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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

A Holistic Protocol for Secure Data Transmission in VANET

TamilSelvan[1], Komathy Subramanian[2], Rajeswari Rajendiran[3]

Department of Information Technology, Christ College of Engineering and Technology, Pondicherry, India [1]
Department of Information Technology, Christ College of Engineering and Technology, Pondicherry, India [2]
Department of Information Technology, Christ College of Engineering and Technology, Pondicherry, India [3]

Abstract: VANET is the emerging area of MANETs in which vehicles act as the mobile nodes within the network. VANETs are deployed in untrusted and unsecured environment. Value-added applications such as geographical location determination, online payment services, etc. in VANET, improve safety of driving, comfort to passenger, offer great business opportunities, and attract more attention in our life. Vehicles which can be enabled to communicate with their nearer vehicles and sharing the states of driving, VANETs avoid accidents potentially caused by lane changing, emergency braking, etc. The characteristics of VANET lay both challenges and opportunities in achieving the goals of security. Providing security to VANET is necessary by means of giving user anonymity, authentication, integrity, and privacy of information. The Various vulnerable attacks in VANETs are as DDOS attack, ID disclosure, Wormhole attack, sinkhole attack, misbehaving and faulty nodes, spoofing, traffic analysis attack, Sybil attack. The existing solution in this paper is, the security should be provided only to the unauthorized users alone but not to the authorized users. In this case the time consumption and the overhead will be more. In this paper we propose a new light weight holistic protocol to secure VANET against insider and outsider attacks.

Keywords: Security, Road Side Unit(RSU), Registration Identity, Certificate, Plausibility checks.

I. INTRODUCTION

VANET stands for Vehicular Adhoc network. It is a form of Mobile Adhoc Networks (MANETs) and it renders communication among between the vehicles, nearby vehicles, and nearby fixed equipments called Road Side Units (RSUs). Fig. 1 shows the VANET architecture. Every node i.e., a RSU or vehicle in the network communicates with other nodes in multiple hop or single hop. VANETs are designed with the goals of providing passenger comfort and enhancing driving safety. In VANETs, the types of communication are available as follows:

- Vehicle-to-Roadside Communication
- Vehicle-to-Vehicle Communication
- Inter Roadside Communication.

The radio used for the communication is DSRC. DSRC stands for Dedicated Short-Range Communications. DSRC/WAVE systems take out the disadvantages in wireless infrastructure by helping low latency, geographically local and high mobility communications [1]. DSRC/WAVE supports vehicle-to-vehicle and vehicle-to-infrastructure communications for Intelligent Transportation Systems (ITS) which is a part of Federal Highway Authority's Vehicle Infrastructure Integration initiative. Different DSRC standards have been in use in US, Europe, Korea and Japan, mainly for applications like electronic toll collection (ETC) and automatic vehicle identification. These standards were not designed to support V2V or safety communication in VANETs. Currently we have at least three different organisations developing standards for safety communication in 5.9 GHz ITS band, each tailored to their specific focus, supporting 802.11p: North American IEEE 802.11p + IEEE P1609 (WAVE), European C2C-CC Communication System (ETSI TC ITS) standardised by European TelecommunicationsStandards Institute (ETSI) , and Global ISO TC204 WG16 (CALM).

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

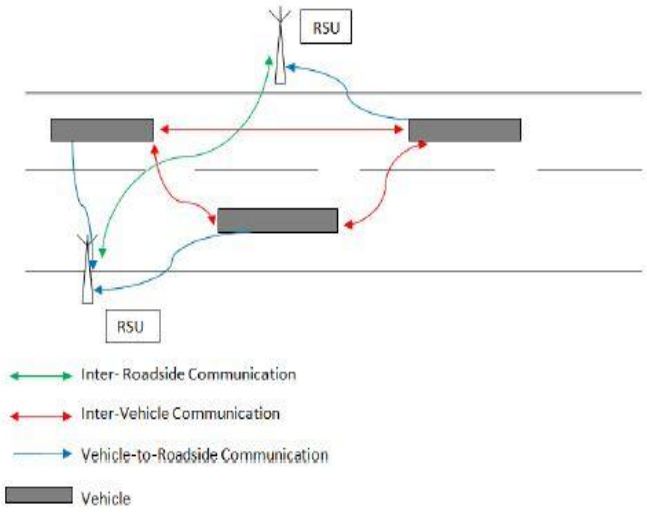

Fig1. VANET architecture

IEEE 802.11p [1] is a standard to add WAVE. WAVE stands for Wireless Access in Vehicular Environments and it should define enhancements to 802.11 and supports Intelligent Transportation Systems (ITS) applications. They include information exchange between low-speed vehicles and the high-speed vehicles in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz).

