ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

"Various Types of Vehicular Attacks and Its Preventation Techniques in VANET"

[1]Aditi Selokar, [2] Prof. Vaishali Sahare,
[1] Student, Computer Science and Engineering, G.H R.I.E.T. for Women, Nagpur, Maharashtra, India.
[2]Assistant Professor, Computer Science and Engineering, G.H R.I.E.T. for Women, Nagpur
[1]aditi.selokar@gmail.com[2] vaishali.sahare@raisoni.net

Abstract- **In this century,there is continuously increasing the automobile industry market and their safety related applications.This safety applications could be provided to the driver and passenger for getting comfort and secure feeling. But as per the nature rules, each coins has two sides one is tail and other is head.In such a way that all the application run in the nature has two sides,one is its advantage and other is disadvantage.In such way that VANET have the two side, first one is VANETs applications and second side is VANET attacks.In first side VANET can provide the security by broadcasting the messages to the vehicles by sending the various types of warning messages like collision warning, lane change warning, work zone warning, inter-vehicle communications, etc. It means that VANET provide the all types of safety related application to secure the human lives and provide to comfort feeling to driver and passenger. But in other side the VANET application would be interrupted by the attacker and this is the main disadvantage of the VANET. In VANET, there are various types of attack and attacker can attack on the VANET application such as interrupt the message, changing the order of the messages, retransmission's of message again and again, jamming the network, false information transmission, etc. In this paper we can discuss the various types of attacks and its prevention techniques.**

Index Terms: **VANETs, Vehicular attacks, prevention technique, VANET security**

I. INTRODUCTION

Vehicular adhoc network is the advance research in the mobile adhoc network in which each and every node can communicate with each other freely in specified coverage area and remain connected properly with each other. VANET have the special case in the mobile adhoc network,which have fix and infrastructure less network.All the node can be communicated in a single hope or multi hop structure. The main difference between the vehicular adhoc network and mobile adhoc network is the high speed mobile vehicles, higher processors speed, large storage capacity and higher autonomous battery power. VANET can turn every release car into a wireless router or node and allowing cars to communicate in approximately up to the range 100 to 300 meters and at the time of turning create a the network with a wide range.

The in- vehicular network consists of on board unit and one or more application units. The connectivity between the OBU and APs were wired and sometimes wireless. Application unit is in vehicle entity and multiple AUs can be integrated with single OBU .In adhoc network vehicles were equipped with the OBUs and RSUs. OBUs can be seen as a mobile node and RSUs can be seen as static node.

Vehicular Adhoc Network is the one of the form of network which have two nodes.1) On Bord Units(OBU) have the moving vehicles which can move freely.2) Road Side Unit(RSU) is the fix node to which vehicles can communicate properly. Road side unit was permantly fixed alongs roads and highways or parking place, bus station.shopping malls etc.The main aim of RSUs unit s to maintain the internet connectivity to the OBUs. Road side unit is part of the base station and perform the functions like to provide authentication to the vehicle or check the vehicular authenticity,to maintain communication link between the two vehicles, packet filtering, calculate which type attack going on and minimize this attack. etc. RSUs could be connected to the internet via gateways.The function of On board unit to provide communication between the vehicle to vehicle,vehicle to infrastructure and roadside unit. OBU provide communication service to the application unit and forward data on behalf of OBU. Both RSU and OBU based on the IEEE 802.11p standard.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

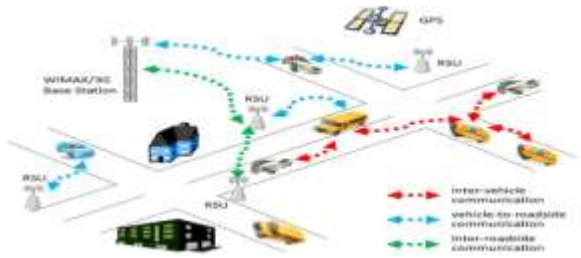

Fig1:VANET communication [1]

