International Journal of Electrical Electronics & Computer Science Engineering
Volume 3, Issue 1 (February, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Security Issues And Challenges In Vehicular Ad Hoc Networks (VANETs)

Megha[1], Sapna Gambhir[2]
[1]Research Scholar, Department of Computer Engineering, YMCAUST, Faridabad, Haryana, India
[2]Assistant professor, Department of Computer Engineering, YMCAUST, Faridabad, Haryana, India
[1]meghvashist@gmail.com, [2]sapnagambhir@gmail.com

Abstract: This paper presents the overview of vehicular ad hoc network which is subclass of MANETS. Overview of intelligent transportation system (ITS) which uses VANETs for better traffic environment and vehicle safety has being discussed here. Then presents the architecture overview of VANETs and also the brief introduction of communication model used in VANETs for message sharing. Due to high mobility of vehicles on road reliability, security, privacy and fast communication among the vehicles is extremely challenging in VANETs. We explore VANETs on the basis of security threats and recent measures taken regarding to those threats. This paper presents the different issues in securing the VANETs from malicious users and enhances the security parameters. Then we present some of the research challenges in security aspect which are yet to be explored. And then we finally concluded the paper with different perspectives of securing the VANETs.

Keywords: VANETs, ITS, RSU, OBU, Security Issues.

I. INTRODUCTION

Information and communication technology leads to most important innovations in automotive industry and in our society too. Mobile communication has changed the way of exchanging information in last two decades. Using mobile devices, user can exchange information anywhere any time. The use of such mobile communications systems in vehicles is expected to be a reality in few coming years. This new paradigm of sharing information among vehicles and infrastructure will enable variety of applications for safety, traffic efficiency, driver assistance, infotainment, and urban sensing, which will be soon incorporated into modern vehicle designs [1]. To improve the road safety, interest were made in deployment of MANETS and sub field Vehicular ad-hoc networks (VANETs).

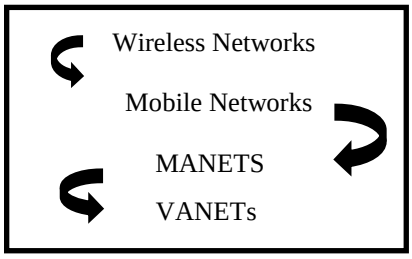

Fig1.Evalution of VANETs

Vehicular Ad hoc Networks (VANETs) are a further evolution of MANETs as shown in Fig 1. It is a promising approach for the Intelligent Transportation System (ITS). ITS is essentially the application of computer and communications technologies coming in aid of the transport problems. ITS technologies enable gathering of data and then providing timely feedback to traffic managers and road-users. ITS results in improved safety to drivers, better traffic efficiency, reduced traffic congestion, improved energy efficiency, improved environmental quality and enhanced economic productivity. Some examples of ITS include Advanced Traffic Management Systems, Advanced Traveller Information Systems, Advanced Vehicle Control Systems, Electronic Toll Collection Systems, Advanced Public Transportation Systems [2].Vehicular ad hoc networks (VANETs) aim at enhancing safety and efficiency in transportation systems. They comprise network nodes, that is, vehicles and road-side infrastructure units (RSUs), equipped with on-board sensory, processors, and wireless communication modules. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication can enable a wide range of applications. But, VANETs are vulnerable to attacks and jeopardize users' privacy. For example, an attacker could inject beacons with false information, or collect vehicles' messages, track their locations, and infer sensitive user data. To thwart such attacks, security and privacy enhancing mechanisms are necessary or, in fact, a prerequisite for deployment of VANETs [3].

Nowadays, the users can access the internet using their mobile devices anywhere anytime and it is becoming the today's necessity. But unlike other wireless environments that are either stationary or with very low mobility, data transmission in VANETs poses more challenges to be resolved. As the vehicles change their topology very frequently, while in motion vehicles basically move away from their home network and cause connectivity breakage. In order to cope with this problem, a vehicle connected to the wireless network should be able to move using different access points available along the road. These access points could belong to different networks or wireless technologies like Wi-Fi, Wi MAX or 3G. Network Mobility (NEMO) is one of the proposed solutions to keep connectivity of users in VANET [4]. If a mobile node is controlled independently then the amounts of control messages get increased and overload the wireless link. In VANETs all nodes follow same trajectory and normally moves with almost same speed,

International Journal of Electrical Electronics & Computer Science Engineering
Volume 3, Issue 1 (February, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

managing the mobile nodes in group deeply affects the amount of control information over the wireless link and bandwidth is effectively utilized. Thus NEMO BS is used to manage nodes mobility in VANETs [12].

