Security Threats in VANETS: A Review

Vipin Malik[1], Savita Bishnoi[2]

[1]M.Tech Scholar, Rohtak Institute of Engg. & Management
[2]Assistant Prof, Rohtak Institute of Engg. & Management.

***Abstract*—A subset of MANETS (Mobile ad hoc network) is VANETS (Vehicular network) and both are self-organized network but in VANET, node is a vehicle and is mobile. Vehicular network got attention of industries and researchers as it could be a life saver or decrease the number of accidents on road. The methodology used by VANET for ensuring safety of people is through exchange of warning messages between vehicles. VANET is also used in non-safety applications like toll collection, location of nearest hotel, using e-services while driving etc. Safety messages are sent over control channel. This channel can be used by anyone in the network and has the higher priority over other channels. More no. of attackers in the network causes more harm.**

Risk assessment is a crucial element which helps in accessing the risk a threat could pose to the assets of the system. Risks in VANETS will help in determining the impact of an attack. In the work the attack which have higher risks are modeled. The attacks use the concept of forge messages that are flooded on the network and delay generated in the network. The attacks are performed by more than one attacker. The impact of the attacks on the network performance is measured on the parameters of throughput, congestion, delay. This paper discuss the various security threats to VANETs.

***Keywords*— VANETs, DOS attack, MAC layer.**

I. Introduction

The inset of wireless has tremendously grown up, the fascination for mobility, accessibility and flexibility makes wireless technologies the dominant method for transferring all sorts of information.

Satellite televisions, cellular phones and wireless Internet are well-known applications of wireless technologies. This work proposes a promising wireless application and offers a small contribution to research community.

Wireless research field is growing faster than any other one. It serves a wide range of applications of different technologies and every one of which comes with some new specialized protocols. In the research, an introduction to a wireless technology that is now adopted by both government and manufacturers in past few years is discussed. The usage of wireless technology can directly affect and lead to decrease in number of car accidents (which is the first cause of death in the age group 1 - 44 years [1]) and increase the sales in automobile markets. Eventually research will help to build a technology for creating a robust network between mobile vehicles; i.e. an environment where vehicles can talk to each other. The technology is called as Vehicular Ad-Hoc Networks (VANET).

The aim of this paper is to familiarize with VANET as well as model novel attacks on VANET.

II. What is VANET?

VANETS stands for Vehicular Ad Hoc Network. It is a subset of MANET (Mobile Ad Hoc Network) which is highly dynamic in nature. In VANETS there is a communication between moving vehicles which is also referred as Inter Vehicle Communication (IVC) [2]. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range.

Both in MANET and VANET nodes are self-organized and self-managed & information is in distributed manner. In VANETS client server relationship does not exist. But VANET differs from MANET in many aspects like high dynamic nature, frequent disconnectivity, pattern mobility, unlimited battery, on board sensor [3].

2.1 Securing Vehicular Communication

In [6], the problem with vehicular communication is delivery of messages safely & timely, so security threat & security architecture should be known. Some open problems are also addressed. Vulnerabilities of VC like jamming, forgery, impersonation, on-board tampering are discussed along with the challenges like network volatility, delay sensitivity, heterogeneity etc .Which hardware is to be used for securing vehicle and the authorities that are involved for the authentication of vehicle are discussed. This paper rendered our knowledge base that we could have more security in VANETS and even appropriately took into account parameters like high speed, irregular connectivity, geographic location, privacy etc. These challenges can be met if all the parties (vehicle manufacturer, transportation authorities, law enforcement agencies, insurance companies and academic researchers) work together to generate new solutions.

