VANET Security Analysis

Pallavi Patil[1] Prof. Pooja Gundewar[2]
[1]M.E. Student [2]Professor
[1,2]Department of Electronics & Telecommunication Engineering
[1,2]MITCOE, Pune

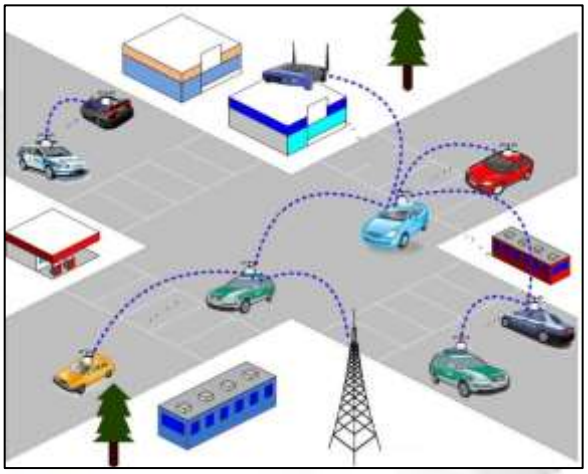
Abstract— *Recently many researches had mean made in Vehicular Ad Hoc Networks (VANET) has gained the main attention of current generation of research efforts, while a scenario solutions to get secure VANET problems, to secure a network system from unauthorized user, hackers and attacks still not good, In this proposed methodology we are trying to get a satisfactory level of output for the driver of the car and manufacturer of the VANET to achieve security of live and infotainment. A robust VANET (Vehicular Ad Hoc Network) is fully dependent on their safety, security and privacy roles, which will are discussing in this proposed paper. In the proposed paper a different types and variety of security problems and challenges of system has been analyzed and discussed to resolve the problem.*

Keywords— Vehicular Ad Hoc Networks (VANET), Inter-Vehicular Communications (IVC), Road-Vehicle Communications (RVC), Mobile Ad Hoc Networks (MANETs), Network on Wheels (NOW), Intelligent Transport System (ITS), Bootstrap

I. INTRODUCTION

The members of IBM-Corporation and Delphi Delco Electronics System proposed a networking vehicle aimed at a wide range VANET application in the year of 1998[1]. The technology of network car frame acquired the attention of all over the world scenarios in the advancement of telecommunication technology.

So many new projects have been launched in recent decade to provide security and targeting on the dream of networking car by realizing it and implementation of VANET vehicular networks[6]. A German researcher founded (NOW) the project Network on Wheels under guideline of Daimler Chrysler AG, AG, BMW, Fraunholfer, Volkswagen AG and Institute of open communication systems, Siemens AG in the year of 2004[3]. The latest technology of IEEE 802.11 Standard for communication accessing data. The data security for car to car communication and resolving the technical issues in wireless communication. Its goal to make a European industrial standard for car to car wireless communication implanting over all the brands and franchises[2]. Fleet Net is other program of European which ran the program for a duration of 2000 to 2003 and this ad hoc research is dominated full efforts by standardize protocols MANET, and protocol like MANET researches focused mainly on network layer and the ultimate issues and challenges are solving the problem of how to get reach point not only directed with radio range technology by employing as forwarders/members, while the pushing for a new research effort in the respective area in order to gain the goal and target of reducing the accidents of car up to 50% by 2010 with the help of European Commission aiming to obtain a satisfying level of safe VANET[4].



The wireless radio technology used for such type of communication is used for Short-Range Communications (DS-RC)[7], which had been associated as new band in the year of 1999 by the (FCC) Federal Communications Commission. Such band allocated is supporting the frequency of 75 MHz at 5.9 GHz in Intelligent Transport System (ITS) applications in upper America [2]. VANET safety and security should give assurance of four targeting goals:-

1) It should be guaranteed for the information received are completely correct.
2) Message integrity and source authentication (source is who he claims to be the associates).
3) A point or a location which is sending the data cannot be identified.
4) Tracking system (privacy) and robust system.

Our paper of VANET attack and attackers to present a problems that is facing by the VANET, in coming section we are analyzing 3 VANET challenges like Tracking, Privacy and mobility which considered as hardest and biggest problem of security for VANET [8][1].

