ISSN No. 0976-5697

Volume 6, No. 6, June - July 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Research on various Attacks in VANET

Namarpreet Kaur
M. Tech Computer Science
Punjab Technical University, India

Aman Arora
H.O.D, M.Tech Computer Science,
Department of CSE

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 . In Vanet Communication takes Place between Vehicles Or Between Vehicles and a fixed equipment Which is known as Road Side unit [1]. Road Side Unit (RSU) are wireless access points, that act as intermediates to the DMV (Department of Motor Vehicle) by provisioning along the road. The Vehicle Records are maintained By DMV Which is a trusted Party and it also Send Certificates to Authorized Vehicle When it Applys For the Registration or renew its registration The DMV generated these Certified Pseudomics more early because of the so much resources it had .These Certification is necessary When we Want to check that the vehicle is authorized or not. DMV cant give the Certified Pseudomics to malicious vehicles .However all the communication takes place on Communication Channel depends on DMV Thus it acts as a Bottleneck .All the Vehicular activities are Monitored by RSU and it reports to DMV if it Found Some illegal Behavior Of Vehicle . The RSBs may get compromised, hence the DMV cannot use them for critical functions. However, they can be used to improve the scalability of a system.[2]

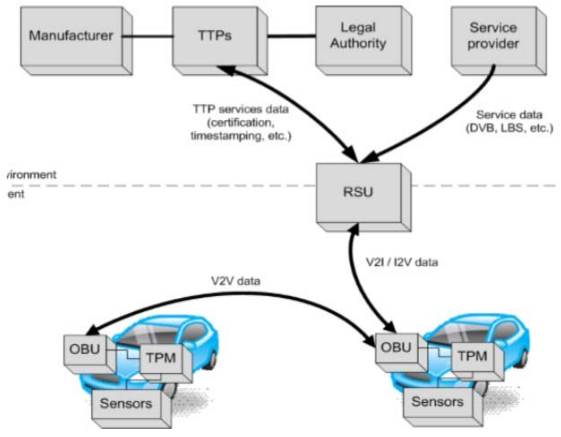

Figure. 1 : Road Side Unit [2]

Fig 2 shows the VANET architecture in Which one hope called vehicle or Road Side unit Communicates With other hope called Vehicle in the network. Vanet is designed to improve the Safety of Driver and Provide Comfort to the driver So that the mishappenings on the road can be avoided. In VANETs, the types of communication are as follows:[1]

a. Vehicle-to-Roadside Communication
b. Vehicle-to-Vehicle Communication
c. Inter Roadside Communication.

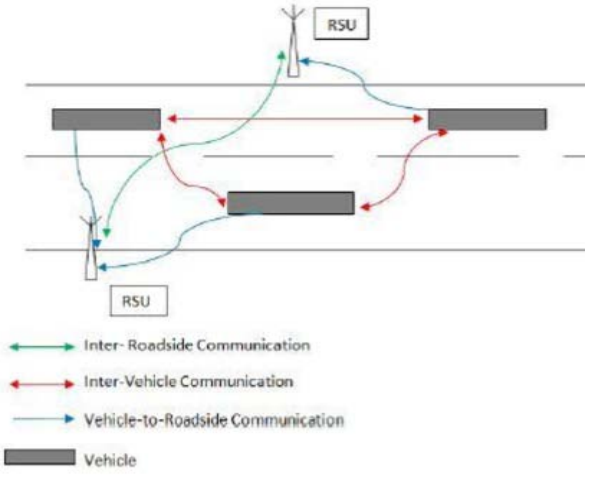

Figure 2 : Vanet Architecture [1]

The radio used for the communication is DSRC i.e Dedicated Short-Range Communications [1]. With the help of Which we get all the information about the network in which the Vehicle Communicates in order to avoid the problems Such as delays in Commuication or Delays in Vehicles to Reach their destinations that Occur due to Road Accident [3]. Infrastructure is Called as MANE and it is applied to ITS to form Vanet[4]

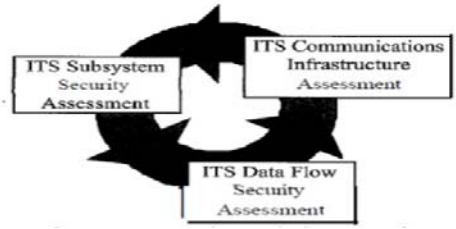

Figure 3: ITS Security Analysis Approach[4]

Hence in Fig 3.ITS relies heavily on collaborative operation of Many Sub systems Which in turns depend Upon Communication Resources that are expected to operate Without delays. ITS Provides Many Benefits [4]:

a. Improved Safety
b. Reduced Traffic
c. Improved Public Transportation
d. Reduced Commercial Spending
e. Reduced Government Spending
f. Reduced Pollution [4]

The drawback to use 802.11P is that it is low scalable it means the Protocol used in this is not available to Povide timing Acuuracy When the traffic load on the Same area is high i.e. when the number of cars in the same area is high [5].