2.2 DOS attack at MAC layer in wireless Ad hoc Network

Author discussed DOS attack in paper [7]. DOS attack can take place at routing layer and MAC layer. Attack at routing layer disrupts just routing functionality but attacks at MAC layer disrupt channel access which may result in wastage of bandwidth and power that causes low throughput and latency of network. In wired network DOS at MAC is discussed but research in ad hoc is not yet explored. FAIR MAC protocol emulates the IEEE 802.11 MAC protocol. GLOMOSIM is used for the simulation. For the simulation 12×12 grid is taken which has 144 nodes separated by 350m each. Transmission range of each node is taken as 376m. Four attacks are considered and their effect on the throughput is compared. Four attacks are as follows 1-hop neighbor attack, 2-hop neighbor attack, nodes attack on the server even if they are not neighbors to each other, and Dos attack to separate network into two parts. In MAC protocol media can be captured by a single node but not in case of Fair MAC. Unidirectional, bidirectional, high and low packet rates are some parameters on which comparisons are hold. In the previous work capture effect was highlighted. Heavily loaded node continuously sent the data which made light loaded node to back off again. But in this author considers a Fair MAC protocol. Simulations states that Fair MAC is necessary to prevent capture attack but not sufficient. If the attacking node tampers the MAC protocol then there is no countermeasure for it. Authentication should be done more precisely so that two nodes never collude.

2.3 Classes of Attacks in VANETS

In [8], author discussed usage of VANETS to ensure safety of human life on roads. If any wrong message is delivered then it may result to mishaps. Proposed model classified five classes of attacks and each class attack has its threat level and priority. Even some new attacks are proposed in some of these classes. The solution given in this paper identifies the attack and its class to which it belongs. Different types of attacks are carried in different time slots as per attacker's behavior. In previous work attacker model was described which was fixed but attack can be changed with the behavior of the attacker. Attacks can be identified but to detection of the behavior of attacker is quite difficult. So a system can be developed that makes use of current attacks and access those attacks that could be generated in future.

2.4 DOS Attack and Its Possible Solutions in VANETS

In [9], different DOS attacks are discussed and a solution is proposed. VANET is a part of wireless, thus network availability is an important issue. If availability gets compromised then safety messages would not reach on time. When a message is received by the OBU it has 4 options to decide on handling of DOS attack i.e. channel switching, technology switching, FHSS, multi radio transceivers. After the detection, processing is done and the message is send to next respective OBU. The level of threat is analyzed on the basis of different attacks and their solutions. DOS and DDOS are the attacks which are at the highest level in the hierarchy as after these attacks network is no more available. Attacks were known before but there was no solution to detect them. If DOS attack takes place then it results in compromising of the trust in the network. If the attacker is detected it should be removed from the network so that trust can be rebuilt.

2.5 Detection of Radio Interference Attacks in VANETS

Author of [10] focused on availability of network. The availability of the network in public, leads to explicit problems like privacy and security. DOS attack can be performed through jamming which decreases the QoS of the network. Solution proposed is based on correlation. Attacker is always dependent on the network but when it wants to jam the network then it becomes more dependent. Degree of this dependency is used to detect the jamming attack. CC (correlation coefficient) and EP (error probability) are calculated by each node. If CC>EP then the jamming is detected. Simulators like NS2 and SUMO are used. Previous work was done on the WSN, where DEEJAM protocol was implemented in which channel hopping, frame masking, packet fragmentation, redundant encoding are used to detect the jamming but the overhead of all these was very high. This protocol offers solution for constant jamming and doesn't resolve random or reactive jamming. From the proposed method jamming is detected with high degree of confidence. But in this paper only jamming is taken into account. No other DOS attacks are considered.

2.6 A Secure VANET MAC Protocol For DSRC Applications

Author of [11] proposed a secure MAC protocol for VANETs, with different message priorities for different types of applications to access DSRC channels. In previous work VANET security concentrate on particular security mechanisms and solutions on VANET communications, there are not many works on secure medium access control. The one who proposed an approach of secured MAC protocol has not considered the DSRC channel structures with the DSRC application scenarios. The proposed secure MAC protocol used part of the IEEE 1609.2 security infrastructure including PKI and ECC, the secure communication message format for VANETs, and the priority based channel access according to the QoS requirements of the applications. Author used the concept of digital signature and certificates issued by the CA. The effect of this protocol on throughput increases linearly as no. of nodes increases. For Class 1, throughput grows as no. of nodes increases but in case of lower classes it gets decreased. Delay for the class 1 was stable as no. of nodes increases.

