ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Achieving Security and Data Privacy for VANET using X.509 Certificates

Sowmyashree H[1], Sharmila K.P[2]

4th SEM M.Tech Student, Dept. of Telecomm Engg, CMR Institute of technology, Bangalore, India[1]

Associate Professor, Dept. of Telecomm Engg, CMR Institute of technology, Bangalore, India[2]

Abstract: Vehicular ad hoc networks (VANETs) are emerging as functional technology for providing a wide range of applications to vehicles and passengers. Ensuring secure functioning is one of the prerequisites for deploying reliable VANETs. However, the open-medium nature of these networks and the high-speed mobility of a large number of vehicles harden the integration of primary security requirements such as authentication, message integrity, non-repudiation, and privacy. Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other and with roadside units (RSUs). REACT system that takes advantage of the RSUs that are connected to the Internet and that provide various types of information to VANET users. REACT faced a problem of delay, hence an enhanced version of REACT is proposed called M-REACT. In M-REACT focuses on making the proposed system more scalable in terms of the number of users that can connect to an RSU. M-REACT provides the security for data and scheduling mechanism of RSU divided into number of time slots. Public key cryptography or public key certificate is about a set of techniques that together combine in a particular system to enable secure communication. This work aims to promote the use of x.509 certificate due to its ability to reduce security risks. The results are compared to those of another system, its feasibility and efficiency.

Keywords: service oriented vehicular ad hoc network, x.509 certificate, road side unit (rsu), security, m-react, public key infrastructure.

I. INTRODUCTION

A Vehicular Ad-Hoc Network, or VANET, is a form of mobile ad-hoc networks (MANETs), to provide communications among nearby vehicles and between vehicles and nearest fixed equipment, usually described as roadside unit. Vehicular Ad Hoc Network (VANET), aiming to enable road safety, efficient driving, and infotainment. Vehicular Ad hoc Networks (VANET) is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected, each node can communicate with other nodes in single hop or multi hop, and any node could be Vehicle, Road Side Unit (RSU).

Vehicular Networks System consists of large number of nodes, these vehicles will Require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9G hz), for range can reach 1 KM, this communication is an Ad Hoc communication that means each connected node can move freely, no wires required, the routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, drivers identity, trip details, speed, rout..etc.
Prior to realizing Enjoyable value-added applications into practice in vanets, need deal with security and privacy issues. Fundamentally, it is important to guarantee identity authentication and data Integrity. In value-added applications, confidentiality is also required. In addition, the requirement of privacy preservation must be reached in terms of user-related private information, including user identity and user location.

In this paper, we study the security of data messages exchanged between users and RSUs and the location privacy of VANET users who exchange these messages. The nodes in the Vehicular Ad Hoc Network (VANET) is different from Mobile Ad Hoc Network(MANET) that in VANET the vehicles moving randomly. Here the vehicles acts as nodes, such as car, bus, truck. VANET is used for information sharing, co-operative driving, and internet access. The vehicles are communicated with each other within 100 to 300 meters VANET and it is used for safety, information sharing and internet access. Vehicle communication system is classified into two categories vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The communication between V2V and V2I are ad hoc connection.

Ad Hoc Network is a method for wireless devices for directly communicating with each other. It controls in which way nodes decides to move. V2V provides the short range of vehicular network, whereas V2I provides long range of vehicular network. The VANETs are supported by fixed infrastructure, which deploys at critical situation such as slip roads, dangerous intersection, and weather conditions.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

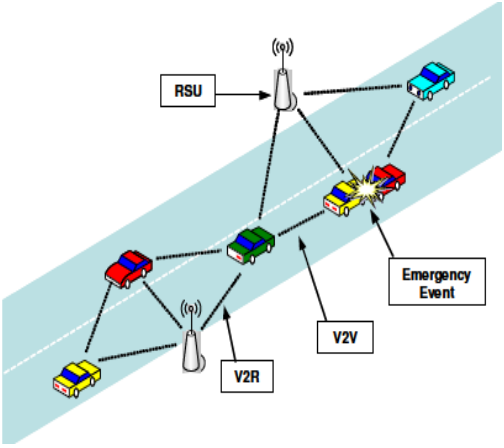

Fig1. VANET architecture.