A. The characteristics of VANET are as follows [1]:

a. Large Connections are Established and large number of nodes are Covered
b. No power issues
c. Network size is not bounded means We can increase it or decrease it depend upon our requirement .
d. The data or Information can be exchanged on time[1]

The Security in Vanet is an Important Concern because the Communication can take Placed in Wireless environment Thus in Order to avoid Malicious Vehicle to Participate in Communication Short range Radios are installed in Vehicle Or at Road Side unit to identify the Vehicle [1]..

II. SECURITY GOALS

The goals to assure or secure VANETs are same as that for secure any network. The main goals of Security are authentication, integrity, availability, confidentiality, and non-repudiation [1] [6] [8].

***a. Authentication*:** It is used to Assure that the Communication has been takes Place Between the Valid nodes Means it is use to check the identity of all Participating nodes so as to assure one node That it receives the message from authorize Sender [1] It is also use to assure the Identity Of Vehicle and Fixed Equipment In this Many keys Which may be Public or Private In order to assure that only authorized Vehicles can acess Fixed equipments[6].

Authentication using Virtual Certificate authority(VCA) [7] It will Provide the Trust between the Vehicle Means the Vehicle Which Contain Certificate assures other Vehicles and Fixed equipment that it is authorized user and it has authority to acess Road Side Unit [7]. 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. [7].

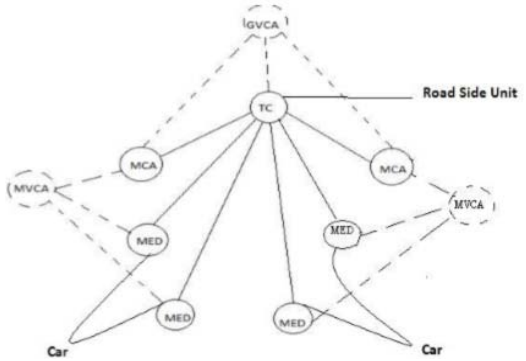

Figure 4: Network With Virtual Certificate Authority [7]

b. Confidentiality It deals with the Protection of data from unauthorized user which is necessary to assure that the data transmission takes place between authorized users Because in case of vanet data security is main concern So that the data is not hacked by unauthorized user otherwise Many Confidential information is disclosed to malicious vehicles [1].

c. Integrity It deals With the Integrity of the message that means the message cant be edit or erased by the hackers otherwise the authorized users cant get What they want to get [1]. In order to obtain integrity digital signatures With Passwords has been used that is very helpful in maintaining the Integrty[6]

d. Availability: It assures that the authorized users get the data Whenever they required it Without any delay such as loss of power etc [1]

e. Non-repudiation Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received some message. It is needed for the sender in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be employed for liability purposes[8].

III. ATTACKS IN VANET

In order to design the security solution for VANETs we should learn different types of security threats, the types of attackers and attacks.[1]

A. Classification Of Attackers [1][9][11]Different types of attackers are there:

a. Snoops: In this attack the attacker found the Position of particular vehicle or target vehicle with the help of driver's house address and his Working address and after knowing all this he will missuse this address.[9].

b. Passive Attackers: This type of attack has been done under Wireless communication. In this attack the attackers collect traffic data and passed it to other attackers who are not participating in the communication. [1].

c. Active attackers: This type of attack has been done by the attackers who are participating in communication they can send wrong packets on the network instead of actual receiving packets. [11]

d. Malicious Attackers: Malicious attackers are the attackers that are not personally benefited by the attack but its workl is to harm the functionality of other vehicles. [11]

IV. TYPES OF ATTACKS

There are many different types of attacks occurred in vanet [1][4][7][5][10][11]

a. ***Denial of Service (DoS)*** : In this type of attack the malicious attacker disturbs the whole communication channel at which the communication takes place thus due to this disturbance it results delay in all services and this delay in real time system even for a short period affects the whole task [4] .

b. ***Fabrication Attack*** : In this attack the attacker send false messages on the network. This information may actually be false or attackers claims that it may be anything else[7].