In this paper, the overview of architecture of vehicular ad hoc network is discussed in section 2. Communication model used for communication between two vehicles to send data has been discussed. Recent security issues occurring in VANETs and literature survey has been done in section 3. Open research problems are presented in section4th, and then finally the paper is concluded in last section.

II. ARCHITECTUREOF VANETS

VANETs don't have any fixed architecture or topology that it can follow. However, a general VANET consists of moving vehicles communicating with each other as well as with some nearby RSU. A VANET is different than a MANET in the sense that vehicles do not move randomly as nodes do in MANETs .Basically moving vehicles follow some fixed paths such as urban roads and highways. If it is easy to consider VANETs as a part of MANETs, it is also important to think of VANETs as an individual research field, especially when it comes to designing of network architecture. In VANET architecture, an On Board Unit (OBU) in a vehicle consists of wireless transmitter and receiver which get installed on vehicles itself as shown in Fig 2.

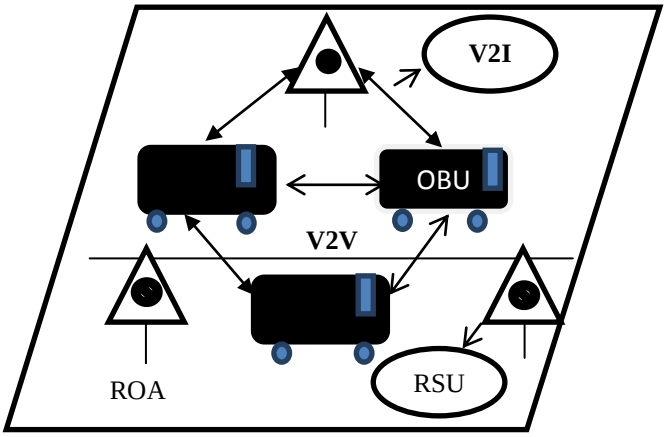

Fig.2. Network Architecture in VANET

In general there can be basically three types of communication based upon the connection establishment among devices.

Firsts cenario is in which connection is established between two vehicles i.e., Vehicle to Vehicle communication (V2V). This can be classified as Ad-hoc architecture. Second scenario is in which connection is established between vehicle and RSU. This architecture may resemble wireless local area networks (WLAN). In third scenario, some of the vehicles can communicate with each other directly while others may need some RSU to communicate. This can be referred as hybrid communication as shown in Fig 3.

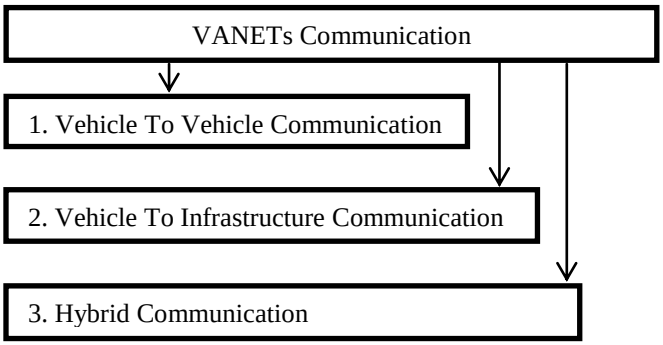

Fig 3.Types of Communication

After introduction of three different and basic types of communication in VANETs the communication model is used for message sharing. The designers of communication model distilled the process of transmitting data to its most fundamental elements. The protocol stack used in VANETs for data exchange consists of five layers and three planes. The planes are to help sensor node to coordinate the sensing tasks and lower overall power consumption.

- The First plane, the power management plane, manages power consumption for example defining sleep and wake status for the nodes.
- The second plane, Mobility management plane monitors the movement of sensor nodes, so a route back to the user is always maintained.
- And finally, the task manager plane balance and coordinates the sensing tasks given to a particular given region.

The five layers of communication model work as follows:

- In physical layer, Federal Communications Commission (FCC) assigned a new 75 MHz band Dedicated Short Range Communication (DSRC) at the 5.9 GHz frequency for Intelligent Transportation Systems (ITS) applications in North America. The band is divided into seven channels [13].
- The data link layer operates on an individual link or sub network part of a connection, managing the transmission of the data across a particular physical connection. Therefore, some mechanisms for service differentiation and admission control are

indispensable. Three levels of priority for messages in VANET can be defined as follow:

(1) Event driven safety messages,

(2) Beaconing safety messages,

(3) Comfort messages

The required mechanisms are dependent on MAC layer policy.