Fig 1 shows the structure of vehicular communication in VANET.In VANET,there are three types of communications such as 1) vehicle to vehicle communication.This communication could be also called as intervehicle communication.This communication is shown in the figure by red bidirectational arrows.2)vehicle to roadside communication.This communication is shown in diagram by blue bidirectational arrows.3)Intra roadside communication.This communication is shown in figure by green bidirectational arrow.In such a way vehicles and infrastructure can communicate with each other by bradcasting messages and this message can broadcast securely.VANET security satisfy the four goals such as, they should maintain the messsage and vehicles identity.It mean that to maintain authentication of the message and source, to maintain message integrit, to maintain privacy and also maintain non repudiation.

In vehicle to vehicle communication, vehicle can communicate directly or indirectly by using the RSU place along the roadside or by using infrastructure.When these vehicles can communicate with each other then that time they are exchanging their valuable information with each other such as network traffic information,warning messages,whether condition,safety alarm message, etc. VANETs have aim to broadcast information securely. But some of the attacker could attack on that valuable information and make changes in the message and make use of the message for self purpose.So our aim was to provided security to this broadcasting message..

In our paper section 2 describe the vehicular attacks. Section 3 describe the prevention techniques from the various types of attacks.and then at section 4 we can conclude the paper. In last section we can see the references .

II. VEHICULAR ATTACKS ON VANET

In VANET, when the vehicals are moving then they are broadcasting the secure messages.When messages are broadcast then some attacker attack on the messages and destroyed that message or change the format of the messages. So we have to see the various types of attacks goning on VANET.

2.1 Sybil Attack

The Sybil attack is very famous and harmful type of attack.It was discovered by Douceur in the context of peer-to-peer networks. This attack can perform, when the two vehicles can transmitting the messages at same time or it is in processing. Sybil attack is very dangerous when the vehicles are in different position at the same time then there is a very high security risk in the network. The Sybil attack can damage the network topology, connection and bandwidth also.

Fig.2.1. Sybil attack [5]

In figure 2.1 shows that the Sybil attack .In this attack, attacker A transmits the multiple messages having different identity to the other vehicles. For that other vehicles assume that there was new heavy traffic on that road. To secure from the Sybil attack, there are three defenses techniques 1) Introduction. It is also called as re registration 2) position verification 3) radio resource testing. In registration secure technique, it is not itself enough to prevent from Sybil attack because there are various types of malicious nodes in the network and they have possibility to register in the network with multiple identities by non-technical ways such as stealing etc. If strict registration can be done then there is an effect on the privacy trouble. In position verification, the position of the vehicles should be verified. The advantage of position verification is that each node has its unique identity and Radio resource testing based on assumption that all physical entities were limited in network.

2.2 Bogus Information

The Bogus Information attack can be performs on insider and outsider both. In this

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

attack, the incorrect or bogus information transmitted in the network.

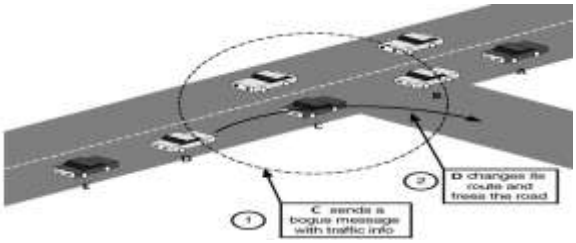

Fig.2.2. Bogus information attack [5].

Fig 2.2 shows that the bogus information attack. In figure two attackers (A and C) transmit false information. So that this false information affects the decision of other vehicles (D) and thus it clear the way of attacker E.

The solution of this attack is ECDSA (Elliptic Curve Digital Signature Algorithm). ECDSA is a message authentication scheme. ECDSA use hashing technique to keep message more secure and provide strong authentication scheme to the destination vehicles. Each vehicles consists of private keys and public keys. The public key is publicly available to all vehicle users in VANETs and private key is private. The source and destination nodes are agree upon the elliptic curve domain parameters. ECDSA scheme was more secured for message authentications. So that hashing is a strongly secure technique .If there is changes in messages then there will also changes in the hash message, which is make it unique message.