The characteristics of VANET are as follows:

- Large scale connection range and large number of nodes
- High mobility with the constraint of road topology
- Accurate positioning access (GPS)
- No power issues
- Potentially unbounded network size
- Deployment in direction of roadway
- Time-sensitive data transfer

The security of VANETs is a main critical issue because the data transmission is in wireless environment. It makes short-range radios installed in Road Side Units (RSUs), central authorities and vehicles those are responsible for management and registration of their identity. Vehicular Adhoc Network projects have been used by various governments, academic institutions, and industries around the world. But VANETs are vulnerable to intruders ranges from inactive eavesdropping attack to active tampering, spamming, and interfering.

In this paper, we study the attacks in VANET and propose a holistic protocol for secure data transmission and detecting misbehaviours sent by the authorized users. In our proposed work, the vehicle which should register with near by Road Side Unit(RSU) and then RSU authenticate the vehicle by means of using the certificate provided by the RSU. If the authentication is successful then only the data was provided. Otherwise the data/node will be blocked. If authorized user itself sent false event means that should be detected through the plausibility checks. The motivation behind this paper is that to provide a secure and lightweight protocol for data transmission against insider and outsider attacks.

The rest of this paper is organized as follows. We introduce the security goals in section II. In section III, we define the previous work and in Section IV, presents attacks in VANET. Section V, we define existing detection mechanisms for attacks in VANET.Section VI introduces the proposed work i.e. a new lightweight holistic protocol for secure data transmission in VANET. In section VII, we define the environmental setup and in section VIII, we presents the implementation and the result. Finally we conclude our paper in Section IX.

II. SECURITY GOALS

The goals to assure or secure VANETs are same as that for secure any network. The main aim is to provide authentication, integrity, availability, confidentiality, and non-repudiation.

- Authentication is assurance that their communicating entity is the one that it claims to be and enables a node to ensure the identity of their communicating node. It is mainly for checking whether the vehicle is authorized or not. It is necessary that the node receiving data is sure that the data is sent from a valid sender.
- Confidentiality deals with the protection of data from unauthorized disclosure. Confidentiality of data ensures that the data is not leaked or disclosed to unauthorized nodes or vehicle in the network. For eg. The data being transmitted by the vehicles should be received by the registered vehicles only. Disclosure of this data may lead to identification of vital information.
- Integrity is particularly important for critical safety. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

- Availability assures that the system works properly and their service is provided to authorised users alone whenever it is required. An adversary may deny services to valid nodes by jam their channel, by disrupting their routing protocols, by draining battery of power, etc. For eg. The services provided by the RSU should be available to the vehicles whenever it is necessary.
- Non-repudiation provides protection against denial by any one of the entities and they are involved in a communication of being participated in all or part of the communication. For eg. After sending a message, the vehicle should not deny having those sent message is called as sender non-repudiation. Also after receiving a message, the vehicle should not deny having those received message is called as receiver non-repudiation.

III. PREVIOUS WORK

Several researchers studied security challenges related to VANETs. In this section, we conduct a brief study of recent and relevant works.

Raya and Hubaux [2] describe security vulnerabilities and challenges in vehicular networks. A detailed threat analysis, a basic attacker model, and appropriate security architecture are provided.

Dan Greene, Jessica Staddon, Philippe Golle[3], gives an idea of Sensor driver technique or method that lets nodes to determine incorrect data and also identify the incorrect data's source i.e where the incorrect data originated with high probability.

Zhu, Richard and Tang[5], proposed prevention based technique which make use of an authentication protocol referred as ALPHA protocol (adaptive and lightweight protocol) which is based on hash chains and Merkle trees (MT), i.e., a tree of hashes. The main disadvantage is the loss of single packet may lead to multiple packet loss.

Bo Yu, Cheng-Zhong[6], we study the feasibility of using signal strength distribution analysis to detect Sybil attacks. First, we propose a cooperative method to verify the positions of potential Sybil nodes. In cooperative detection method, from the source the selection of node will be done and it act as claimer then it claims and identifies its position. The main drawback in this method is that not to ensure that all signal strength measurements originate from honest physical nodes instead of Sybil nodes. In our next proposed system Presence Evidence System(PES)[6], it remove the Sybil witness candidates and to improve the detection efficiency by means of observation period for collecting the signal strength measurements. In statistical detection method, the observation time will be extended then it easily detect the Sybil nodes and this is only for Sybil and not for other type of attacks.

