ISSN 2349-0292
Impact Factor 3.802

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

A REVIEW ON SECURITY ISSUES AND THEIR SOLUTION IN VANETS

A. Israr*, M. Ashraf
* Department of Electrical & Electronics Engineering, University of Engineering & Technology Peshawar, Pakistan

DOI: 10.5281/zenodo.1456385

ABSTRACT

Vehicular Adhoc Networks are of major interest of researchers nowadays. Despite of the huge attention of the researchers towards VANETs, there are still many issues regarding security of VANETs. Researchers are still going to secure the VANETS from different types of attacks and adversaries. There is a strong link between reliable network and security and privacy features. This paper provides a survey of problems in wireless networks like jamming attacks and their impact on the network. Many security issues are analyzed and have been discussed. Many researches about the solutions of the security attacks to the wireless networks have also been sum up in this paper.

KEYWORDS: Vehicular Adhoc Networks, Security issues, jamming attacks.

INTRODUCTION

Because of increase in the number of vehicles on the roads, the traffic accidents are also increasing. According to a report by National Highway Traffic Safety Administration more than 30 thousand of accidents happened in 2012 in which drivers, passengers and other road users were affected. This number is increasing as there is direct relationship between the traffic and the fatalities. To avoid the fatalities, the vehicles and the roads should be made safer.

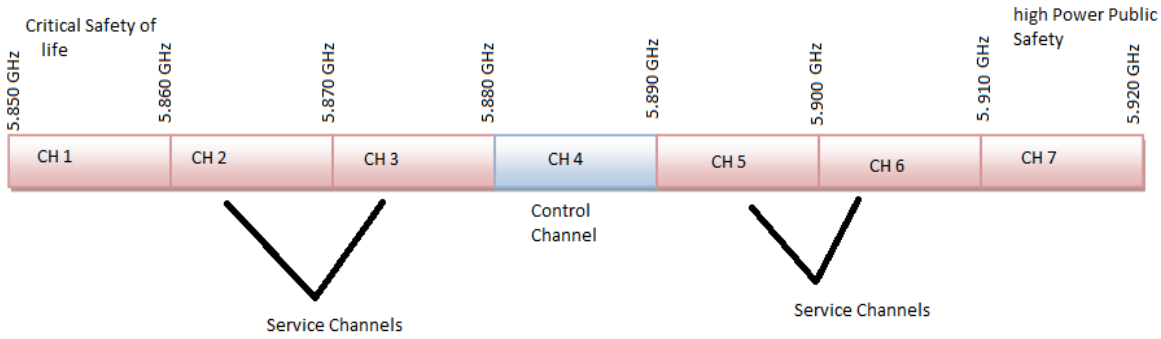
To achieve this goal, the very first step which is taken is to make the vehicles safer by embedding and installing computers in the vehicles. These computers help the drivers to diagnose the problems occurring in the internal systems of the cars. Chevrolet was the first company to install computers in the cars in 1975. After that many other cars started adopting the same technique. Computers which are being installed in the cars are composed of Electronic Control Units (ECU). It has different modules which controls the electrical systems of the cars. Modules are like engine control module, transmission control module, and brake control module [1] [2]. Quality of driving's safety is increased as a result of installing ECU in cars. But these ECUs address only the internal problems occurring to the car. The external problems like road scenarios, hazards, weather behavior and traffic blocks on the roads are some of the factors that also need to be addressed for the safety of the drivers.

To make the cars able to gain information about the external hazards the Intelligent Transport System (ITS) is the first step. ITS is the national program which uses modern computers for the purpose of communication so that vehicles are communicated about the external hazards or scenarios of the road. Automatic Toll Collection, Traveler Information System, Intelligent Traffic Control are some of the examples of the ITS [3]. The main purpose of ITS is to embed such hardware in very car so that each car is capable of communicating to other cars (Vehicle to Vehicle "V2V") and to the fixed infrastructure units installed on the road sides which are termed as Road Side Units (RSUs) which is called Vehicle to Infrastructure (V2I) communication. V2V and V2I is collectively called as VANETs. For the purpose of communication VANETs a bandwidth of 75MHz is allocated in the spectrum of 5.9GHz which is called as Dedicated Short Range Communication (DSRC) [4]. DSRC is based upon two points:

