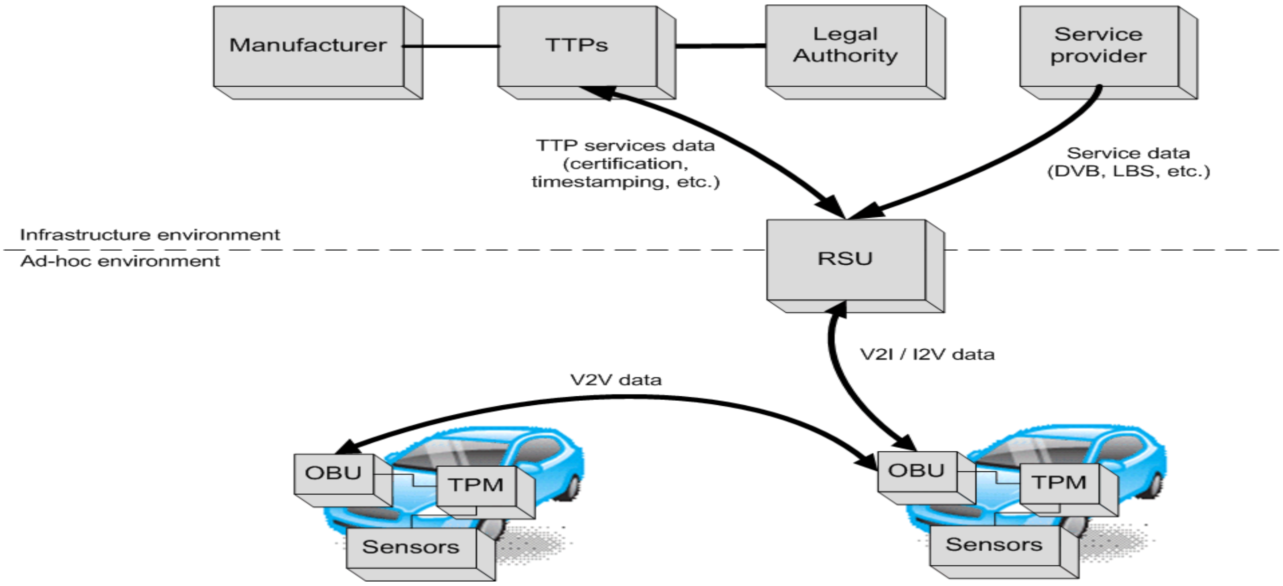

Figure 2.Common VANET Entities

a. Infrastructure Environment:

As shown in above Fig.2 the infrastructure within the upper part of the figure is fixed and that contain following entities[3].

I. Manufactures :As the manufactures are the one who had made the vehicle as the manufacturing process they can identify each vehicle uniquely so they are consider within the VANETs sometimes.

II. Trusted Third Parties :Trusted Third Parties (TTPs) or Central Authority (CA) are used in the VANET for credential Management and provide certficates and provide public/Private key within the VANETs.For its working TTPs are required to communicate with Manufacturer and Legal Authority.

III. Legal Authority :Legal Authority provide the Unique Identification Number that is Registration Number or licence plate number to the vehicles as the part of the registration process.

IV. Service Provider :Service Providers provide the services related to Infotainment e.g.downloading, web surfing and digital video broadcasting and location based services.

b. Ad-Hoc Environment:

As shown in above Fig.2 the infrastructure within the lower part of the figure is Ad-hoc and that contain following entities[3].

I. On Board Unit (OBU) :OBU are mounted on the vehicle and are used for V2V and V2I communication.

II. Trusted Platform Module(TPM) :Trusted Platform Module or Tamper Proof Device is the tamper proof devices and are tamper resistance used to store certificates and secret keys for the vehicle's On Board Unit.

III. Sensors :Sensors are used for gathering vehicles own information e.g fuel consumption and for enviornment e.g road slippery.

B. VANETs Messages Types

Several applications are enabled by VANETs, mainly affecting road safety. Within this type of application, messages interchanged over VANETs have different nature and purpose. Taking this into account, four different communication patterns can be identified[3]:

a. V2V warning propagation

There are situations in which it is necessary to send a message to a specific vehicle or a group of vehicles. For example, when an accident is detected, a warning message should be sent to arriving vehicles to increase traffic safety[3].

b. V2V group communication
In this type of message pattern, only vehicles having some features can participate in the communication. These features can be static (e.g. vehicles of the same enterprise) or dynamic (e.g. vehicles on the same area in a time interval)[3].

c. V2V beaconing

Beacon messages are sent periodically to nearby vehicles. They contain the current speed, heading, braking use, etc. of the sender vehicle. These messages are useful to increase neighbor awareness. Beacons are only sent to 1-hop neighbour vehicles[3].

d. I2V/V2I warning

These messages are sent either by the RSUs to vehicles or a vehicle to RSU when a potential danger is detected. They are useful for enhancing road safety. As an example, a warning could be sent by the infrastructure to vehicles approaching to an intersection when a potential collision could happen[3].

