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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

Authentication Solution for Security Attacks in VANETs

M. Bharat[1], Dr. K. Santhi Sree[2], T .Mahesh Kumar[3]

M.Tech, Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India[1,3]

Professor of Computer Science Department, Jawaharlal Nehru Technological University, Hyderabad, India[2]

Abstract: Vehicular Ad hoc Networks is used for communicating with nearby vehicles and between vehicles and nearby fixed equipments. VANET is also a kind of MANET. VANETs are mainly used for improving safety and efficiency of (future) transportation. There are many chances for the possible attacks in VANET due to open nature of wireless environment. There are different types of attacks in the wireless medium. In this paper, we have discussed about the attacks in the VANETs. We have also proposed the solution for the attacks by providing Authentication in the VANET by using Virtual Certificate Authority among the vehicles. Also, an efficient solution is being proposed for Denial of service (DOS) based attacks which uses the redundancy avoidance mechanism consists of rate of decreasing memory among the vehicles. This solution will basically add more security to the already existing solutions of using various alternative options like frequency-hopping, channel-switching, communication technology switching and multiple-radio transceivers to counter affect the DOS attacks.

Keywords: VANET, sensors, Virtual Certificate Authority, Denial of service.

I. OVERVIEW OF VANET

A Vehicular Ad-Hoc Network (VANET) is a technology that uses moving vehicles as nodes in a network (mobile network) so each vehicle can receive and send others messages through the wireless network. VANET turns every participating vehicle into a wireless router or a node, allowing vehicles approximately 100 to 500 meters distance between them to connect and, in turn, create a network with wide range. As vehicles fall out of the signal ranges and drop out from the network, other vehicles can also join the network, connecting vehicles with other vehicles using the internet. The vehicles are equipped with advanced wireless communicating devices without any wire between them. These types of networks are useful to provide variety of services like Intelligent Transportation System (ITS).

For ITS, safety applications are very important. For example, if a vehicle detects any road accident, it will immediately inform the other neighboring vehicles about this road accident. The safety messages must and should be delivered to each and every neighboring node without any delay. If there is any delay in the messages, there could be loss of life (accident). Valets are useful for communication hunch, notifications of emergencies and warnings about the traffic conditions, and also in distributing information about road conditions and maintenance, weather forecasts or some other related data distribution requirements among the vehicles.

The first systems that will join the technology are the police and the fire vehicles for communicating with each other for the safety measures. VANETs use some Ad-hoc Communication to provide the advanced driver assistance systems (ADAS) for performing an efficient driving assistance and the vehicle safety. The communications may include data from the roadside and from other vehicles. VANET research aims to provide drivers with information about the obstacles on the road and emergency events, mainly due to visible horizon limitations and processing delays. So, we can surely say that VANET is very important component of Intelligent Transportation Systems, by having a rich set of applications that can provide to the customer. Fig 1. Shows the VANET Structure.

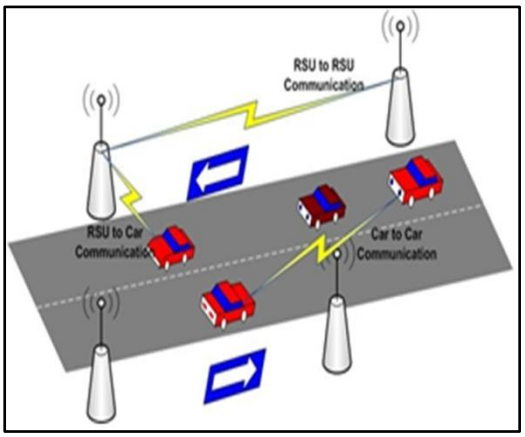

Fig. 1 VANET Structure

II. TECHNOLOGY

Wireless Communication is used to transfer information between two or many points that are not physically connected. Earlier we know only radio and television. Later technology is increasing. We have cell phones, pagers, Bluetooth etc. Over Last few years, technology for wireless communication has many advantages. It allows efficient working, mobility etc. Wireless technology is divided into many groups. These are divided based on the bandwidth. Moderate bandwidth is GSM, GPRS or UMTS and high bandwidth is WLAN (Wireless Local Area Network). Here we mainly use the WLAN. We have two different standards in Wireless LAN: HIPERLAN from

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

European Telecommunications Standards Institute (ETSI) and 802.11 from Institute of Electrical and Electronics Engineers (IEEE). These days' 802.11 standards are almost dominating in the market. Every device is well engineered. So every device is fitted with sensor to use the wireless technology. Here in this paper we use DSRC (Dedicated short Range Communications).

Let us consider an example how the transfer of messages from different nodes take place. We take an example of University. Nodes are placed at different places. The nodes can communicate with each other via road or with WLAN. Through road, the transfer of message takes long distance and takes more time to travel. The distance the messages need to travel from different nodes are shown below in Table 1. The distance is shown in meters. The map is also shown below in Fig 2.