1. Safety of the connected vehicles is of top priority.
2. DSRC is the only available technology that offers latency, accuracy, and reliability required for the safety of the connected vehicles of the network [3].

n DSRC the 75 MHz of bandwidth is divided into 7 sub channels of 10 MHz each. Out of which one channel is called the Control Channel CCH which is used for the safety related information and the rest are Service Channels SCH which are used for the broadcasting of service related information like entertainment etc. The following figure shows the pictorial view of DSRC band and its sub channels.

Figure 1:



DSRC Spectrum Band & Its Channels

As VANETs are wireless in nature, these networks also faces many issues regarding their security because of which safety of drivers come at stack. If safety is kept at priority by the researchers then the Quality of Service (QoS) is compromised because both the security and QoS are inversely related to each other. So the main goal of the researchers is to balance between the security of the network and QoS.

There are different types of attacks which can affect the security of the network which can be categorized in terms of authentication, availability and non-repudiation [5]. Authenticity and Non-repudiation are also important but the availability of the network is most important to assure the security of the network. One of the main threats to availability is jamming attack. This type of attack is easy to launch but hard to detect.

Jamming attack targets the availability of the network in VANETs, because jamming blocks the regulation of informative messages between the nodes of the network. Imagine for a second that an accident is happended on the road and a vehicle broadcast a message to the cars heading towards that direction about the mishap, if that message is blocked, what will be the devastating results of that? So jamming is a major problem in VANETs.

This paper addresses the security issues of the VANETs and also summarizes the solutions which are proposed by different researchers.

SECURITY CHALLENGES IN VANETS

Although security is of great importance in VANETs but it is not taken in consideration to that level by the researchers. Vehicles in VANETs broadcast the informative packets which contains important information. Now these packets need to be delivered to their destination without any alteration. For this delivery of the packets from the source to the destination, the security of the VANETs must be kept in consideration while designing the architecture of the VANETs [5]. This section gives the security requirements that need to be satisfied before the deployment of such networks.

1. Availability: availability means that the network should always be available to the nodes whenever the nodes want to access the network for the transmission of some important messages. Denial of Services (DoS) attack is the main threat to the availability.
2. Confidentiality: Confidentiality means that the privacy of the nodes constituting the network should be kept secret so that the un-authorized nodes cannot effect the information shared by the authorized nodes of the network. Eavesdropping is an attack which can effect the confidentiality.
3. Identification & Authentication: The purpose of this requirement is to ensure that the nodes and the messages of the network are legitimate. This requirement can be effected by the Impersonation and Sybil Attack.

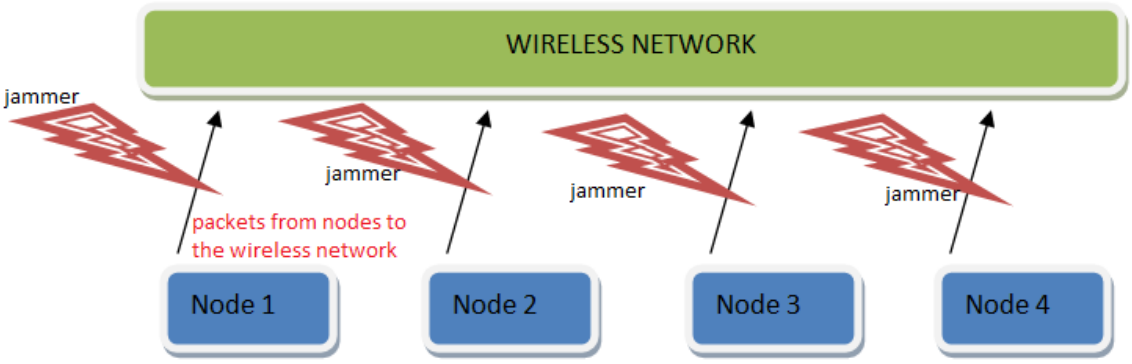
By studying the above requirement we concluded that security in VANETs is of great importance. But to secure network from all types of attacks and to fulfill all the above requirements is a very difficult task in itself. But the main problem which is of top concern nowadays by researchers is availability of the network.