III. SECURITY REQUIREMENTS IN VANETS

A. Security Requirements For VANETs

Along with growth of VANET there are many security and privacy challanges are imerged as below.

a. Entity Identification & Athentication :

Entity Identification imposes that each participating entity should have a different and unique identity. However, identification itself does not imply that the entity proves that it is its actual identity – this requirement is called entity authentication.In V2V warning propagation it needs identification to perform message routing and forwarding – identifiers are essential to build routing tables and sender authentication is needed for liability purposes.[3]

b. Privacy Preservation

Privacy preservation is critical for vehicles. Privacy is achieved when two related goals are satisfied 1) untraceability and 2) unlinkability(Gerlach, 2005).First Property states that vehicle's actions should not be traced (i.e. different actions of the same vehicle should not be related). On the other hand, second property establishes that it should be impossible for an unauthorized entity to link a vehicle ́s identity with that of its driver/owner[3].

However, this privacy protection should be removed when required by traffic authorities.This requirement is present in all V2V communications in case of liability.However it does not apply to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs[3].

c. Non-repudiation

Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received some message. It is needed for the sender in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be employed for liability purposes[3].

In case of I2V and V2I warnings, non- repudiation of origin is needed, so wrong warning messages can be undoubtedly linked to the sending node. Non-repudiation of receipt is not currently needed, but it will be in the future.[3].

d. Confidentiality

Confidentiality, that is, to assure that messages will only be read by authorized parties. This requirement is only present in group communications, in which only group members are allowed to read such information. The remaining VANET settings transmit public information[3].

e Availability

Availability implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment.By Designing communication protocols and mechanisms of such type can save as much bandwidth and computational power as possible can fulfill this requirements. It is present on all communication patterns, that is, it affects not only V2V communications, but also I2V ones[3].

f. Data Trust

Related to the information itself, data integrity and accuracy must be assured.This needs are globally referred as data trust. Data at stake should not be altered and, more importantly, it should be truthful. False or modified data should lead to potential crashes, bottlenecks and other traffic safety problems. For this reason, data trust must be provided on all VANET communications[3].

IV. VANET SCHEMES

A. Public Key Infrastructure (PKI)

In VANETs, the primary security requirements are identified as entity Authentication, Message integrity, and Nonrepudiation. The PKI is the most viable technique to achieve these security requirements[11][14].

In that scheme each vehicle register it self to the Trusted Authority (TA) or the Central Authority (CA).They can either get the credintial online via RSU or either offline by the CA.The Central Authority Provides the Certificate[10] and the pair of Public/Private keys.The public key of the vehicle will be provided to all the vehicles while the vehicle will use its private key to provids the signature to the message by using ECDSA[1][8][13](Elliptic Curve Digital Signature Algorithm).

All implementations of this standard shall support the signing algorithm ECDSA over the two NIST curves p224 and p256.ECC.IEEE 1609.2 suggest the inclusion of an ECDSA[1](Elliptic Curve Digital Signature Algorithm) signature in every packet to provide broadcast authentication,Integrity and Non Repudiation.OBU signs a safety message using its private key, and then sends the message, signature and its certificate OBU OBU : M , Sig⇨ (prk _ OBU , M), cert _ OBU as shown in below Fig 3[1][12].

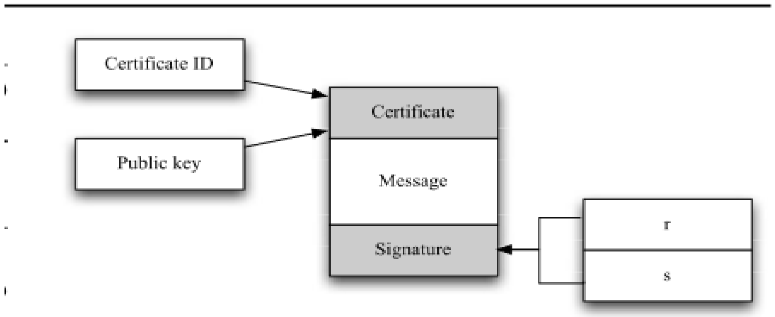

Figure 3. Message Format using ECDSA algorithm[1]

Fixed public keys allow an eavesdropper to associate a key with a vehicle so as to violate driver's privacy.To provide privacy ABAKA scheme provide to use psudoidentity to vehicle[2].