A. How VANET works?

Vehicular Networks System used for VANET consists of the large number of points/nodes/location, its approximately number of time the vehicles exceeding 750 million user in the world currently today, these vehicles will needed an authority to govern it, here each and every vehicle can communicate with other vehicles using wireless radio communication signals DS-RC (5.9 GHz), of range that can reach up to 1 KM, this communication is an type o Ad Hoc wireless communication that means that every connected location can move freely, no wired communication is required [3], the routers which is used for such type of communication devices is called Road Side Unit (RSU), the RSU works as router between vehicles on the respective road and communicating with other networking devices [4]. Each vehicle has separate on board unit (OBU), such kind of unit communicating using the vehicle with RSU with DSRC radios, and other device is Tamper Proof Device

(TPD), this VANET device holding the secrets vehicle information, like all the information about the vehicle like drivers identity, keys, trip details, Mileage, rout, speed, etc[6].

II. VANET SECURITY ISSUES

These are the various types of attacks which are suffered by VANET are discussed in the following categories.

A. Attacks:-

In our proposed paper we are focusing on attacks and security issues to get perpetrated against the false message itself rather than the car system, as scope of this paper is limited to physical security [1].

B. Denial of Service attack:

In the system of computing the data, a (DoS attack) denial of service attacks is a cyber security attack where the hackers seeks to the make machine or network resource system unavailable to intended login users by indefinitely or temporarily disrupting service of the host connected to the wide range Internet protocols [2]. The (DoS attack) Denial of service is typically implemented by flooding or exploding the pointed/targeted resources or machine with superfluous requests in attempt to override systems functionality and prevent all legitimate requests [9].

When the hackers take control of VANET resources or jams system the wireless communication protocols using by the Vehicular ad hoc Network, so it is critically important to prevent critical information from receiving [1]. It also leads to increase in the danger to the driver life, if it is dependent on the applications of the system information [10]. For instance solution, if malicious wants to form a massive attack pile up on the highway road, it can be done by making an accident and using the DoS attack for preventing the warning for reaching to the approaching vehicles/car [2]. In this section we discussed a solution for DoS attacking problem and exploring that the existing solution on such topics as hopping do not completely capable of solving the problem. The multiple radio transceivers is very useful for operating in disjoint frequency wavelength band, can be approaches

C. Message Suppression Attack:

A hacker and attackers dropping a selectively packets from the network system, these can hold the packets which contains a critical information from transmitter for the receiver, the attacker attack these packets and can gain the required information and able to use them again in other time for destroying the system [3]. The goal of such attacker is to prevent insurance authorities and registration to learning about collusive involvement to his vehicle or/and to avoid delivering collision packets for reporting roadside access points [5]. The warning will not receive to the vehicle and forcefully has to wait in the giant traffic.

D. Fabrication Attack:

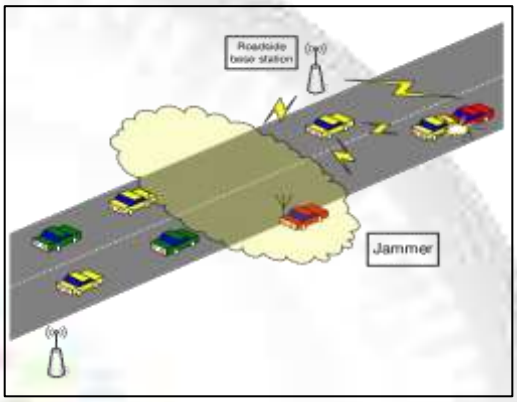
An attacker can able to create this type of attack by sending/ transmitting false information into the system of network by wireless medium, the transmitter could claim that it is somebody else or information could be the false [1]. This attack included fabricating messages, certificates, identities, and warnings.

E. Alteration Attack:

This attack take place of action when the hacker or attacker alters an existed data files, it contains delaying of time to the transmission of the data packets, altering the actual entry and replaying earlier transmission of the data transmitted for current scenario [2].

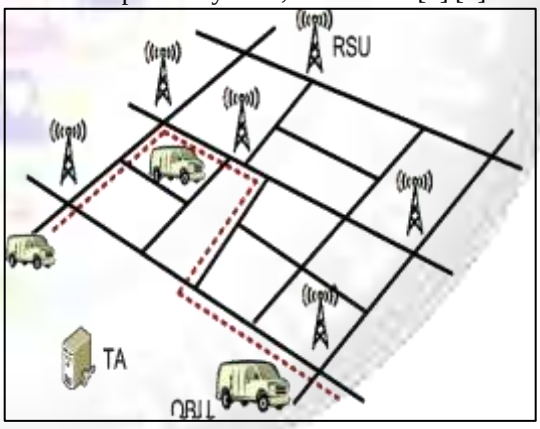
F. Replay Attack:

The situation of the message at time of sending take advantage of attacking when an attacker answer the transmission data of an earlier information [8].