c. ***Message Suppression Attack***,: In this attack the attackers drop particular packets which contain important information from the network and used these packets later [5]. Its aim is to prevent the registration authority to learn about the collision occur in the vehicles [10].

d. ***Cheating with Sensor Information*** : This type of attack has been done by the attacker who is active it changes the direction , position and speed of other vehicles in order to misguide other vehicles[11].

e. ***Sinkhole Attack*** : In this attack the attacker has a full control on the particular area and when the traffic pass over it the attack has been made by the attacker and this results other attacks has introduced[1]

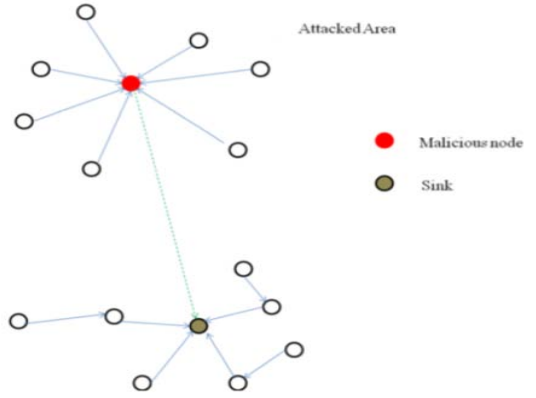

Figure 7 : Sinkhole Attack [1]

V. RELATED WORK

Vanet is the emerging area of Manet in Which the vehicle act as a Mobile nodes. Vanet is mostly used today because of many important features it provided such as security and online toll payement etc .There are some attacks occur in vanet and it use holistic protocol provide solutions to these attacks [1] Privacy and security is becoming an important feature in intelligent transportation system because of many important feature it provided.

Vanet is an example of todays ITS .Which has many promidential features. ITS approach is very useful in providing security and prevent the vehicles from global transportation system Which enables the group of malicious vehicles to create fake identities[4]. In Vanet the communication has been done in Wireless environment due to this many attacks are possible . In order to overcome these attacks We use Authentication Certificate Scheme in Which First of all RSU monitor the Performance of all Vehicles and then report to the WAVE .If the vehicle is not malicious then the certificate has been send to the authorize user otherwise the node will be blocked[7].

VI. PROPOSED WORK

This segment compares the the working of signature verification in our protocol with that in ECPP and GSIS (V2V communication scenario).With our protocol, to verify n safety messages (essentially, to verify signatures in n safety messages) from the same group, in the required time

$$T_o - 2\tau_m + \frac{14n\tau_e}{4.8} - 2 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms.}$$

The cost required to verify n safety messages from two different groups is

$$T_o' - 4\tau_m + \frac{14n\tau_e}{4.8} - 4 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms.}$$

Time cost with ECPP, to verify n safety messages, the time cost is

$$T_E - 3n\tau_m + 11n\tau_e - 3n \times 4.5 + 11n \times 0.6 \text{ ms.}$$

With GSIS, the time cost of verifying n safety messages increases with the number of revoked certificates of vehicles in the revocation list. It is fair to Compare our protocol with GSIS when the revocation list is empty. In this case, the computation time of signature verification with GSIS is

$$T_G - 5n\tau_m + 12n\tau_e - 5n \times 4.5 + 11n \times 0.6 \text{ ms.}$$

Fig 10 Shows the Time Cost Ratio $T1 - T_0/T_E$ and T2 - T_0/T_G . Fig 11 Shows the Time Cost Ratio T3-T_0'/T_E and T4-T_0'/T_G

From Figures 10 and 11 , it is apparent that the computational over head of signature verification in our protocol is always much lower than that in This advantage of our protocol is more obvious when the number of vehicles within the communication range grows. In VANETs, vehicles broadcast safety messages every 100-300 ms to other vehicles. In this way, a vehicle may receive lots of safety messages from other vehicles in a very short period of time. Hence, the efficiency of the signature verification is vital when the number of vehicles within the communication range is high

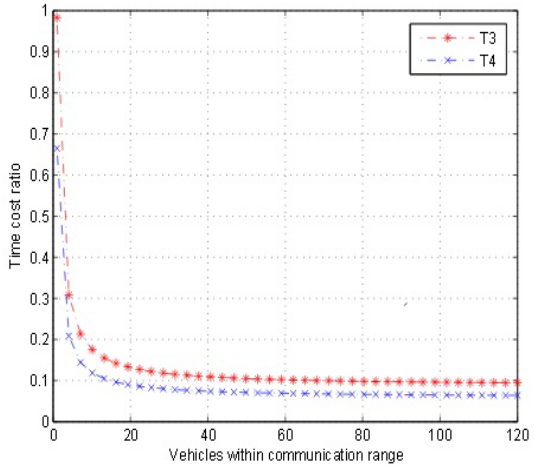

Figure 10 : Vehicles Within Communication Range

The group signature can only be verified one by one, while in [Lu08], before verifying a signature from a vehicle, one should first verify the short-time anonymous certificate of the vehicle. In contrast, in our protocol, no short-time anonymous certificates are required and the batch verification technique s used. This largely improves the efficiency of our signature verification.