B. Multiple Certificates Per OBU

Raya and Hubaux in 2007 use a classical PKI to provide secure and privacy preserving communications to VANETs.In that the each OBU owns a set of certified public/private key pairs.In this scheme A large set of keys needs to periodically renewed (during regular vehicle maintenance visits)**.**OBUs contact trust authorities through RSUs and send the created pseudonym and public key. Authorities send the built certificates back[12].

In this scheme the vehicle use the private key for short period of time so an evasdropper can not track the vehicle by its key or identity.The drawback of this scheme is that it suffers from a Sybil attack.A malicious OBU can pose as multiple vehicles by using the different private key for short perod of time.Other drawack is that we have to preload vehicle with large number of certificates wich consumes memory and large overhead to revoke a OBU incase of dispute[12].

C. Group Signature

To provide privacy Group Signatures scheme is provided by the Lin et al in 2007.In that scheme the vehicles form the group and the group leader or Group Manager is selected randomly.The real identity of the each vehicle is recorded by the Group manager so Group manager and it only can trace the identity of a signer from the group signature and revoke the group member in case of dispute. That scheme is used by AMOEBA[6].

Group signature guarantees the unlinkability of the messages since group member can anonymously sign on behalf of the group.OBU uses a group signature to sign a message to prove that the signer is a valid OBU (not which OBU).

It reduce the storage cost of multiple public/ private key pairs and the bandwidth consumption used to transmit the certificate revocation list.The drawback of this scheme is Computationally expensive.In the AMOEBA [6] that is based on the group signature scheme in that vehicles form groups. The messages of all group members are forwarded by the group leader, which implies that the privacy of group members is protected by sacrificing the privacy of group leader. Moreover, if a malicious vehicle is selected as a group leader, all group members' privacy may be leaked by the malicious leader[7].

V. ECDSA ALGORITHM

A. ECDSA algorithm

ECDSA is a variant of the Digital Signature Algorithm (DSA), which operates on elliptic curve groups. ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. To use ECC all parties must agree on the elements defining the elliptic curve,which are domain parameters of the scheme. Each participant does not usually achieve the generation of domain parameters since this involves counting the number of points on a curve, which is time-consuming and troublesome to implement it. As a result, NIST and SECG published domain parameters of elliptic curves for several common field sizes. Johnson signature scheme[13] is an algorithm to compute ECDSA, and includes three phases: key generation, signature generation and signature verification.

B. Complexity of ECDSA

a. Scalar multiplication

In ECDSA, a scalar multiplication of a given random point is used in signature generation and verification. This operation is the most time-consuming part of the total signature computation . Specifically, given a n-bit long scalar k and a point P on the curve, we have to compute the elliptic curve scalar multiplication kP.There are two possible algorithms to calculate kP ; the Add-and-Double algorithm and the Montgomery algorithm[1][15].

b. Modular multiplication

Modular multiplication is typically the most critical operation in the computation of elliptic curves scalar multiplication. Given a word length of n bits, an n-bit integer m called the modulus, and two n-bit operands x and y, the problem is the computation of xy mod m[1][15].

c. Modular inversion

The modular inversion is another time consuming operation in scalar multiplication. The Montgomery inversion is a way to compute x −1 mod m. The Montgomery inversion is based on Montgomery multiplication algorithm. Montgomery inverse of an integer x ∈ [1, m − 1] is j = x −1 bn such that where m is prime and n = log2 m is the bit-length.The time complexity of the Montgomery modular inversion is O(n).

d. Time complexity

ECDSA signature generation and verification are fully performed by modular multiplications, squaring, modular inverse and hash functions. So the time complexity of ECDSA is given in function of TMUL , TSQR , TINV and THASH[1][15] .