Karan and Ashok kumar[7], gives an efficient IPCHOCKREFERENCE method to detect and defend against UDP flooding attacks under different IP spoofing types. In this it requires low computational costs and resources but it is suitable for only Dos attacks.

IV. ATTACKS IN VANET

In order to design the security solution for VANETs [8,9], we should learn different types of security threats, the types of attackers and attacks.

A. Classification of Attackers

Attackers could be classified according to nature, behavior, and scope of the attacks [10,11]. Some types of attackers are discussed as follows:

- Some attackers eavesdrop only on wireless channel to collect traffic data like jamming and lane changing etc which may be passed onto other attackers in the network. As these attackers do not involve in the communication process of network, they are called passive attackers i.e inactive attackers. At the same time, some of the attackers either generate or give packets containing wrong data or do not transfer the received packets and those are called as active attackers.
- An authentic or authorized member of a Vehicular Adhoc Network having authentic public keys is also an attacker. They also have access to other members in the network and those attackers are called as insider attackers(insider). Outside attackers (outsider) can set up attacks of less diversity and they are as intruders. The outside attackers are unauthorized users which attack the information in the network.
- Local attacker establishes an attack with a limited nature, scope and behavior, that is, an attack is baned to a particular area. An attacker can control the several entities or area distributed across the network where an attack can be extended.

B. Types of Attacks

Owing to large number of independent network members and the presence of misbehavior of nodes, human factor in future vehicular adhoc networks and can't be ruled out. There are many different types of attacks [20] have been classified and identified based on the layers. An attacker can rebroadcast an old message and introduce the false messages

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

also. At network layer, an attacker can include or insert the false routing messages or overload the system with routing data. At the link and physical layer, an attacker can trouble the network by overloading the channel of communication or media with useless messages. Privacy of drivers can be exposed by revealing and covering the position of the drivers and these attacks are briefly explained subsequently.

1) Bogus Information
In this type of attack, the attacker can be outsider/intruder or insider/legitimate user. The attacker broadcast false information in the vehicular network to affect the decisions of other vehicles by spreading the false information in the network.

2) Sybil Attack
Sybil attack[15] is a kind of impersonation and in this network where multiple identities of the attacker node are present. With several entities in the network it would be able to decrease the effectiveness of fault-tolerant techniques. Fig. 2 shows the Sybil nodes assuming multiple personalities of the attacker node.

- In Sybil attack, a malicious node makes up different identities in the form of multiple nodes in the network.
- These fabrications mislead nearer vehicles by communicating with other physical nodes and distributing false traffic data (e.g., traffic jam or accidents).

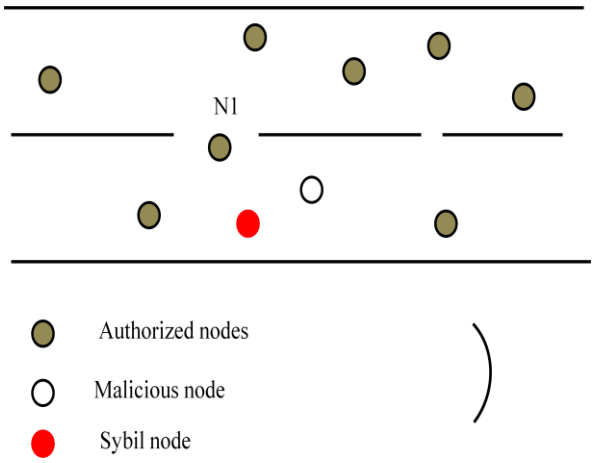

Fig2. Sybil attack

3) Misbehaving and Faulty Nodes
Vehicular network (VN) nodes (road-side infrastructure units and vehicles) that take part in network operations has a certificate or digital signature provided by a Certification Authority (CA). But the ownership of a certificate does not ensure correct data from the node: a node may inject false information (e.g. alerts, warnings, coordinates) while at the time of binding with the implemented protocols [12]. Also, a node which is revoked for administrative reasons (e.g. the vehicle owner did not renew its registration), it becomes difficult for the authority to obtain and validate sufficient evidence that a node is faulty or compromised. Therefore messages from this node will not be valid after the certificate revocation.