II. REACT SYSTEM ARCHITECTURE

M-REACT focuses on making the proposed system more scalable in terms of the number of users that can connect to an RSU. M-REACT provides the security for data and scheduling mechanism of RSU divided into number of time slots. . In M-REACT, the proposed RSA algorithm that uses the PBKDF2 key derivation function in several iterations to strengthen the security of the encrypted message. The hardiness of cracking the final message is much increased at the expense of slight overhead in executing the algorithm.

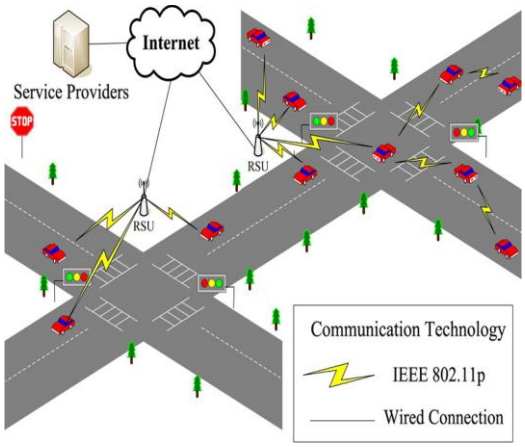

Fig2. M-REACT architecture

A. *Ensuring Location Privacy*

Many methods have proposed so far to provide the location privacy of users. They described the major disadvantages that exist in these methods, such as pseudonyms refill and unknown adversary locations. To deal with these disadvantages, we adopt the concept of ad hoc anonymity in M-REACT while modifying it by making an RSU give the user a new pseudonym each time it sends a packet to him/her. Each RSU will have its own address pool, which can be viewed as a hash function that hashes the username to an integer within a certain range.

B. *Packet-Based Keys*

Many proposed systems for VANET security disagree on the best key-management method to be used when assigning encryption keys to vehicles. Using a single key to encrypt all messages in a session allows an eavesdropper to relate the key with its source, which violates the user's privacy. Hence, shortlived keys are used to strengthen the confidentiality of data and preserve the user's privacy.

The TA and periodically renewed after all the keys have been used. In this, it is proposed that the encryption keys should frequently change (e.g., every couple of minutes), depending on the driving speed. Another approach assumes that the encryption key is changed whenever connecting to a new SP. A recent scheme assumed that the keys should be changed depending on the frequency with which the vehicle joins the network. The approach of periodic key renewal is considered unsafe, because an attacker can eaves drop the packet that contains the new keys and apply a brute-force attack to get the keys. In REACT, the concept of packet-based keys is used, where each set of keys will be used to encrypt a single packet. In addition, a packet key is not sent from the RSU to the user in a specific packet; rather, it is derived from the encrypted content of the current packet. When a user *U* starts a new session with an RSU *R*, the RSU obtains from the TA a packet key Ks and sends it to *U*, encrypted with his K*m* . *U* uses Ks to encrypt the next packet that he sends to *R*. Then, each packet will be encrypted with a new set of keys.

The body of each packet will contain a start_of_key variable of type integer that contains the index of a random byte in the packet body. A string *S* will be chosen starting from this byte. For example, if the size of *S* is 40 and if the value of start_of_key is 47, then *U* will count 47 B from the start of data and will save the next 40 characters as the new value of *S* with which the next set of packet keys will be derived. The user must check the entropy of *S* before sending the packet. If the resulting *S* has an entropy below a certain threshold (e.g., 60), *U* changes the value of start_of_key, checks the entropy of the new *S*, and so on. If *U* tries many values of start_of_key without finding a suitable *S*, he generates a suitable random value of *S* and adds it at the end of the packet.