2.7 Secure Position based Routing for VANETS

Problem addressed in [12] paper is: network layer uses multi hop routing which partitions the network and makes some nodes unaware of the safety messages. PBR protocol is considered as it is a multi hop routing. PBR has three components: beaconing, location services and forwarding. Attacks against PBR are taken from attack tree. Three mechanisms are proposed for security:

a. Digital Certificate: Provide authentication, non repudiation, integrity. In this two signatures are sent during transmission of the packet one is of the source and other is of the sender. For HBH protection forwarders sign the packet in mutable field and pass it.
b. Plausibility check: Reduces the impact of false position on the routing operation. Some predefined checks (time, acceptance range, velocity) are performed on the received packet if any of the check fails that packet is dropped.
c. Robustness mechanism: Reduces the effect of packet injection on large network. Basically rate limit mechanism is used. Emergency and RSU has high rate. If any vehicle exceeds the predefined threshold then attack is detected. Followed by implementation and testing.

Security level is achieved as Sybil attacks are prevented, message freshness is achieved. Both end to end and hop to hop authentications are taken in hybrid scheme. Implementation is done using Open SSL library, ECDSA with a key of 160 bits for nodes and 224 bits for CA. Parameters like no. of packets, latency are varied. Previous work only presents the design principles and components. Some has considered the geographic routing but that was not volatile and on small scale. More plausibility checks can be added so that more no. of threats can be detected. More analysis on security is required.

2.8 Performance Evaluation of the IEEE 802.11p WAVE Communication Standard

[13] Author provides a performance evaluation of the IEEE 802.11p WAVE, considering collision probability, throughput and delay, using simulations and analytical means. In this DSRC and WAVE standard has been discussed. An analytical approach was used that introduces packet collisions on the channel, reducing the throughput. The probability of a collision depends on the number of different contention window periods. A vehicle can switch between CCH and one SCH at a time having different queues. In a scenario with N sending nodes a collision will occur if at least two nodes select the same contention period and no other node selects a less value period. Performance evaluation was done by taking the low and high data traffic on Manhattan Grid Scenario. Messages for the CCH queue up further during the SCH intervals, resulting in longer queues and a higher end-to-end.

2.9 Establishing delay strict priorities in IEEE 802.11p WAVE vehicular networks

In [45], author proposed an effective solution for two problems. One problem was related to the use of EDCA at the MAC layer which could not establish strict priorities for high priority messages. Other problem was regarding the acknowledgement of broadcast message over the control channel. The proposed solution for the first problem was based on the AIFS value for each AC. The high priority messages has to wait for only AIFS time but the message of low priority has to wait for its AIFS as well as CWmax of the high priority message. To overcome the acknowledgment problem passive clustering was used in which cluster head sends acknowledgement for the high priority message whenever it is received correctly from any of its cluster members. Simulation was performed and it was noticed that delay, losses of critical message got reduced. But the low priority messages suffered from high delay.

2.10 CMAC: A Cluster Based MAC Protocol for VANET

Author in [14], proposed a cluster based MAC protocol that delivered the message with high reliability and low delay. IEEE 802.11p standard was developed for MAC in VANET. But, it was unable to provide an upper bound on the frequency access delay due to usage of CSMA/CA for channel access coordination. The previous protocol was not scalable and decreased the performance quickly as load and traffic density increases. So, this protocol adopts centralized approach by shifting the control and management of wireless channel to RSU. For each RSU frequency band is divided into eight fixed time slots separated by guard time. Logical channels consist of frequency bands which are divided into four bands: control band, frequency band1, frequency band2 and inter handoff band. Every safety message is send to the RSU by the vehicle through the control channel. This protocol removes the problem of hidden/exposed terminal. But, the limitation of this protocol is that it works only in the presence of RSU.