G. Sybil Attack:

The attack like Sybil attack completely dependent on how lowest identities can be identified and generated, the level at which the computing system accepts input from receiver that don't have a chain of trust linking partner to a trusted entity, and whether the given system treated all entities identically or varies partially [7]. When the attacker make a large number of pseudonymous, and claims [4] [1].



III. SECURITY REQUIREMENTS

A. Authentication:

In Communication system every data must be authenticated and secured to create surety for its domain and to control excessive level of the vehicles communication to do such vehicles will assign each and every message to encryption with their certificates and private key along with its signature, at the end user side [2]. the end user will access the message and verify for the passcode key and certificate once to acquire the access, the receiver end confirm the message. Signing in each data port with causes an overhead,

this overhead we can use the approach the reduce Elliptic Curve Cryptography (ECC), the efficient public key for decryption of cryptosystem can sign the public and private key both just for the critical data node only [3].

B. Availability:

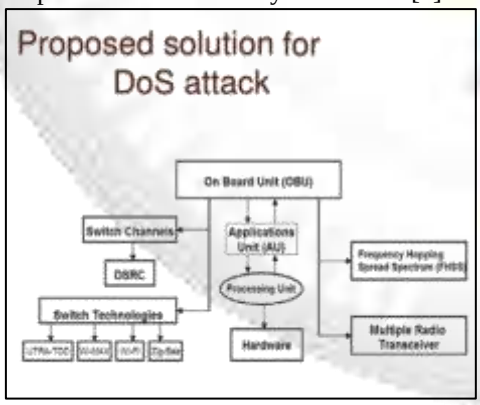
VANET network has to be available all the time for the security reasons, for many application of vehicular VANET networks are needy of real- time application and use, these applications serves faster response time from sensor networks which are used in this proposed method or even Ad Hoc Network, leads to delay in seconds for some applications will create a message useless and maybe the result will be very devastating of availability [6]. The DoS attack make attempt to get real-time value upto demands to makes the system vulnerable and much more effective [4]. In number of data, a delay is present in millisecond which make the data packet meaning-less; this type of problem is much bigger and social, where it is unreliable for the application layer, the potential to recover transmission with unreliable facts to store temporary data messages to completed in next real-time transmission [1].

C. Non-repudiation:

The ability to gain the ability to the attackers even after the crime is happens. This prevents frauds from denying their attack. Any data related to the VANET such as: the speed, time, trip rout, any violation that will be able to store in the TPD, which help for authorization that can retrieve this data [2].

D. Privacy:

The data and details of the VANET drivers are kept away from unauthorized persons and observers, such kind of information like identity, speed and trip path, etc [8]. The privacy can be done by using (partial) anonymous keys and login, these type of login will be changed at specific time of interval in very frequently manner as each and every key could be used for one time only and expires after a duration, TPD is the place where all the keys are stored [1].



IV. CONCLUSIONS AND FUTURE WORK

VANET (Vehicular Ad Hoc Networks) is future technology which gives a surety of security and safety, here we have abundant point which gives chances for attackers and hackers, who will to try challenge to ruin the network with their malicious and various other type of virus attacks [3]. This proposed paper gave a wide analytical result for the current challenges with definitely good solutions, and critics for these solutions with good results, in our future scope we are working on the propose new solutions and analysis that will help to gain and maintain a security of VANET network strongly, and testing it by simulation process [5].

REFERENCES

[1] Second International Conference on Network Applications, Protocols and Services" Security Analysis of Vehicular Ad Hoc Networks (VANET) " Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3 #National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia,2010.

[2] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux,"Certificate Revocation in Vehicular Networks " , Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences ,EPFL, Switzerland, 2006 .

[3] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006.

[4] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.

[5] J. Douceur," the Sybil Attack", First International Workshop on Peer-to-Peer Systems, 1st ed, USA, Springer, 2003.

[6] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[7] M Raya, J Pierre Hubaux," The security of VANETs", Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.

[8] 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.

[9] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and JP Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks ", IEEE Magazine, vol. 10, October 2007.