III. PROPOSED SYSTEM MECHANISMS

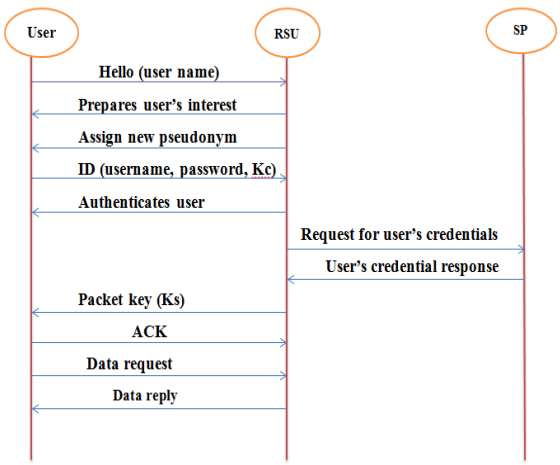

Fig3. Sequence diagram of m-react

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

The service oriented VANET is introduced to overcome all the problems in the previously proposed system and also to provide efficient security. This approach produces internet facilities to the users who are connected to Road Side unit (RSU). To provide confidentiality the cryptographic algorithm is used which provides unique private key for all users who are registered in RSU.

A. *Registration in RSU*

RSU is placed at each corner of the road. When the user of the vehicle needs to connect to RSU, first user must register to RSU. This registration is done through web. It is done only once to create an account. For registration the user must specifies the name, address, username, password and the current location. Each user selects the default RSU by sending the hello packet to the nearest RSU which sends back the needed information to the user. RSU connects to internet and provides the information such as traffic data, map, email, internet access.

B. Providing master key to the user

After the account is created for user, the RSU contacts the TA to obtain key. The user receives the master key once they connected to RSU. To provide this key the encryption function is used in the Iteration Count(IC). The secret key is provided for each user to encrypt the authenticated data from the user. Using this private key the user information is transformed very secure and confidential manner. This master key is unique for all user registered in RSU.

C. Participating in session

The user sends the hello packet to the RSU and starts the session. Each packet has a timestamp to reduce the attacks. The transformation of delay is occurred until the user sends the master key to verify whether the user is authenticated. The pseudonym is used to reduce the attacks. If the username and password matches then the RSU sends the needed information to the user.

D. Switching connection between RSU (handover):

A vehicle observes its current location and calculates the distance from all nearby rsus using digital map. If any RSU is closer than the current RSU then the vehicle switches to new RSU. This is done by sending the handover request to old RSU. The old RSU sends the handover packet to the new RSU with the username, master key, and pseudonym.

After receiving the particular request the new RSU sends back the handover confirm message to the user connected to the new RSU. This process is called handover scheme.

The protocol used for transmitting the information from user to RSU and from RSU to user is OCSP. In many systems only one key is used to encrypt all messages which may allow for eavesdropper hence to reduce this service-oriented VANET uses single key to encrypt single message. For each and every request a pseudonym is assigned to enhance the location privacy. For each user a pseudonym is created by RSU, when a request is sent from the user the reply from the RSU sent along with that pseudonym is added and sent to user. Then the user uses that duplicate ID and sends for another request. Then again RSU sends reply with the another duplicate ID. This process continues until there is a connection between RSU and user. If the user uses the old ID then RSU sends the alert message to the user, then the user reassigns the ID and back the previous request to RSU. Then the correct transformation occurs without any error or attacks.

IV.PROPOSED SECURITY SOLUTION IN VANET

PKI is a infrastructure that can be used to support digital signing and encryption for electronic transaction. The aim of PKI is to support security using X.509 certificate. In this paper X.509 v3 certificate is evaluated. X.509v3 added certificate extensions to augment X.509v1/v2 Certificates.