2.11 Contention Window Analysis for Beaconing in VANETs

In [15], author discussed the contention window size for the transmission of beacons in VANET. Previously, while sending beacon the load on the channel can increase rapidly as traffic density increases and 802.11 broadcast performances deteriorates as the load on the network increases. But similar to flooding and network layer broadcast, deteriorated performance at the MAC layer results in a reduced probability of successful reception and in increased delay. Author was expecting that increasing the Contention Window in reaction to an increased traffic density could improve performance. In simulation, they study the effects on Beacon Reception Probability, Delay and Beacon Inter-arrival Time and drawn the conclusion that Contention Window increase as performed in the experiments does not improve beaconing performance.

2.12 Design Secure and Application-Oriented VANET

In [17] author proposed a secure and application-oriented network design framework for VANET. Because security and different applications are the major challenges to deploy VANET successfully. They consider both security requirements of the communications and the requirements of potential VANET applications and services. The proposed framework consists of two basic components: an application-aware control framework and a unified routing scheme. Application aware control framework contains the list of available applications and their types. With the availability of information for the application, a unified routing scheme will be designed such that all the applications will be supported. Different case studies were considered to check the framework. Security management, key management and secure routing and network coding are used to design the framework. The proposed design will help to develop a more secure and practical VANET.

2.13 Increasing Broadcast Reliability in Vehicular Ad Hoc Networks

The goal of [17] paper is to develop an adaptive broadcast protocol that improves the reliability of delivering broadcast messages in a VANET. In the previous work, author proposed a single-hop broadcast protocol that increases the probability of a message's reception by sending the message multiple times. In VANET a node can't judge whether the message is delivered or not but it can estimate the network traffic by analyzing the received packets. According to the protocol, every node maintains a table which has information regarding MAC address, last sequence number, a weighted reception rate and a timestamp. CW size is increased or decreased according to the estimation of local reception rate. As a result of adaptively adjusting the CW size, the probability of a collision is reduced. Future work will focus on adaptive control of transmission power, based on observed network condition.

2.14 Dynamic Adaptation of Joint Transmission Power and Contention Window in VANET

In [18], authors proposed an algorithm for joint adaptation of transmission power and contention window to improve the performance of vehicular network in a cross layer approach. In vehicular ad hoc network, the communication between the two vehicles remains active for a short duration of time. Instead of taking fixed transmission power, the proposed algorithm takes transmission power dynamically based on estimated local traffic. This paper also includes the EDCA 802.11e to implement a priority based V2V communications. The two proposed algorithms always assign the maximum transmission range for the vehicle that carries priority 1 messages. In order to adapt to the transmission power and the contention window (transmission time) dynamically, each vehicle runs both algorithms in a periodic manner so that the proper tuning of these values occurs according to the local density of vehicles and the network conditions.

2.15 Modeling Roadside Attacker Behavior in VANETs

In this [48], modeling of attackers is done that target active safety applications. Risk analysis of assets, threats and vulnerabilities in VANET is conducted. The most severe attack is performed by roadside attacker that distribute forged message. Detail study of this attack is discussed including attacker's degree of freedom and attacks compositions. The main motive of this paper is risk analysis. If assets, threats and vulnerabilities are known then severity of an attack can easily be calculated. Characteristics of an attacker are also discussed that include its mobility, motivation, intention, co-operative nature etc. Qualitative assessment is also a good technique to determine the threat and to find attacker. Future work includes the detection of presented attack.

III. Conclusion

According to the previous papers discussed, various types of attacks, priority of messages in VANET were highlighted. A mechanism of risk analysis which uses Qualitative Assessment laid a milestone in the study. EDCA mechanism is used to prioritize messages i.e. safety related messages has higher priority. These points lead to attacks that may be possible in VANET.