4) ID Disclosure
An attacker is insider, passive, or malicious. It can monitor trajectories of target vehicle and can use this data to determine the ID of a vehicle.

5*) Sinkhole Attack*
In sinkhole attacks, all the traffic from a particular area goes through attacker node. Therefore, the attacker will have control over the traffic, enabling the occurrence of many other attacks, such as selective forwarding [15]. Fig. 3 shows the malicious node transferring the data to the sink node.

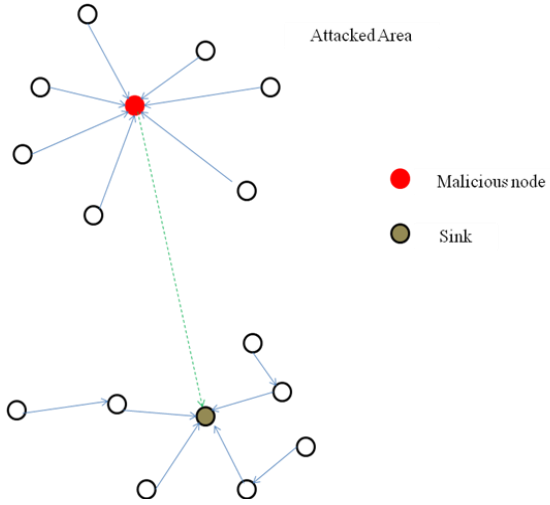

Fig3. Sinkhole attack

6) Denial of Service (DOS)
Attackers may be malicious, active, or local in this case. Network which should be bring down by sending unnecessary messages by the attacker on the channel. Example of DOS attack includes injection of dummy messages and channel jamming.

7) Replaying and Dropping Packets
An attacker may neglect legitimate or legalize packets. For example, an attacker can neglect or drop all alert messages by meant for warning vehicles proceeding towards the location of accident. Similarly,an attacker can replay the

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

packets after that event has been occurred to create the delusion of accident.

8) Selective Forwarding
In selective forwarding always some specific packets are dropped. As discharging all packets can be easily identified by nearer nodes , the attacker performs a selection on the packets. Thus attacker transfers the messages, being able to degrade service anyways [12].

9) Worm Hole Attack
It is a challenging task to detect and prevent wormhole attack. A malicious node record packets at one location in the network and tunnel them to other location through a private network shared with malicious nodes. Severity of this type of attack increases if the malicious node sends only control messages through the tunnel and not the data packets.

V. EXISTING DETECTION MECHANISMS FOR ATTACKS IN VANET

In our existing work[13], in the first time the user or the vehicle which should register with the near by Road Side Unit(RSU) by means of giving username and password. The user send the hello packet(username) to the RSU then the RSU prepares the users' interest like web pages, certain news, traffic information in certain areas etc. RSU assign new pseudonym to the user and also it contact the Trusted Authority(TA) and provide the key called as master key(K_m). Those should be given in the form of ID packet to the user. The ID packet consists of username and pseudonym. Then the user send the identity packet which consist of username, password and secret key(K_c) to the RSU. Both the packets will be encrypted by using K_m.

RSU authenticates the User and it should fetch the user credentials from the database by using K_c. RSU again contact the TA and provide the new key called session key(K_s). Then the RSU sent the packet key packet which have K_s. At last the acknowledgment is sent from the user to the RSU and also request for data is also sent then the reply is to be get back from the RSU to the Vehicle.

In general, the vehicle should register with the near by road side unit in the first time of entering the range then if the vehicle want to get the data from the RSU at the time authentication will be performed. If the authentication is successful then the data has to be provided otherwise the the data or node is blocked. The main problems in our existing detection mechanism are

- It uses heavy weight protocol.
- The time consumption will be more.
- If more users will connect to a single RSU at the time the overhead will be more.
- It should not provide the security to insider attacks.

VI. PROPOSED WORK

In our proposed work, the vehicle which should register with nearby Road Side Unit(RSU) and in Registration phase, the user which should register the Road Side Unit(RSU) by means of giving the username and password then the RSU provide Registration id to the the user which consist of licence number and the vehicle registration number. Then RSU authenticate the vehicle by means of using the certificate provided by the RSU. If the authentication is successful then only the data was provided. Otherwise the data/node will be blocked. This type of protocol is holistic protocol and this protocol was concerned with the whole rather than with the individual parts. If authorized user itself sent false event means that should be detected through the plausibility checks.