JAMMING PROBLEM

In jamming attacks the adversary launches the noise signals upon the frequency on which the nodes of the network are communicating. These noise signals get interfered with the original signals and thus decreases there Signal to Noise Ratio (SNR). So the receiver of the signal will not be able to extract the useful information from the signal. Jamming attacks are classified into 4 different types depending upon their nature.

Constant Jamming: In this type of jamming continuous jamming signals are transmitted by the jammer without analyzing the state of the channel. **Deceptive Jamming:** in this a stream of random bits is injected to the channel without having any gap between the packets. **Random Jamming:** In this time of jamming the adversary alters itself between sleeping and jamming mode for the purpose of saving energy. **Reactive Jamming:** This is the most difficult attack to be detected. In this attack the attacker only launches the jamming signals when it senses any activity upon the network. Figure 2 gives the pictorial view to understand the concept of jamming.

Figure 2:



Interfering with the Data Packets sent by the Nodes to the Wireless Networks

SOLUTIONS OF THE JAMMINNG PROBLEM

Author of [6] explained the need of network's availability for the purpose of assuring security. The author addressed the Denial of Services attack and also proposed a solution for that. DoS attack is divided into 3 categories by the author. 1). Basic Level 2) Extended Level 3) Distributed Denial of Services DDoS attack. Author proposed a solution that vehicles and drivers should depend upon On Board Units (OBUs) which are installed in each vehicle. OBU is made capable of decision making to avoid DoS attack. Techniques like Channel Switching, technology switching and frequency hopping are proposed for that. In [7] the author proposed a technique for the detection of jamming inn wireless networks. Detection technique uses the Correlation Coefficient (CC). CC is the statistical measure between the 2 variables whose values lies in between -1 and 1. Each node of the network compares 2 values CC and Error Probability (EP). If the value of EP is less than that of CC then it is considered as jamming. The author of [8] the issues related to security of VANETs and proposed a technique for avoiding jamming. Author proposed a technique called Hideaway technique which depends upon Packet Send Ration (PSR) for the determination of the network that whether it is jammed or not.

R. Raw et al [9] addressed the security challenges and the significant requirement for the security of VANETs. Various attacks along with their possible solutions were discussed. Author concluded that the confidentiality is not required at all in VANETs. According to author the messages in the VANETs do not contain any confidential data. A table is provided for measuring different attacks, security requirements, technology and solutions used for the defense. In [10] the jamming attack is studied in detail by the author and is classified into Active and Reactive categories. Author concluded that the reactive type of attack is much difficult to detect than active one. Author of [11] proposed a hybrid routing protocol model for the security of VANETs. The proposed protocol is termed as Position Based Secure routing Protocol (PBSRP) which is a hybrid of Most forward within Radius (MFR) and Border Node based (B-MFR) routing protocols. RSU and RSU key agreement protocols are integrated with a security module for the provision of defense against active and passive types of attacks. In [12] the effects of DoS attack are minimized by the Multi Packet Transmission and Multi Packet Reception. A routing protocol called

Road Based Routing Vehicles in VANETs (RBVT) for the better routing of the vehicles in VANETs. The protocol uses real time traffic information for the creation of road based paths. Two sub protocols are also proposed by the author named as RBVT-R and RBVT-P to work as reactive or proactive protocols. Network on Wheels (NoW) project is the German research project which is described by the [13]. The project was done in collaboration with the car manufacturers, suppliers, researchers and educational institutes. A system was developed in this project which unifies safety and infotainment. The main contribution of that project was the development of CAR-X communication where X can be another car or the RSU. Provision of safety, networking, radio, privacy and security is the main goal of this project. The author of [14] describes the advantages and disadvantages of different routing protocols which are being used for VANETs. Author divided the routing protocols into 5 different categories:

1. Topology Based
2. Position Based
3. Cluster Based
4. Broadcast Based
5. Geocast Routing Protocol

The following table is taken from the paper for the purpose of illustration.