- Network layer is responsible for source to destination delivery of packet. VANET inherits network layer issues from traditional wireless sensor networks and Mobile Ad Hoc networks (MANET) such infrastructures, unstable topology, multi-hop networking, energy efficiency data-centric, routing localization, etc.[14]
- Transport layer makes a busty traffic in to the network. Significant sensory data must be reliably delivered to the base station to obtain detection and tracking an event signal. Simultaneously, if the multi-hop network capacity exceed, congestion is the result. The splitting capability of the transport protocol allows one session to be conducted over a number of parallel network communication paths.
- In case of wireless sensor networks, application layer may be responsible for some functions like generation of information, interest and data dissemination, feature extraction of event signals, and data aggregation and fusion [15].

III. SECURITY ISSUES IN VANETS

Security in VANETs is most prior as this deeply influences and improves road safety and driving conditions. There are different security issues such as authenticity, integrity, privacy, liability that must be taken care of because any malicious behavior of users such as modification and replay attacks with respect to disseminated traffic related messages could be fatal to other users. In VANETs, number of autonomous entities move at very high speed, the randomness of the connectivity between the vehicles and their relative geographic positions raises concerns about users and data security. When information is gathered from and shared among different nodes in VANETs raises the main concern of reliability and data authenticity. As discussed in Raya [5], attacker scan be of mainly three types – “insider or outsider”, “malicious or rational” and last is “active or passive”. And we can classify attacks over messages as “bogus information”, “cheating with position information”, “ID disclosure”, “Denial of Service” and “Masquerade”. Several approaches were proposed by researchers which aim to prevent or diminish the consequences of attacks. It is important to protect life critical information from the attackers as well as the privacy of driver and passengers. [6]

Some of security issues in VANETs are:

- In case of VANETs, the information must be available for all vehicles at any time. The security concern here is, if control channel get flooded with high amount of artificially generated messages either by inside or outside attackers then network nodes ,on board units(OBU),and road side unit(RSU) can’t able to sufficiently handle the data and lead to het attacked by malicious user.
- Another security issue is when some inside user broadcasts the false message or inject some malware or virus into the network then it can cause the fatal harm to VANETs users by ignoring the other useful information. And introduction of spam messages on VANETs also by inside user can increase transmission latency. And spam messages are not very easy to detect because of lack of basic infrastructure and administration in VANETs.
- There arises another security issue, when a reliable node refuses to participate in established network voluntarily. And this leads to broken route and leading to failure of propagated messages.
- In VANETs to become a legitimate user there is only need of functioning onboard unit(OBU). And that user can fake its identity and can cause fatal harm in VANETs if it gets into the network.
- Next security issue is if any attacker re-injects previously received packets back into the network. Thus authentic and accurate reporting of vehicle position information must be ensured so that accurate source of time must be maintained. And also vehicle involved in communication can’t able to fake its own position which can lead to Sybil attack.
- Next issue is that, periodic safety messages are basically single hop broadcast, thus focus has been mostly only on securing the application layer. For e.g.- IEEE 1609.2 std. doesn’t bother about protection of multi-hop routing. And this allows attackers to potentially partition the network and the delivery of event-driven safety messages gets impossible.
- Another security issue is of eavesdropping of frequent user over the road and collection of their data and gathering of their location information. Thus location privacy and anonymity are important security issues for VANETs user.

International Journal of Electrical Electronics & Computer Science Engineering
Volume 3, Issue 1 (February, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

IV. LITERATURE SURVEY ON SECURITY ISSUES IN VANETS

In [7], Authors created a secure MAC protocol considering the DSRC channel structure. This protocol discusses different security parameters and ensures the freshness of the message using some time stamp, digital signature and trusted certificate. The protocol basically uses the concepts of IEEE 1609.2 security infrastructure including PKI(public key infrastructure) and ECC(elliptic curve cryptography).Queues are maintained for different messages according to their priority and a scheduler is used to schedule high priority message over lower priority message. In this paper, each OBU maintains a secure database consists of cryptographic keys used for digital signature and these keys are always refreshed by some central authority. For safety messages confidentiality is not much required so they can be sent in plain text but needs authentication and integrity thus digital signature is attached. Message remains of very short size.