A. Base station to Road Side Unit communication

In Base station to Road side units communication, firstly the Road Side Unit(RSU) get a message from the Base Station in which a variable R and a group identity (Idg1). The Road Side Unit responses to the base station whether it is passive or active. Then Base Station get response from the Road Side Unit(RSU) then sends the certificate to RSU.

The certificate which contains three variables and they are as following - public key of road side unit (PU_{RSU}), a variable R and group identity (Idg1). The channel is encrypted only by means of R and after receiving that certificate it should be decrypted by using the same variable R. Thus R is responsible for only the authentication purpose and the communication is shown in Fig 4.

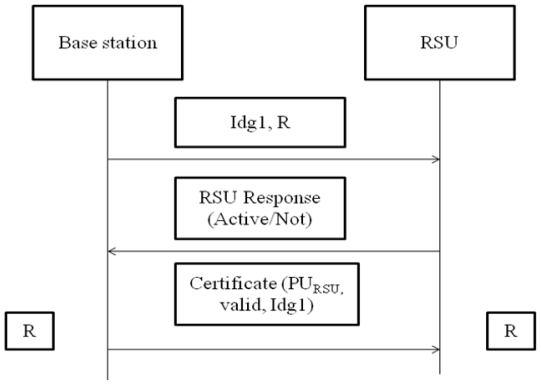

Fig4. Base station to RSU

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

B. Road Side Unit to vehicle communication

In Road Side Unit to car communication, a car or vehicle which is already has a registration identity. The Regid includes car registration number, license number. Firstly road side unit(RSU) which gets a message from car in which it consists of registration identity (Regid) and public key of the car (PU_{car}). Car which gets a response from Road Side Unit by means of sending a message which includes registration identity (Regid) and certificate of RSU ($CERT_{RSU}$). Then the Car will store the $CERT_{RSU}$ and then sends a message to the RSU which includes $CERT_{RSU}$ and Regid . Registration id is mainly used for checking the authentication of car and RSU. Thus mutual authentication is done and then the communication is preceded and the communication is shown in Fig 5.

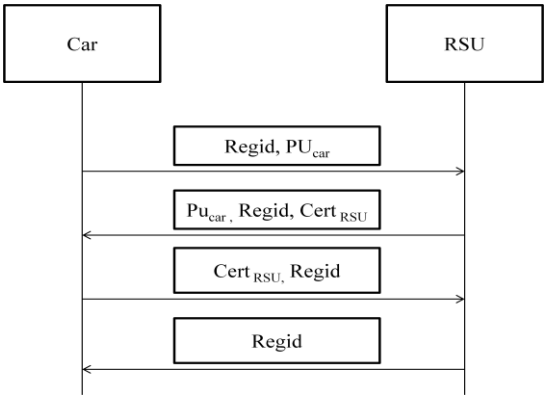

Fig5. RSU to Car

C. Vehicle to vehicle communication

The certificates will be sent inbetween the car to each other in vehicle to vehicle communication. If the certificate is same for those vehicles and authenticated then the communication will proceed on and the communication is shown in Fig 6.

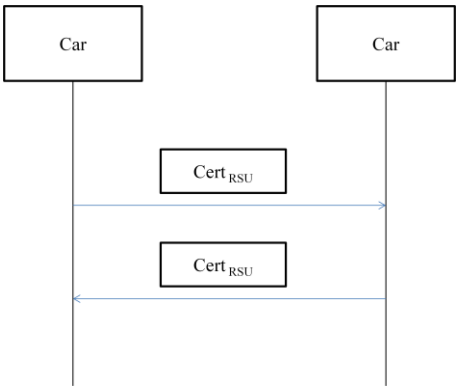

Fig6. Car to Car

In all the above communication the insider attacks can be avoided by plausibility checks. i.e if the authorized user itself sent the false information then that should be detected throught plausibility checks[14]. Every vehicle has to check the reliability of their received messages. Apart from assuring the used cryptographic values (if any), it has to determine if the contained data could be true. For this purpose, plausibility checks have been proposed. In such mechanism, vehicles examine every message. The message or data forwarded to the RSU. If other vehicles also forward the same data, the RSU will use Message Linkable Group Signature scheme[14]. In this the Group Manager will group the messages and check its trust value. If its trust value will be more then we can easily understand that it is not a false information and the data will be transmitted. Otherwise we can identify that it is a false information then data will not be transmitted and the node or data will be blocked.