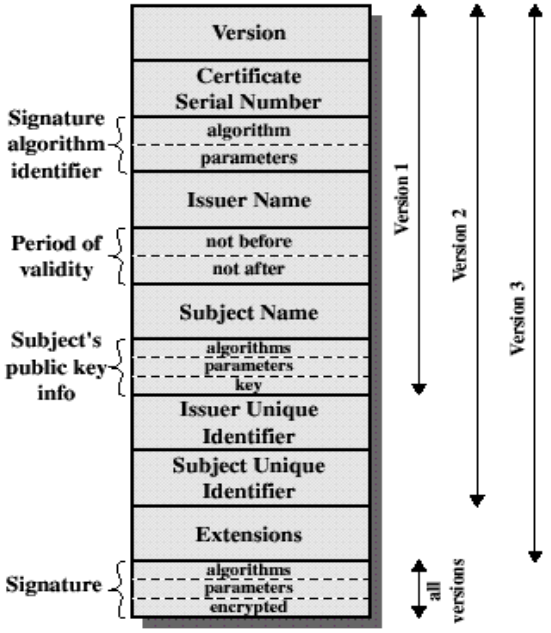

Fig4. X.509 Certificate

Version 3 introduces a mechanism whereby certificates can be "extended," in a standardized and generic fashion, to include additional information. There are numerous reasons why this additional information is required, and some of these reasons will be discussed as the standard extensions are presented. The term standard extensions refers to the fact that the version 3 X.509 standard defines some broadly-applicable extensions to the version 2 certificate. However, certificates are not constrained to only the standard extensions and anyone can register an extension with the appropriate authorities (e.g., ISO). Over time, it is expected that new broadly-applicable extensions will be added to the set of standard extensions. It is

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

important to recognize, however, that the extension mechanism itself is completely generic. Each extension consists of three fields: **type, criticality, and value**.

The **extension type** field defines the type of the data in the **extension value** field. The type could, for example, represent a simple text string, a numerical value, a date, a graphic, or a complex data structure. To promote interoperability, all extension types should be registered with an internationally-recognized standards organization. The **extension criticality** field is a single-bit flag. When an extension is flagged as critical, it indicates that the associated **extension value** contains information of such importance that an application cannot ignore the information. If a particular certificate-using application cannot process a critical extension, the application should reject the certificate.

A. *Attribute-Based Privacy*

The AA will perform the basic or extended path validation process to verify that credentials have not been revoked. The provided certificate could also consist of a short-term certificate based on an underlying pseudonym solution. On successful validation, the AA will then issue to the vehicle the corresponding ABCs. ABCs will include encoded certificate's information, such as, the expiration date, the CertID, revocation information, etc. Additional information needed to generate presentation tokens will also be included.

1) Presentation Tokens

Tokens are data artifacts that contain the required information, and the support cryptographic evidence, which are exchanged between the vehicles and the service providers. A token is generated from the vehicle's /driver's P-ABCs, and in ABP are assumed to be pseudonym-based and therefore unlinkable (a SP cannot tell if two different tokens were derived from the same credentials), unless the token has been intentionally generated to reveal linkable information (e.g. in case of liability) the AA could trace back the underlying credentials. In general, a token will be generated specifically to meet the corresponding SP's conditions in order to grant service access. As a result, when a token has been generated, it will be attached to the vehicle's request. On reception, the SP will perform two different actions, i) the token-certificate related validation through the AS, and, if positive, ii) the ABC validation of the token.

2) Credentials Revocation:

In ABP, the revocation of credentials will be done by the AS, providing near-real time certificate validation via the multi-CA OCSP component. In addition, since certificates issued by the AS are short-term, the related P-ABCs will be regularly updated, in particular the non-revocation evidence attribute.

3) Providing Minimal Information Disclosure

This section presents the communication of the ABP, and how the minimal information disclosure could be achieved in an inter-regional scenario, next credential issuance will be described.

B. Privacy Attribute-Based Credentials (P-ABCs)

P-ABCs, are basically a PKI with privacy enhancing features. P-ABCs are issued just like ordinary cryptographic credentials (e.g. X.509 credentials) using a digital (secret) signature key .However, the main enhancing feature in P-ABCs, is that, credential's attributes could be transformed into `unlinkable' presentation tokens able to protect the holder's privacy, and verifiable in a similar form, just like cryptographic credentials.