2.3. Timing Attack

In timing attacks, when malicious vehicles receive a transmitted message, then they do not forward it as normal way but they add some time slots to the original message to create some delay. For that reason destination vehicles cannot receive the message at a proper time.

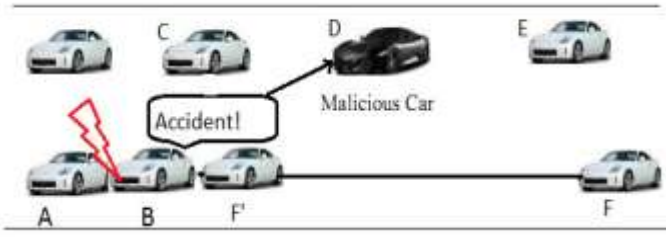

Fig 2.3 Timing Attack [5]

Above figure shows the timing attack. In that there is an accident between the two cars A and B. Car D is a malicious car and he announced about the accident but there was delay in the transmitted messages. This delay can perform by the malicious node D because he add the some time slot to the original messages. When car F reaches the accident place then he receives the message. Car F receives the message late because of the delay in transmitted message (F').

To avoid the Timing Attack, data integrity verification is required. This verification can eliminate any time slots that can be added to packets. Also there is another technique from which we can be avoid timing attacks i.e. TPM (Trusted Platform Module). TPM is security approach for maintaining the integrity of messages by using strong cryptographic functioning modules. Timing attack was avoided by using two protocols, Privacy Certification Authority (PCA) and Direct Anonymous Attestations (DAA).TPM has two main advantages: (1) –Secure piece of hardware with cryptographic capability and (2) - Ability to protect and store data in shielded location. TPM is the powerful solution for evenly other attack that violates data integrity. However, like any other cryptographic solution, TPM cannot positively affect to the performance of network.

2.4. Hidden vehicle Attack

Providing the false information about the position of the vehicle is the example of the Hidden vehicle.

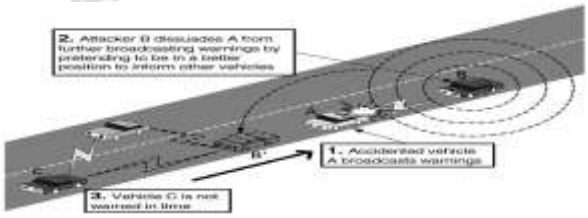

Fig.2.4. hidden vehicle attack [5]

Above figure shows the information about the hidden vehicles. In this figure vehicle A does not receive the information about the vehicle B. Vehicle A assumes that the vehicle B is in better position Vehicle A only receive the warning messages but he doesn't receive the accident message.

2.5. Illusion Attack

In this attack, the destination vehicle does not receive the correct information that is derived from the sensors in the car. For this reason the incorrect traffic

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

warning information is broadcast from one vehicle to another vehicle. Thus in this way illusion attack is successfully generated. In general, drivers' behaviors will be depends on the traffic warning information that have been received. Due to the illusions attack, vehicles received the wrong traffic information. Because of this reason the behavior of the driver is change simultaneously. Thus the disadvantage of the driver behavior becomes the advantage of the attacker. And attacker can create accident, traffic jam and decrease the performance of the network topology. Message authentication and message integrity verification cannot provide the protection against the illusion attacks because attacker can manipulate the system of the vehicle directly and confuses the sensors in the vehicle to send the false information to the other vehicle. Plausibility Validation Network (PVN) is one of the securities Model that can provide security against the illusion attacks. PVN can collect the raw sensors' data and verify that data whether the collected data are plausible or not. There are two types of incoming data consider as input: incoming data from antennas and data collected by sensors. PVN has been provided security against the various types of cryptography methods and various types of attack.