IV. References

[1]. M. Heron, D. Hoyert, J. Xu, C. Scott, and B. Tejada-Vera "Deaths: Preliminary Data for 2006," Division of vital statistics, National Vital Statistics Reports, Vol.56, N.16, 2008

[2]. S.Youseif, M.S.Mousavi, M.Farthy "Vehicular Ad Hoc Network challenges and perspective" 6th International Conference on ITS Telecommunications Proceedings, 2006.

[3]. Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas, "VANET Routing Protocols: Pros and Cons", International Journal of Computer Applications (0975 – 8887) Volume 20– No.3, April 2011

[4]. "Car 2 car communication consortium." Available: www.car-2-car.org

[5]. "Statewide Plan," Department of Transportation (DOT), Intelligent Transportation Systems (ITS), September 2005

[6]. M. Raya, J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, january 2007, pp: 39-68.

[7]. Vikram Gupta, Srikanth Krishnamurthy and Michalis Faloutsos, "DOS attack at MAC layer in wireless Ad hoc Network"

[8]. Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, "Classes of Attacks in VANET"

[9]. I.Ahmed Soomro, H.B.Hasbullah,J.lb.Ab Manan,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET",WASET issue 65, april 2010 ISSN 2070-3724.

[10]. Ali Hamieh, Jalel Ben-Othman, Lynda Mokdad "Detection of Radio Interference Attacks in VANET" in the IEEE "GLOBECOM" 2009 proceedings.

[11]. Yi Qian, Kejie Lu, and Nader Moayeri, "A Secure VANET MAC Protocol For DSRC Applications". IEEE Global Telecommunications Conference (GLOBECOM) 2008.

[12]. Charles Harsch, Andreas Festag, Panos

Papadimitratos, “Secure Position-Based Routing for VANETs”, Proceedings of IEEE 66th Vehicular Technology Conference (VTC Fall), Baltimore, MD, USA, September/October 2008.

[13]. Stephan Eichler, “Performance Evaluation of the IEEE 802.11p WAVE Communication Standard”, In IEEE 66th Vehicular Technology Conference VTC-2007, pp.2199-2203, 2007.

[14]. Nemi Chandra Rathore, Shekhar Verma, Ranjeet Singh Tomar, G. S. Tomar, “CMAC: A Cluster Based MAC Protocol for VANETs”, In International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010.

[15]. Ren´e Reinders, Martijn van Eenennaam, Georgios Karagiannis and Geert Heijenk “Contention Window Analysis for Beaconing in VANETs”

[16]. Y. Qian, N. Moayeri, ”Design of Secure and Application Oriented VANETs”, IEEE Vehicular Technology Conference 2008, 11-14 May 2008, Singapore.

[17]. Nathan Balon and Jinhua Guo, “Increasing Broadcast Reliability in Vehicular Ad Hoc Networks”, VANET’06, September 29, 2006, Los Angeles, California, USA.

[18]. D. Rawat, G. Yan, D. Popescu, M. Weigle, S. Olariu, “Dynamic Adaptation of Joint Transmission Power and Contention Window in VANET”, 2009, pp. 1–5.

[19]. Hamid Menouar, Fethi Filali, and Massimiliano Lenardi. “A Survey and Qualitative Analysis of MAC Protocols for Vehicular Ad Hoc Networks”, IEEE Wireless Communications, 13(5):30_35, October 2006

[20]. Kevin C. Lee, Uichin Lee, Mario Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks," Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, IGI Global, Oct, 2009

[21]. IEEE P802.11p, “Amendment 3: wireless access in vehicular environments (WAVE),” Draft D0.26, January 2006.

[22]. Dedicated Short Range Communications (DSRC) Home, http://www.leearmstrong.com/DSRC/DSRCHomeset.htm http://grouper.ieee.org/groups/scc32/index.html

[23]. Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems – 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ASTM E2213-03, September 2003

[24]. Notice of Proposed Rulemaking and Order FCC 02-302, Federal Communications Commission, November 2002.