The main advantages in holistic protocol for secure data transmission in VANET are

- It uses lightweight protocol.
- The time consumption will be less.
- It should provide the security to both outsider as well as insider attacks.

VII. ENVIRONMENTAL SETUP

The environment for implementation of our proposed work as OMNeT++. The OMNeT++ simulation IDE is based on Eclipse platform and extends it with new editors, views, wizards, and other functionality. OMNeT++[15] is an modular, extensible, component-based C++ simulation framework and library primarily for building simulators to the network.

OMNeT++[16] is a simulation framework rather than itself in a simulator. Instead of having hardwired and explicit support for networks or other areas, they gives the infrastructure for writing such simulations.OMNeT++ is free to use in educational and academic institutions. Corporate use requires, however, a paid license of OMNEST. So OMNeT++ is neither open source nor free software.

VIII. IMPLEMENTATION AND RESULT

In this paper we implement our proposed work by using the tool as OMNeT++. In our proposed work the vehicles and the RSU are communicated then the information is transferred between them through the authorized nodes alone by means of the authentication. In this the misbehavior data should also be detected. The nodes which are shown as the vehicles and data are transferred successfully by removing the malicious node as well as the malicious data. The result

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, December 2013

of this is, the data which can be forwarded successfully and the malicious data are identified.

IX. CONCLUSION

Safety and security is getting a necessary for VANET applications. As Vehicular Adhoc Networks, they use wireless technology and it is dangerous to many attacks. We studied, the security goals compromised by the attacks, the attacks in VANETs, and their prevention/detection mechanism have been discussed. In this paper, we proposed lightweight holistic protocol for secure data transmission against insider and outsider attacks. In this the data which transmitted securely and the misbehaviours also detected successfully. When a malicious or unauthorized node is detected on the network then the data passed to the other authorized node by isolation of that malicious node. Even under strong attacks holistic protocol demonstrates steady improvement in network performance. In future we would like to implement our research work in the tool OMNet++.

REFERENCES

[1] IEEE Standard for Information Technology – Telecommunication and Information exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements, IEEE Std 802.11p – 2010
[2] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. SASN*, Alexandria, , Nov. 2005.
[3] P. Golle, D. Greene, and J. Staddon, ― Detecting and correcting malicious data in vanets, in VANET '04: Proceedings of the 1st ACM international workshop on Vehicular Ad hoc networks, pp. 29–37, ACM, 2004.
[4] M. Raya, and J.P Habaux ,"Securing Vehicular ad hoc networks".
[5] Li Zhu, F Richard Yu, Bin Ning ,"A joint design of security and quality-of-service (QoS) provisioning in vehicular ad hoc networks with cooperative communications and Tao Tang ",2013
[6] Bo Yua, Cheng-Zhong Xu, Bin Xiao," Detecting Sybil attacks in VANETs", February 2013
[7] Karan Verma, Halabi Hasbullah and Ashok Kumar,"An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET",2013.
[8] T. Leinmuller, E. Schoch, and C. Maihofer, (2007)"Security requirements and solutions concepts in vehicular ad hoc networks". In Proceeding of Fourth Annual Conference onWireless on Demand Network Systems and Services.
[9] P. Papadimitratos, V. Gligor, and J.-P. Hubaux,(2006) "Securing vehicular communications— assumptions, requirements, and principles". In Proceedings of the Workshop on Embedded Security on Cars (ESCAR).
[10] M. Raya and J.-P. Hubaux,(2007)" Securing vehicular ad hoc networks". Journal of Computer Security, 15(1), 39–68.
[11] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, andT. Leinmuller,(2006) "Attacks on inter-vehicle communication systems—an analysis". In Proceedings of the 3rd international Workshop on Intelligent Transportation (WIT).
[12] J.T. Isaac, S. Zeadally, J.S. CaMara, ―Security Attacks And Solutions For Vehicular Ad Hoc Networks, IET Communication‖., 2010, Vol. 4, Iss. 7, Pp. 894– 903.
[13] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", February 2013
[14] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", 2010
[15] en.wikipedia.org/wiki/OMNeT
[17] www.omnetpp.org
[18] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient detection of sybil attack based on cryptography in VANET"
[19] Senthil Ganesh N, Ranjani S, "Security Threats on Vehicular Ad Hoc Networks (VANET): A Review Paper"