2.6. ID Disclosure

In ID Disclosure attack, a node in the network discloses the identity of neighboring node and then tracks the current location of the target node, and uses this data for a range of the other purposes. This attack fails to agree with the requirement concerning not only the authentication but also provide the privacy. So for prevent from this attack use a holistic protocol. This protocol provides a secure data transmission and detecting misbehaviors sent by the authorized users. Firstly the vehicle should register the nearby RSU. The first phase is the registration phase. In this phase the RSU create a user name and password. Then RSU provide Registration ID to the user. The Registration ID consists of license number and the vehicle registration number. Then RSU authenticate that vehicle by providing verifying certificate. If the authentication failed then data or node should be block. In this the holistic protocol should be used and this protocol consists with whole part rather than individual part. The advantages of protocol are authentications, integrity, availability, confidentiality and non-repudiation properties for VANET.

2.7. Denial of Service (DoS) and Distributed Denial of Service (DDos)

Denial of Service is one of the most important types of attack in the network. This attack performs very different scenarios. In this attack our is aim to prevents the authenticate user in the network. In DoS attack attacker transmit a dummy message to the other vehicle to jam the road or channel. For sending dummy message the efficiency and performance of the network and channel should minimize.

Fig.2.7.1. Denial of Service (DoS) attack [5]

Fig.2.7.1 shows that the DoS attack. In this attack the malicious car transmit both fake identities and dummy messages "Lane close ahead" to the authenticated car and RSU worked for jamming the network.

The Distributed DoS (DDoS) is more dangerous than the DoS attack because in DDoS attack, the number of malicious cars attack on the authenticated cars in a distributed manner with different locations and different time slots.

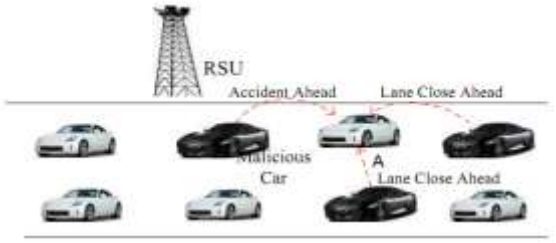

Fig.2.7.2. Distributed Denial of Service (DDoS) Attack [5]

One of the solutions of DDoS attack is use OBS and that is equipped in a vehicles. In vehicle, there is a processing unit that has an important role to suggest to the OBU to switch channel, technology or use frequency hopping technique or multiple transceiver in the case of DoS attack. The DDoS attack work in a distributed and strongly provide protection against the DoS attack where

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

malicious node strongly transmit a large no of fake identity.

In DDoS attack all the vehicles frequently exchange their beacon packets for their presence in the network and also they aware their neighbor. Each node periodically updates a record of its database by exchanging the information with the neighbors. If a node detects in its record that there are some similar IP addresses, then these IP addresses are likely similar of the DoS attack. For prevention from DDos attack, use IP-CHOCK protocol that gives us a significant strength of the locating malicious node without the any other secret information.

2.8. Black Hole Attack

A black hole is an area where the network traffic is changing its direction. In Black hole either there is no node place in that area or the nodes can make community in that area was not interested to participate in the network. In a black hole attack, malicious node introduced itself and it should have a short path to the destination node and thus forms a routing protocol. In this way the malicious node cheat the network routing topology. Instead of firstly seeing the routing table, host node can advertise its rapidly. For this reason the node get the new and fresh route request. When the false route is established then malicious node decide whether to drop or forward the packet.

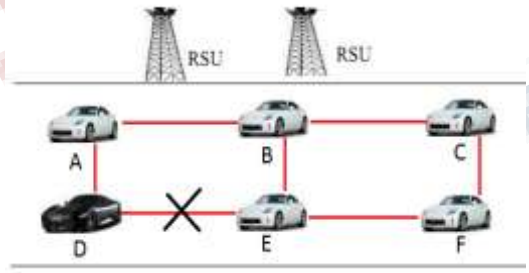

Fig.2.8. Black hole attack [5]

The above figure shows that the Black hole attack. Figure says that when node A wants to send data to the node F but node A does not know about the route from node A to node F. Therefore node A initiate the route discovery process. If malicious node inform that the node A initialize the route discovery then malicious node going active state and form a false route from node A to node F and advertise this route again and again and pretended that this is a very shortest path from node A to node F and node A send his data packet successfully to node F. The attacker itself defines its routing protocol.