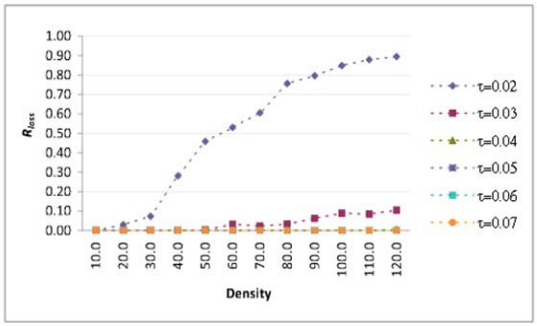

Figure 11 :

To obtain lower average message delay, the batch verification interval should be as small as possible. However, if is too small, some messages cannot be verified and the average message loss rate grows. Hence a balance point has to be found, and from might be an ideal balance point

VII. CONCLUSION

We have focused on providing security and privacy in VANETs. Several protocols were proposed to secure vehicular communications. Our first protocol is designed for mature VANETs, in which the RSUs are densely distributed. a devise for VANETs in an early deployment stage, i.e.with few available RSUs, and it aims to process emergency announcements as soon as possible. This concentrate on signature aggregation/compression in VANETs, by noting that signatures might have to be stored for a long period for possible liability investigation. Our last protocol deals with value-added services in VANETs, and specifically it focuses on providing secure and privacy-preserving LBSs in vehicular networks.

VIII. REFERENCES

[1]. TamilSelvan1, Komathy Subramanian2, Rajeswari Rajendiran3, "A Holistic Protocol for Secure Data Transmission in VANET". International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, December 2013 ISSN (Print) : 2319-5940 ISSN (Online): 2278-1021.

[2]. Mukul Saini1, Kaushal Kumar2 and Kumar Vaibhav Bhatnagar3, "Efficient and Feasible Methods to Detect Sybil Attack in VANET International Journal of Engineering Research and Technology. ISSN 0974-3154 Volume 6, Number 4 (2013), pp. 431-440

[3]. Khalid Abdel Hafeez,, Lian Zhao, , Bobby Ma and Jon W. Mark, "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 7, SEPTEMBER 2013

[4]. Amit Kumar Tyagi, Surendra Kumar Tyagi, Prafull Kumar Singh "A Survey on Security Provided for DoS(Denial of Service) Attack in Intelligent Transportation Systems,". International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 2, February 2014 ISSN: 2277 128X

[5]. Alexey Vinel, "3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Application" IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 1, NO. 2, APRIL 2012..

[6]. RashmiRaiya*,Shubham Gandhi "Survey of Various Security Techniques in VANET". International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6, June 2014 , ISSN: 2277 128X

[7]. M. Bharat1, Dr. K. Santhi Sree2, T .Mahesh Kumar3, "Authentication Solution for Security Attacks in VANETs", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 8, August 2014 ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940

[8]. Sumegha Sakhreliya*, Neha Pandya**, "A Review on Security Issues and Its Solution's Overhead in VANETs", International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013 ISSN 2250-3153

[9]. Megha Nema1, Prof. Shalini Stalin2, Prof. Vijay Lokhande3, "Analysis of Attacks and Challenges in VANET". International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 7, July 2014)

[10]. S.I.S.Jaffarvalli, D.Ganesh', "Brief overview of VANET routing protocols and their security attacks". International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 6 June, 2014 Page No. 6767-6769

[11]. Mina Rahbari 1 and Mohammad Ali Jabreil Jamali 2., " EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

Short Bio Data for the Authors

Namarpreet kaur She obtained her B.Tech (computer science & engineering) from Sai College of Engineering and Technology, Manawala, Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Security in Vanet

Aman Arora is working as an head of department in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. He obtained his B.Tech (computer science engineering) from Guru Nanak Dev University, Punjab, India, M.Tech (computer science & engineering from Guru Nanak Dev University, Punjab, India.