Table 1. Different Routing Protocols and Their Comparison

Protocol	**Proactive**	**Reactive**	**Position Based**	**Delay Bounded**	**Cluster Based**	**Broadcast**	**Geocast**
Prior Forwarding Method	**Wireless Multihop Forwarding**	**Wireless multihop Forwarding**	**Heuristic Method**	**Carry and Forward**	**Wireless multihop Forwarding**	**Wireless multihop Forwarding**	**Wireless multihop Forwarding**
Digital Map requirement	**NO**	**NO**	**NO**	**NO**	**YES**	**NO**	**NO**
Virtual Infrastructure Requirement	**NO**	**NO**	**NO**	**NO**	**YES**	**NO**	**NO**
Realistic Traffic Flow	**YES**	**YES**	**YES**	**NO**	**NO**	**YES**	**YES**
Recovery Strategy	**Multihop Forwarding**	**Carry & forward**	**Carry & Forward**	**Multihop forwarding**	**Carry and forward**	**Carry and forward**	**Flooding**
Scenario	**urban**	**urban**	**urban**	**sparse**	**urban**	**highway**	**highway**

The paper of [14] presented a technique for encountering the jamming attack. According to the author the effects of jamming upon the source and receiver are not isotropic. Author suggested that when jamming attack is detected the transmission power of the original signal should be adjusted so that SNR could be improved.

CONCLUSION

Jamming attack is considered as serious threat to the wireless networks by the Federal Communication Commission and is termed as criminal offense. Hence jamming is an illegal thing to do. Our paper studies different jamming attacks which are addressed by the authors in the previous years and also gives a detailed survey about the proposed solutions of that. This paper is the base of the study for our future work which will be in the field of Detection and Minimization of jamming attacks in Vehicular Adhoc Networks.

ACKNOWLEDGEMENTS

I would like to thank UET Peshawar Pakistan which helped me a lot during my studies and also to my supervisor M.Ashraf.

REFERENCES

[1] Engine Control Unit, Working of ECU, http://en.wikipedia.org/wiki/Engine_control_unit.
[2] "Electronic control unit", Wikipedia: The Free Encyclopedia. Wikipedia Foundation, Inc. September 2014. Web, http://en.wikipedia.org/wiki/Electronic_control_unit.
[3] U.S. Department of Transportation, Intelligent Transportation Systems (ITS) Home, http://www.its.dot.gov/index.htm.
[4] Y Qian, K Lu, and N Moayeri, "A Secure VANET MAC Protocol for DSRC Applications", IEEE Globecom, 2008.
[5] R Raw, M Kumar, and N Singh, "Security Challenges, Issues and Their Solutions for VANET", Vol.5, pp95-105, IJNSA 2013.
[6] H. Hasbullah, I. Soomro, and J. Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", World Academy of Science, Engineering and Technology, 2010
[7] A. Hamieh, J. Othman, and L. Mokdad, "Detection of Radio Interference Attacks in VANET", IEEE, 2009.
[8] I. Azogu, M. Ferreira, J. Larcom, and H. Liu, "A New Anti-Jamming Strategy for VANET", Globecom 2013 Workshop, IEEE, 2013.
[9] R Raw, M Kumar, and N Singh, "Security Challenges, Issues and Their Solutions for VANET", Vol.5, pp95-105, IJNSA 2013.
[10] S. Babar, N. Prasad, and R. Prasad, "Jamming Attack: Behavioral Modeling and Analysis", IEEE, 2013.
[11] S. Bhoi, and P. Khilar, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International conference on Communication and Signal Processing 2013, IEEE, 2013.
[12] J Nzouonta, N Rajgure, G Wang, and C Borcea, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information", Vol. 58, pp3609-3626, IEEE, September 2009.
[13] A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch,"NoW – Network on Wheels': Project Objectives, Technology and Achievements", International Workshop on Intelligent Transportation (WIT), 2008.
[14] W. Xu, "On adjusting power to defend wireless networks from jamming," in Proceedings of the 1st Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems, pp. 1–6, 2007.