To provide prevention from Black hole attack firstly consider the routing protocol in which there are more than one routes from the source to the destination. This solution is only suitable for MANET because In MANET have the large no of mobile nodes and higher end to end delay to find the additional shortest path from source to destination. And second solution is that use sequence number of the packet in packet header. If any packet would be lost then it is easy for the destination node to search the packet by using its sequence number.

2.9. Malware and Spam attack

Malware and spam attacks are also called as a viruses and spam messages, can cause serious disruptions in the normal VANET operation. This kind of attack is executed by the malicious node is in insider or outsider. In this attack, attacker sends a spam messages in the network for consuming the bandwidth and increasing the transmission latency. This attack is not easy to control because the lack of necessary infrastructure and centralized administration. Malware are just like a viruses that interrupt the normal operation of the network. Normally VANET get abscessed due to OBU and RSU software update. Antimalware embedded framework are still providing a problem in VANET network**.**

2.10. Man in the Middle Attack (MiMA)

In this attack, the introducer listen the communication between the two vehicles and pretended to be the one of them by replying the other and inject false information in their conversation.

To provide security from this attack use confidential communication between the two parties and also provide secure authentication and data integrity verifications for preventing messages modifications.

III. VANET PREVENTION TECHNIQUES

In VANET, security is an important issue to secure the human life. For that we consider the five security services to save the human life.

1) Availability:

In VANET, vehicular adhoc network will be available for all the time. To the .application in real time network vehicular network is compulsory.For that availability deal with the various types of nodes and their

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

bandwidth and connectivity. When the availability issue, prevention and detection techniques are come together then new method will formed and this method called as group signature method. This method was focusing on the messages exchange between the vehicles and RSU. In that case group signature method is playing an important role to secure the message communication bandwidth and connectivity.

***2) Confidentiality*:**

This service provides the confidentiality to vehicular network and their communication between the nodes. To maintain the privacy between the nodes, pseudonym scheme will be use. Each vehicle has two keys, one is public keys and other is private keys to maintain the security in the network. In the process of exchange the message between the vehicles, then these vehicles can exchange their keys with each other. But the exchange of the messages and keys s in encrypted form. When this message will reach on the receiver side, then receiver can decrypt the messages and key by using pseudonym scheme. In this scheme the encrypted messages is signed with different pseudo and this pseudo are different for every communication. And this pseudo code will be obtaining by the vehicles from RSU before the pseudo expires.

***3) Integrity*:**

Data integrity is providing the guarantee about the data is to be reach at the receiver side at proper manner. This data was generated by the sender and receiver by the nodes, RSUs, base station. Data integrity can check the data which is send by the sender which is receive at the receiver side properly. To protect the Data Integrity of the message, hashing algorithms, digital signature will be use.

4) Non-repudiation:

Even after the attack happen, non-repudiation provide the facility to identify the attacker. This can prevent cheater from crimes.

5) Authentication:

In vehicular adhoc network, every messages, nodes and application which will be run in real time all are authenticated. The communication between the vehicles can be done when these vehicles and their messages are authenticated. The authentication of the vehicles and messages can be check by RSU. All this process can be done to make sure about the vehicle origin and its authentication level. For that each vehicles can assign pair of keys along with their certificates. And at the receiver side, receiver will check the keys and certificate and assure that sender and messages is authentic and pure.

IV CONCLUSION

Hence, in this paper can describe the various types of attacks which can be done in vehicular adhoc network and how this attack can be work on. We can also the various types of prevention techniques and the performance of these prevention techniques. This paper provides the detail knowledge of the attack and its prevention techniques. With the help of all this information we can provide the security the network and save the human lives.