In [8], a symmetric –masquerade security scheme (SMSS) has been discussed. This reduces the system overhead in V2V communication. IN this scheme, the privacy is maintained of vehicle by assigning a pseudonym by some base station and one to one mapping is maintained so that no two vehicles get the same pseudonym and corresponding real name is only known to base station (BS).BSs maintain a table record high allows BS to identify the imposture immediately. This scheme reduces the overhead of exchanging of keys between communicating entities. And this all happens when a vehicles enters in the vicinity of the BS.

In [9], the security solution depends upon the location information and corresponding time. In this a mobility pattern is used which can detect the misbehaving nodes to increase the security and privacy. Vehicles sign the message and broadcast their current location. Every node creates a packet consist of their public key and pseudonym address and broadcast to their neighbors. Location and time id exchanged between nodes in small intervals of time. The communication paradigm among vehicles and the periodic location information is used to detect misbehavior. A vehicle is represented by series of locations in its trajectory. If random locations are received, this behavior is considered abnormal. In order to protect vehicles privacy, nodes communicate using their dynamic locations since vehicles are assumed to be equipped with positioning systems (GPS). A Location Anonymous Message (LAM) is used by the vehicle to broadcast the signed information to its neighbor nodes. The mobility pattern helps predicting some possible attacks. For example, if a node claims its presence in different locations in a short period of time, this information could be used to detect possible attacks such as Sybil attack.

In [10], Authors discuss a protocol for Authentication with Multiple Levels of Anonymity (AMLA).There is a Security Service Provider (SSP).Basically this server provides the private key to every vehicle connected to it. Whenever a vehicle wants to communicate with the neighboring vehicle and enters in VANETs they require pseudonym and desired life span of that pseudonym. Each vehicle has a tamper proof device storing the keys which are accessible to SSP. To ensure authenticity of messages, AMLA uses the identity based Encryption (IBE) and signature mechanism. A vehicle transmits messages signed with its private key corresponding to one of its pseudonyms, so its identity remains hidden. The private key of a vehicle is a function of its pseudonym. When the neighboring nodes receive the message, they use the public key of the sender and the public key of the SSP.

In [11], Authors discussed about a secure position based routing protocol. Here they applied security mechanism to GPSR (Greedy Perimeter Stateless Routing).In this nodes itself tries to estimate the malicious behavior of other nodes. The security solution has basically two mechanisms: Routing message protection mechanism and node evaluation message. For the protection of routing data, a signature verified scheme is employed to achieve end-to-end authentication and integrity. A signature field is added to the routing packet. For node evaluation, every node is turned in a hybrid mode to check all the messages sent by its neighbors. The reliability of a node is estimated according to its forwarding ratio. The evaluation mechanism used comprises forward evaluation and backward evaluation. Forward evaluation algorithm aims to find out the drop malicious nodes. In the forward evaluation, a sender assesses the receiver to know if it has relayed the packet. The backward evaluation algorithm is used to find out the tamper malicious node. When a node sends a packet to a neighbor node, the later one assesses the source of the received packet. In backward evaluation, the integrity of the packet is verified using the digital signature. an evaluation value is calculated using forward and backward evaluation values. Then, the calculated value is compared to the threshold one in order to decide if the corresponding node can be selected as a next hope.

Above we have discussed some of security issues and there different proposed solutions. But now also there are certain areas which require further research and development. Those are discussed below as research challenges.

V. RESEARCH CHALLENGES IN VANETS

In this section we discuss some of VANETs related research challenges that still need further research and innovative solutions to improve VANET services. The efficient security support is an important requirement of VANETs. Several VANET security challenges still need to be addressed in the areas of authenticity, driver confidentiality, and availability.

- We need lightweight, scalable authentication frameworks that are capable of protecting vehicular nodes from inside and/or outside attackers infiltrating the network using a false identity, identifying attacks that suppress, fabricate, alter or replay legitimate messages, revealing spoofed GPS signals, and prevent the introduction of misinformation into the vehicular network.
- As far as driver confidentiality is concerned, we need reliable and robust secure protocols that can protect message exchanges among nodes of a vehicular network from threats such as unauthorized collection of messages through eavesdropping or location information (through broadcast messages). Secure, efficient message exchange and authentication schemes operating for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications are required.
- The mechanisms that can perform fast authentications between vehicles and roadside infrastructure units are needed to avoid delays.
- Broadcasting continues to be a strong research area of focus by VANET researchers because a significant number of messages transmitted in VANETs are broadcast messages. Novel broadcasting algorithms are required to minimize broadcast storms that arise as a result of packet flooding. Providing reliable broadcast messages with minimal overheads for VANETs introduces several other technical challenges including: the selection of the next forwarding node, the maintenance of communications among vehicles as they leave and join a group, hidden terminal problems since broadcast messages do not use the typical Request to Sender/Clear to Sender (RTS/CTS) message exchange employed by IEEE 802.11.