TABLE 1. DISTANCE THROUGH ROAD.

	N1	N2	N3	N4	N5	N6
N1	0	800	1100	700	700	1200
N2	800	0	700	900	300	900
N3	1100	700	0	1400	600	400
N4	700	900	1400	0	800	1300
N5	700	300	600	800	0	800
N6	1200	900	400	1300	800	0

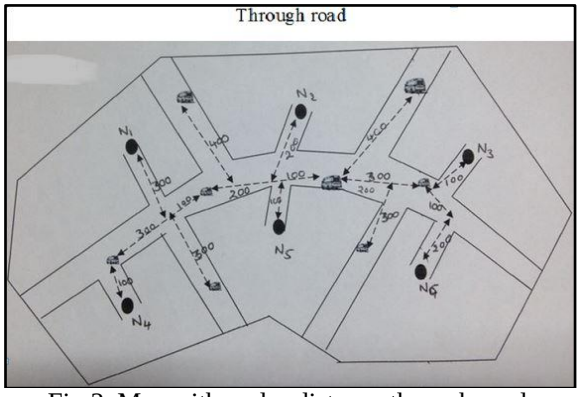

Fig 2. Map with nodes distance through road

The same messages can also travel via. WLAN. Using WLAN the distance the message need to travel will decrease. Since the WLAN uses the medium of air. The distance of the messages are shown in below fig 3.

TABLE 2.DISTANCE THROUGH WLAN

	N1	N2	N3	N4	N5	N6
N1	0	500	800	400	500	800
N2	500	0	500	900	300	500
N3	800	500	0	1100	500	400
N4	400	900	1100	0	600	900
N5	500	300	500	600	0	300
N6	800	500	400	900	300	0

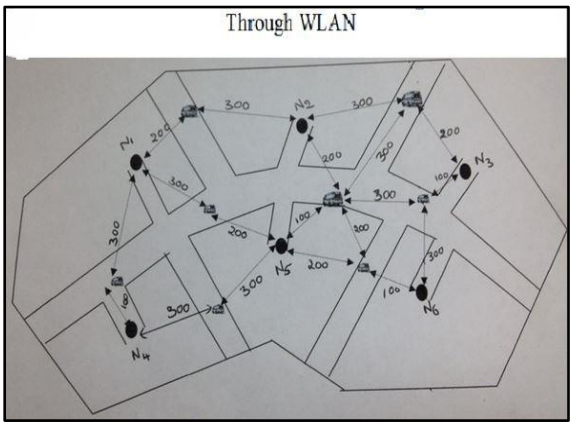

Fig 3. Map with nodes distance through WLAN

III. ATTACKS

While transferring messages will will come across many types of attacks. In this paper we are focusing on attacks against the message itself rather than the vehicle, as physical security is not in the scope of this paper. We focus on the various attacks that are formed in VANETs.

A. *Denial of Service attack*

This attack happens when the attacker takes control of a vehicle's resources or block the communication channel(jam) used by the Vehicular Network, so it prevents important information from arriving. It also increases the danger to the driver, if it is depended on the application's information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles [1], [2], [3], and [4]. See Fig 4.

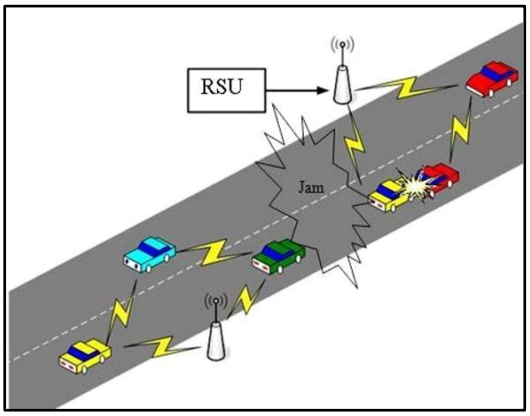

Fig 4. Denial of Service attack

B. *Message Suppression Attack*

An attacker will selectively drop packets from the network, these packets may hold critical information for the receiver, the attackers suppress these packets and can use them again in other time [2]. The goal of these type attackers would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to the roadside access points. For instance, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive any warning and forced to wait in the traffic for long time.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

C. *Fabrication Attack*

An attacker will make attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else. This attack includes fabricate messages, warnings, certificates, identities [2], [4] [5].

D. Alteration Attack

This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested.

E. *Replay Attack*

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending.

F. *Malicious Attacker*

This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets, and they will have access to the resources of the network. For instance, a terrorist can issue a deceleration warning, to make the road congested before detonating a bomb.