Signature generation time is:

$$T_{sign} = 2TMUL + TINV + TkP + THASH$$

$$= (6n+2)TMUL + TINV + 5nTSQR + THASH \qquad \textbf{(1)}$$

Signature verification time is:

$$T_{verify} = 2TMUL + TINV + 2TkP + THASH$$

$$= (12n + 2)TMUL + TINV + 10nTSQR + THASH \qquad \textbf{(2)}$$

e. Processing delay

Vehicles have to generate a signature for each message sent and verify signature for each message received. The time required for these operations is called processing delay.ECDSA with a P-224 curve (respectively P-256) fits with an authentication key size of 224 bits (respectively 256). In Table 1, TkP is almost equal to signature generation time[1][15].

Table 1.Operation times on a Pentium D 3.4 GHz workstation

Key (bit) size	TMUL (µs)	TINV (µs)	TkP (µs)	THASH (µs)
224	1.23	18.91	2468.71	8.47
256	1.39	22.01	3297.23	10.09

Table 2, which gives Tsign and Tverify , shows that using P-256 instead of P-224 in the signature generation adds a time overhead of 33.2%. Using P-256 instead of P-224 in the signature verification adds a time overhead of 33.4%. Theoretical analysis of ECDSA shows a linear-time complexity depending on the key size.In Table 3, the processing delay increases when key size increases. These experimentation results validate the analytical model[1][15].

Table 2.Signature generation and verification times on a Pentium D 3.4 GHz workstation

Key size (bit)	Signature generation (ms)	Signature verification (ms)
224	2.50	4.97
256	3.33	6.63

VI. TESLA

A. TESLA

TESLA has a low overhead since it is built on symmetric cryptography. To secure TESLA, both the sender and receivers are loosely time synchronized[8]. It means that the synchronization is not strictly precise, but the receivers requires to know an upper bound on the sending time.Consider the chain of length n with the values K1 , . . . , Kn for time intervals I1 , . . . , In . TESLA can generate this chain by choosing the last value Kn randomly and repeatedly using a one-way hash function H to derive the previous keys: Ki =H(Ki+1)∀i∈ {0,...,n−1} . The value K0 serves as a commitment to the entire chain, which is used to authenticate the following values of the chain[9].

Moreover, TESLA uses a second hash function H to derive the key Ki : Ki = H (Ki), which can be used to compute the Message Authentication Code (MAC) of message for each time interval.If a sender wants to broadcast a message for the interval Ii,it broadcasts mi , the MAC M ACKi (mi) and the disclosure key Ki−d , where d is the delay interval of key disclosure.Receivers store the message and MAC until the key Ki is broadcast as the key remains secret for the future d − 1 intervals. Then, receivers recover the commitment by iteratively invoking the hash function, and apply the valid key to check the stored MAC[9].

The Drawback of TESLA is that it does not provide the Non repudiation as it is using the symmetric key cryptography algorithm[8].In TESLA as it is using the delay key disclosure technique it has to wait for authentication till the key disclose[9].The below Table 3. shows the time required by MAC algorithm.

Table 3.Computation time of MAC algorithm

Operation	Comp.Time
MAC,MAC Key	1µs

VII. CONCLUSION

In this paper we had seen the various schemes use in VANET to solve the various security issues.We had also discuss the various cryptogarphy schemes that are both symmetric cryptography and asymmetric cryptography scheme and also disscuss the problems with them.so,still this schemes used to provide the various security are come with some computational and processing overhead.The time require to use assymetric cryptography requires more time than symmetric cryptography while symmetric key cryptography used in TESLA requires storage of MAC till the key disclosure.So there is a scope of development of some scheme that gives benefits of both of the cryptographic schemes.

ACKNOWLEDGMENT

I would like to thanks to my guide for guiding me and encourage me to write this paper and all of my faculty to help me to clear my doughts on this topic and also to my family to always there to support me.

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.

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”,IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 60, NO. 1, JANUARY 2011.

3.José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda,”Overview of security issues in Vehicular Ad-hoc Networks”.

4.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.

5.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.

6.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.

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.

8.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).

9.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.

10.Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures,”Efficient Certificate Management in VANET”.

11.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

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

13.Don Johnson ,Alfred Menezes and Scott Vanstone,”The Elliptic Curve Digital Signature Algorithm (ECDSA)”

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

15.Jonathan Petit,”Analysis of ECDSA Authentication Processing in VANETs”,IEEE @ 2009.

AUTHORS

First Author – Sumegha C. Sakhreliya,Student-ME(IT), Parul Institute of Engineering and Technology/GTU,India, sumegha137@gmail.com
Second Author – Neha H. Pandya,Professor-ME(CE),Parul Institute of Engineering and Technology/GTU,India, neh.pandya@gmail.com