REFERENCES

[1] Kyung-Ah Shim "Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc Networks Using a Binary Authentication Tree" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 11, NOVEMBER 2013.

[2] Attila Altay Yavuz "An Efficient Real-Time Broadcast Authentication Scheme for Command and Control Messages" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 10, OCTOBER 2014.

[3] Neeraj Kumar and Jong-Hyouk Lee "Peer-to-Peer Cooperative Caching for Data Dissemination in Urban Vehicular Communications" IEEE SYSTEMS JOURNAL, VOL. 8, NO. 4, DECEMBER 2014.

[4] Senthil Ganesh N. Ranjani S. "Security Threats on Vehicular Ad Hoc Networks (VANET)" International Journal of Electronics Communication and Computer Engineering Volume 4, Issue (6)NCRTCST-2013, ISSN 2249–071X.

[5] Vinh Hoa LA, Ana CAVALLI "Security Attacks And Solutions in vehicular Ad-hoc network" International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[6] Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy " Security on

Vehicular Ad Hoc Networks (VANET)" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013).

[7] Greeshma Sarath1 , Devesh C Jinwala2 and Sankita Patel," A Survey On Elliptic Curve Digital Signature Algorithm And Its Variants" Dhinaharan Nagamalai et al. (Eds) : CSE, DBDM, CCNET, AIFL, SCOM, CICS, CSIP – 2014 pp. 121–136, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4411

[8] Mehdi Khabazian, *Member, IEEE,* Sonia Aïssa, *Senior Member, IEEE*, and Mustafa Mehmet-Ali, *Member, IEEE* "Performance Modeling of Safety Messages Broadcast in Vehicular Ad Hoc Networks" IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1, MARCH 2013.

[9] Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member, IEEE, and Cristian Borcea, Member, IEEE "VANET Routing on City Roads using Real-Time Vehicular Traffic Information" December 14, 2007; revised July 24, 2008 and December 23, 2008. This work is supported in part by the National Science Foundation under Grants No. CNS-0520033, CNS-0834585, and CNS-0831753M.

[10] Rashmi Raiya, Shubham Gandhi" Survey of Various Security Techniques in VANET" International Journal of Advanced Research in Computer Science and Software Engineering 4(6), June - 2014, pp. 431-433 Volume 4, Issue 6, June 2014 ISSN: 2277 128X.

[11] .Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim" A Literature Survey on Security Challenges in VANETs" International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012.

[12] K.Susitra, S.Lakshmi Narasimman" A Survey on the Authentication Protocols in Vanet" K.Susitra ,INDIA / International Journal of Research and Computational Technology, Vol.7 Issue.1 ISSN: 0975-5662, March, 2015.

[13].Rukaiya Shaikh, Disha Deotale" A Survey on VANET Security using ECC, RSA & MD5" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015 Copyright to IJARCCE DOI 10.17148/IJARCCE.2015.4637 167.

[14] K.SIVARAMAKRISHNA, Ms.CH.VIJAYA DURGA" Warning message dissemination in vanets using sumo and move" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.

[15] Aqeel Khalique Kuldip Singh Sandeep Sood" Implementation of Elliptic Curve Digital Signature Algorithm" *International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010*

[16] Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz" SUMO – Simulation of Urban Mobility An Overview" IARIA, 2011. ISBN: 978-1-61208-169-4.

[17] Mahendri, Neha Sawal,"A Survey On Vehicular Adhoc Networks(VANETs)" International Journal of Advanced Research in Computer Engineering &Technology (IJARCET) Volume 4, Issue 5, May 2015.

[18] Bassem Mokhtar , Mohamed Azab " Survey on Security Issues in Vehicular Ad Hoc Networks" Alexandria Engineering Journal (2015) 54, 1115–1126.

[19] Archana Phutela, Tulika Mehta" Vehicular Ad-Hoc Networks (VANETs): A Survey" IJCST Vol. 6, Iss ue 1 Spl- 1 Jan-March 2015.

[20] Divya Chadha, Reena" Vehicular Ad hoc Network (VANETs): A Review" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2015.