VI. CONCULSION

The safety of people is main concern on roads thus security is main issues in VANETs. There are many projects that have been undertaken to improve vehicle to vehicle communication and also for vehicle to infrastructure communication. We have undergone some of the main research areas that have focused on security issues of VANETs. In this paper we surveyed the different attacks on VANETs and security issues that influence the VANETs. The architecture of VANETs and communication model that is used to share information between vehicles is also discussed. After surveying the literature we found some solutions to some of the present issues in security of vehicular ad hoc networks. In this work, we reviewed some of the main areas that researchers have focused on in the last few years and these include security and we highlighted the most silent results achieved to date. The security of road information of every other vehicle is very crucial. Various types of research challenges are studied with respect to vehicular communication. In particular, this paper presented a review of VANET architecture and concerned security issues. In future work we would like to propose an algorithm that would enhance the security in VANETs with less overhead and lightweight scalable framework.

VII. REFERENCES

[1]. Felipe Domingos da Cunha, Azzedine Boukerche, Leandro Villas, Aline Carneiro Viana, Antonio A. F. Loureiro “Data Communication in VANETs: A Survey, Challenges and Applications” HAL Id: hal-00981126 https://hal.inria.fr/hal-00981126v4Submitted on 15 Sep 2015.

[2]. http://deity.gov.in/content/intelligent-transportation-system-its.

[3]. Baraa T. Sharef, Raed A. Alsaqour Mahamod Ismail, Vehicular communication adhoc routing protocols: A Survey, Journal of Network and Computer Applications40(2014)363–396.

[4]. Sasha Dekleva, J.P. Shim, Upkar Varshney, and Geoffrey Knoerzer “Evolution and emerging issues in mobile wireless networks”, ACM Communications Vol. 50, No. 6, June 2007.

[5]. Raya M, Papadimitratos P, Hubaux J P (2006) Securing Vehicular Networks. J IEEE wirelcommun

[6]. Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin, Security and Privacy Enhancement in VANETs using Mobility Pattern, 978-1-4673-5990-0/13,ICUFN, IEEE 2013.

[7]. Yi Qian, Kejie Lu, and Nader Moayeri, A secure VANET MAC protocol for DSRC applications, "GLOBECOM" proceedings, IEEE 2008.

[8]. Lingyun Zhu, Chen Chen, Xin Wang, Azman Osman Lim, SMSS: Symmetric-Masquerade Security Scheme for VANETs, 2011 Tenth International Symposium on Autonomous

Decentralized Systems, 978-0-7695-4349-9/11, IEEE 2011

[9]. Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin, Security and Privacy Enhancement in VANETs using Mobility Pattern, 978-1-4673-5990-0/13,ICUFN, IEEE 2013.

[10]. Bharadiya Bhavesh N, Soumyadev Maity and R. C. Hansdah, A Protocol for Authentication with Multiple Levels of Anonymity (AMLA) in VANETs, 27th International Conference on Advanced Information Networking and Applications Workshops, 978-0-7695-4952-1/13, IEEE 2013.

[11]. Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin, Security and Privacy Enhancement in VANETs using Mobility Pattern, 978-1-4673-5990-0/13,ICUFN, IEEE 2013.

[12]. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. (2005, Jan).Network mobility basic support protocol.RFC Standard 3963. Available: http://www.ietf.org/rfc/rfc3963.txt

[13]. L. Armstrong, "Dedicated Short Range Communications (DSRC) at 5.9 GHZ,Presentation, http://www.leearmstrong.com/DSRC%20Home/Standards%20Programs/North%20American/DSRC%20Summary.ppt.

[14]. Ant Ãsnio Fonseca and Teresa VazÃco. Applicability of position-based routing for vanet inhighways and urban environment. Journal of Network and Computer Applications, 36(3):961–973, 2013.

[15]. Marios D. Dikaiakosand SaifIqbal and Tamer Nadeemand LiviuIftode. Vitp: An information transfer protocol for vehicular computing. In Proceedings of the 2nd ACM InternationalWorkshop on Vehicular Ad Hoc Networks (VANET'05), pages 30–39, 2005.