C. Attribute-Based Privacy (ABP) Protocol

In VANETs the implementation of a VPKI with hierachical certification authorities is envisioned. An AS able to provide PKI-based authentication among untrusted domains. However, although the proposed approach copes with interesting challenges, privacy issues remain unsolved. Thus additional mechanisms to support conditional privacy must be considered as an integration of the underlying solution. This section describes the proposed PKI compliant ABP protocol, which inspired by P-ABCs implements conditional privacy, specifically to address vehicle's tracking

D. Entity's Definition

In compliance with the VPKI and P-ABCs, the ABP defines three different types of entities the will be introduced next. Attribute Authority (AA) the AA is the authority responsible for issuing and revoking the corresponding attribute credentials. In VANET scenarios the AA could be represented by the regional CA or by any trusted authority in charge of issuing, revoking, and when applicable revealing the attribute based credentials. The ABCs are different than the short-term credentials issued by the AS Vehicle/Driver in ABP, entities to which the AA will issue the ABCs, will be mainly represented by vehicles and drivers. This entities will be responsible for managing and selecting from which credentials, which attributes will be disclosed and to which entities, and ultimately will be responsible for generating a presenting the corresponding presentation tokens. Service Provider (SP) The SP consists of any relying party willing to protect access to resources, information or services, in common VANET scenarios the SP could be represented by RSUs, vehicles, authorities, or services provided by the infrastructure

V. PERFORMANCE ANALYSIS

We simulated the proposed solution for providing service availability, attack against data privacy and data integrity. We measured the performance in terms of packet success ratio, packet drop ratio, initialization delay,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

message delay, overhead traffic. From the performance chart that our proposed mechanism is able to reduce the number of security attacks and secure transmission of user data.

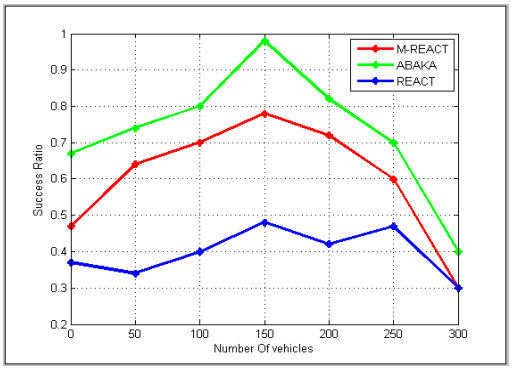

Fig5. MSR wrt number of vehicles

The message success ratio is compared with ABAKA and REACT, the existing system with the proposed system M-REACT. M-REACT is enhanced version of REACT. Success ratio is improved when compared with existing system.

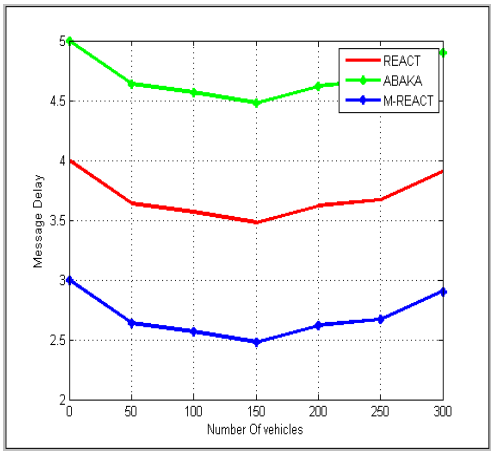

Fig6. MRT wrt number of vehicles

Delay is reduced in the proposed system, that is in M-REACT system when compared to existing systems.