IV. PROPOSED WORK

There are many solutions given by many people and many of them have successful in implementing the solutions for the attacks. Now in this paper, we also have proposed a solution for the Attacks and are solved by using the Authentication process. This Authentication process is discussed below. By using this process we can easily find out who is going to attack us, since the unauthorized person will be easily identified. The Attackers who want to attack the other vehicle or trap other vehicle by false cannot do because the attacker will not be authenticated and the messages from the attacker will not be taken by the authorized vehicle. The authentication is provided by using the virtual certificates. Since the vehicles are attached with sensor to sense the information and as they are with limited memory, the virtual certificate will take less memory compared with the other solution. Lets us see the solution below.

A. Authentication using Virtual Certificate

Authentication using Virtual Certificate authority (VCA) [1] will provide an initial trust between vehicles. This is done by creating and verifying certificates. The certificates are built before the deployment. The Virtual Certificate authority is responsible for the WSN nodes are placed in the network by calculating the nearby cars distances. The Virtual Certificate authority will issue the certificate to each vehicle. Before that malicious vehicles are detected based on the threshold value. The major devices used in this architecture are TC (Trust centre) or Road side Unit, which is the device responsible for defining the communication channel, starting the network, key distribution, key management, and implementation of a network access control policy. The vehicle with the sensor on the road and the road side unit are called is the MED (Manufacturer's End Device) and MCA (Manufacturer's Certificate Authorities) acts as a trusted third party between the TC and the MED. The GVCA stands for Global Virtual Certificate Authority and it is the trusted third party between the TC and the MCA. It is also responsible for signing the certificates of the TC and the MCA prior to deployment at the time of manufacture. The second virtual device is Manufacturer Virtual Certificate Authority (MVCA), is the trusted third party between the MCA and the MED. Both the MCA and the MED have their own certificates signed by the MVCA and implanted prior to the deployment. Fig 5. Shows the network of the cars.

The Fig 5. Explains about the process of the involved authorities and who is contacting whom. The dotted lines show the invisible devices and the normal lines shows the direct contacts between them. GVCA and MVCA are virtual and the TC, MCA, MED are physically present. The physically present objects can directly contact each other.

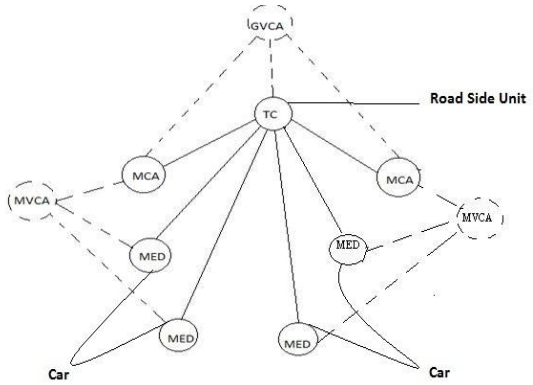

Fig 5. Network with Virtual Certificate Authority

V. CONCLUSION AND FUTURE WORK

Vehicular Ad Hoc Networks is promising technology, which gives a lot of chance for attackers to attack the network and challenge the network with their malicious attacks. This paper gave a wide analysis for the current challenges and solution to the attacks. We have proposed the Authentication by using the Virtual certificate Authority. This authentication will help in identifying the malicious nodes easily. The trusted nodes can avoid the messages from the malicious nodes. This solution will help the drivers to drive safely and easily.The critics for these solutions, in our future work we will propose new solutions that will help to maintain a securer VANET network, and tested by simulation.

REFERENCES

[1] M.Bharat, "A case study on Authentication of Wireless Sensor Network based on Virtual certificate Authority", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol.1(6), July 2014.

[2] I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", Networking, IEEE/ACM Transactions on Volume 16, August, 2008.

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

[3] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October2006.
[4] M Raya, J Pierre Hubaux," The security of VANETs", Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.
[5] Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005
[6] Security & Privacy for DSRC-based Automotive Collision Reporting.
[7] http://en.wikipedia.org/wiki/Vehicular_ad_hoc_network

BIOGRAPHIES

M.Bharat is a student pursuing M.Tech in Information Technology in Jawaharlal Nehru Technological University Hyderabad. His interested areas are Network and Cloud Computing.

Dr. K. SanthiSree is a Professor, Dept of CSE, School of Information Technology, JNTUH, Hyderabad. She has 14 years of teaching and Research experience. Her interested areas are Data mining, Cloud computing, Algorithms, Information retrieval Systems. She is a member of various professional bodies like ISTE, IETE, IEI, and CSI.

T.Mahesh kumar is a student pursuing M.Tech in Information Technology in Jawaharlal Nehru Technological University Hyderabad. He is a Student member of IEEE. His interested areas are cloud Computing, Multimedia and Big Data.