[25]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Std. 802.11e, 2005.

[26]. http://en.wikipedia.org/wiki/IEEE_802.11e-2005

[27]. C. Suthaputchakun and A. Ganz, “Priority Based Inter-Vehicle Communication in Vehicular Ad-Hoc Networks using IEEE 802.11e,” VTC2007-Spring, IEEE 65th, Pages: 2595-2599, Year: Apr. 2007

[28]. Managing DSRC and WAVE Standards Operations in a V2V Scenario by Hindawi Publishing Corporation International Journal of Vehicular Technology Volume 2010, Article ID 797405, 18 pages doi:10.1155/2010/797405

[29]. IEEE P1609.1, “Trial-use standard for wireless access in vehicular environments (WAVE) - resource manager,” Draft D17, July 2006.

[30]. IEEE P1609.2, “Trial-use standard for wireless access in vehicular environments (WAVE) - security services for applications and management messages,” Draft D7, April 2006.

[31]. IEEE P1609.3, “Trial-use standard for wireless access in vehicular environments (WAVE) - networking services,” Draft D22, January 2007.

[32]. IEEE P1609.4, “Trial-use standard for wireless access in vehicular environments (WAVE) - multi-channel operation,” Draft D08, July 2006

[33]. Hannes Hartenstein, Kenneth P. Laberteaux “A Tutorial Survey on Vehicular Ad Hoc Network” IEEE Communication Magazine June 2008

[34]. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, ”Vehicular ad hoc networks (VANETS): status, results, and challenges”, Springer Science and Business Media, LLC 2010

[35]. “Assessment of the applicability of cooperative vehicle-highway automation systems to bus transit and intermodal freight: case study,” California Partners for Advanced Transit and Highways (PATH), 2004. http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1629&context=its/path

[36]. London Congestion Charging Technology Trials,” Transport for London, Feb 2005. http://www.tfl.gov.uk/assets/downloads/technology-trials.pdf

[37]. Katrin Sjöberg, Elisabeth Uhlemann and Erik G. Ström, “Medium Access Control in Vehicular Ad hoc Network,” IEEE VTS Workshop on Wireless Vehicular Communications Halmstad University, Sweden October 12, 2010

[38]. Al-Sakib khan Pathan, “Security of self organizing network; MANET, WSN, WMN, VANET”, Auerbach Publications, Chapter 10

[39]. Nai-Wei Lo and Hsiao-Chien Tsai, “Illusion Attack on VANET Applications - A Message Plausibility Problem”, In Globecom Workshops, 2007 IEEE, pages 1–8, 2007

[40]. Mahmoud Al-Qutayri, Chan Yeun and Faisal Al-Hawi, ”Security and Privacy of Intelligent VANETs”, InTechOpen book, published on: 2010-02-01

[41]. Saleh Yousefi; Mahmoud Siadat Mousavi; Mahmood Fathy; "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives," Proceedings of the 6th international conference on ITS Telecommunications (ITST2006), pp. 761-766, China, June 2006

[42]. http://www.mathworks.in/products/matlab/

[43]. Intelligent Transportation using VANET in PCQuest, Mainak Ghosh & Sumit Goswami, IIT, Kharagpur, February 01, 2009

[44]. Paulos, John Allen. The Mathematics of Changing Your Mind, New York Times (US). August 5, 2011; retrieved 2011-08-06

[45]. Frank A. Haight (1967). Handbook of the Poisson Distribution. New York: John Wiley & Sons.

[46]. Mohssin Barradi, Abdelhakim S. Hafid, Jose R. Gallardo, "Establishing strict priorities in IEEE 802.11p WAVE vehicular networks" IEEE Globecom 2010 proceedings.

[47]. ^ "CAN History". CAN in Automation

[48]. Tim Leinm¨uller, Robert K. Schmidt, Elmar Schoch, Albert Held_ and G'unter Sch'afer, "Modeling Roadside Attacker Behavior in VANET".