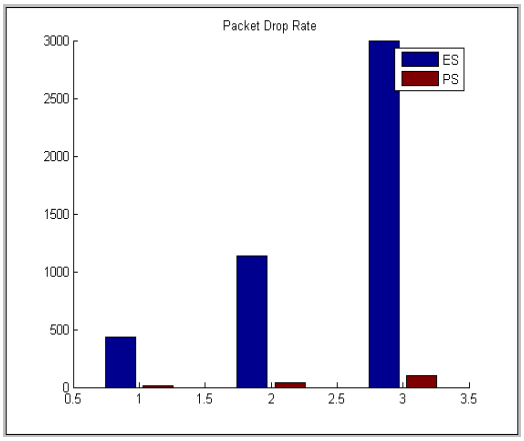

Fig7. Packet Drop Ratio

Packet drop ratio is completely reduced when compared to existing system. Hence there it is possible to transmit data securely using the proposed system.

VI. CONCLUSION

This paper has analysed general security and privacy issues that are present in VANETs. First, the importance of interoperability for VANET's authentication, along with all the challenges it conveys has been introduced. In order to create secure and dynamic interoperability relationships among untrusted CAs, a security model that makes use an Authentication System (AS) has been proposed. Secondly, the privacy issues that remained open despite the AS implementation, were extensively discussed. As it has been explained, to be able to provide conditional privacy/anonymity and prevent attacks related to the big brother scenario, additional mechanisms are needed. To provide conditional anonymity and minimal information disclosure, the Attributed-Based Privacy (ABP) protocol has been proposed. The proposed architecture is demonstrated to achieve desired security objectives and efficiency.

ACKNOWLEDGMENT

The euphoria and satisfaction of the completion of the Dissertation will be incomplete without thanking the personalities responsible for this venture, which otherwise would not have become a reality. I offer my sincere thanks to CMR Institute of Technology, Bangalore, for providing all kinds of facilities to carry out my project. I take great pleasure in expressing my sincere thanks to **Dr. Sanjay Chitnis,** Principal CMRIT for his valuable support. I would also like to express my deep sense of gratitude to **Mrs.Sharmila .K.P** Head of the Department of Telecommunication, CMRIT for providing good facilities, constant encouragement and valuable guidance. With deep sense of gratitude I acknowledge the help and encouragement of my project guide, **Mrs. Sharmila .K.P** Assoc. Professor and HOD, Dept. of TCE, CMR Institute of Technology, for her successful guidance, support, help and suggestions.

REFERENCES

[1] Khaleel Mershad and Hassan Artail, "*A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks* ", ieee trans on vehicular technology, vol. 62, no. 2, feb 2013, pp 536-551.
[2] Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3," *Security Analysis of Vehicular Ad Hoc Networks*", 2010 Second International Confe. on Network Applications, Protocols and Services.
[3] MohamedNidhalMejri a,∗, Jalel Ben-Othman a, MohamedHamdi, "*Survey on VANET security challenges and possible cryptographic solutions*", Vehicular Communications 1 (2014), pp 53–66.
[4] G.Archana ,S. Andal, *"A Framework for Data Security, Identification and Authentication in VANET"*, ICIET'14.
[5] S.Nidhyalakshmi, Mrs.R.Sabarimala, "*An Efficient Data Acquisition and Delivery in Service Oriented Vehicular Adhoc Networks"*, An ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

[6] Prof. Vaishali D. Khairnar and Dr. S. N. Pradhan, *"Comparative Study of Simulation for Vehicular Ad-hoc Network",* International Journal of Computer Applications (0975 – 8887) Volume 4– No.10, August 2010.
[7] Ian Curry, *"Version 3 X.509 Certificates",* July 1996.
[8] S.Bhuvaneshwari1, G.Divya2, K.B.Kirithika3, S.Nithya4, *" A Novel Approach for Secured Data Transmission in VANET through Clustering",* IOSR-JECE Volume 9, Issue 2, Ver. III (Mar - Apr. 2014), PP 23-30.
[9] Shanmuga Priya.S and Erana Veerappa Dinesh.S, "*A Novel Approach for Data Acquisition and Handover Scheme in VANET",* (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, pp-1443-1446.
[10] Ankita Agrawal1, Aditi Garg2, Niharika Chaudhiri3, Shivanshu Gupta4, Devesh Pandey5, Tumpa Roy6, " Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper", ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013.