I J C T A, 9(6), 2016, pp. 2873-2880 ISSN: 0974-5572

Survey: Detection and Solutions of Jamming Attacks in Vanet

G.B. Santhi* and D. Sheela**

ABSTRACT

Vehicular Ad hoc Networks (VANET) is an emerging technology which attracted a lot of attention in recent years. VANETs are used for improving road safety and to provide variety of value added services. There are some security issues and attacks associated with the VANET due to its dynamic changing topology. This paper focuses on the detection of jamming attack and providing solution to this attack and enhances the security. Jamming attacks occur by transmitting continuous radio waves to inhibit the transmission among sender and receiver. In this paper, various detection methods of jamming attacks in VANET are analyzed and solutions are proposed.

Keywords: VANET, V2V, V2I, ECU, ECM, attacks

1. INTRODUCTION

VANET is a network in which nodes are vehicles. These vehicles can communicate in multi hop fashion with each other on the road. VANET applications have been widely classified into safety applications and Non-safety applications. Safety applications are very useful to users and their lives. Non safety applications are comfortable for drivers and passengers. In today's view the abrupt volume of road traffic affects the safety and effectiveness of the traffic environment. Millions of people die around the world every year in road accidents. VANET is a self configuring system in which vehicles are nodes [5].

VANET consists of a number of On-Board Units (OBU) which is located inside the vehicles and a number of Road-Side units (RSU).VANET is shown in Fig-1.The Communication in VANET is divided in to two:

- Vehicle-to-Vehicle (V2V) Communication, where nearby vehicles will share traffic information and road conditions to one another.
- Vehicle-to-Infrastructure (V2I) Communication, where Vehicles communicate their accumulated information to the nearest RSU in order to distribute the information faster and more effectively.

Combining cars with computers was the first step toward minimizing victim. Equipping vehicles with computers to monitor and control car's constituents helps drivers to recognize problems in their cars, e.g., engine failures and improve safety by providing an early warning of cars impairment. Computers in cars first appeared by Chevrolet in 1975. Soon after that, many car manufacturers started adopting the technology and integrated new systems to vehicles. This allowed standardization of systems such as Electronic Control Unit (ECU). ECU consists of different modules that control different electrical systems or subsystems in motor vehicles: engine control module (ECM) and Transmission Control Module. Combining cars with computers was the first step toward minimizing fatalities.

Equipping vehicles with computers to monitor and control car's components helps drivers to discover problems in their cars like engine failures and improve safety by giving an early warning of car malfunction.

* Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, *Email: santhi.bhavani@gmail.com*

** Department of Electronics and Communication Engineering, Tagore Engineering College, *Email: sheela_rajesh@rediffmail.com*

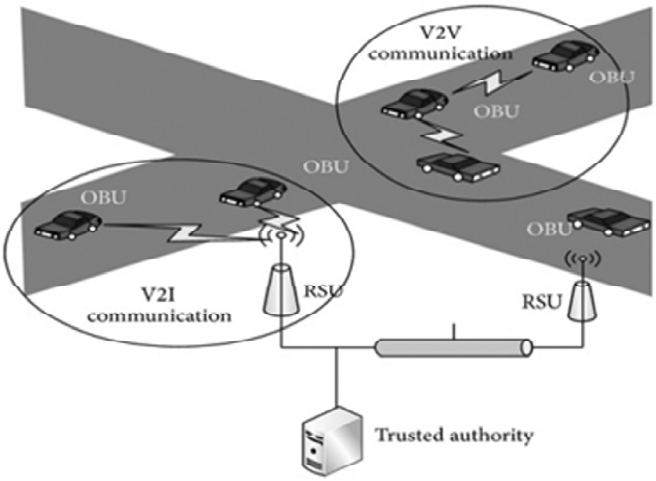

Figure 1: Vehicular Ad-hoc Network

ECU consists of different modules that control different electrical systems or subsystems in motor vehicles: engine control module (ECM), Transmission Control Module, Brake Control Module, is systems referred at as car's computer [6] [14]. While placing ECU in cars upgrades the quality and safety of driving, it only helps drivers to identify car's internal impairment since ECU can only provide information with regard to different car components. ECU cannot report external hazards that are vital to take into counts; road hazards, weather changes, and accidents on roads are only some examples of external factors that affect drivers' safety.

The Research and Innovative Technology Administration (RITA) has acknowledged the need to make use of technology for safety purposes. Hence it allotted 75 MHz in the 5.9 GHz frequency band grand a license to Dedicated Short-Range Communication (DSRC)[24].

The U.S. Department of Transportation commitment to DSRC highlights two critical points: (1) Safety is the highest priority and is the focal point for the connected vehicle technologies. (2) The analysis illustrates that DSRC is the only convenient technology in the short-term that offers the latency, accuracy, and reliability needed for active safety. Thus many organizations and manufacturers started advocating VANET by investing on perfecting it.

The routing protocols in VANET are categorized into three major categories:

a. Proactive Routing Protocol: In proactive routing protocol, the mobile nodes transfer routing information and to keep the network topology information in routing table at periodic interval of time. These protocols are also known as table driven routing protocol.

b. Reactive Routing Protocol: Here the mobile nodes do not transfer routing information at regular interval of time. These protocols get a new path when it is desired. These protocols are also known as On Demand Routing protocol.

c. Hybrid Routing Protocol: It is the combination of both proactive and reactive routing protocols. A table driven mechanism is applied inside the routing zone of each node while an on demand mechanism is applied for the nodes that are not inside the routing zone.

2. JAMMING ATTACK

Jamming attack purposely transmits radio signals to distort the whole communications by decreasing the signal to noise ratio. In VANET, jamming is a serious threat to its security. Jamming attack scenario is shown in Fig-2. Jammers constantly send repeated signals to interfere with the communication between

nodes in the network. The wounded person feels that the state of the channel is still busy. The objective of a jammer is to interfere with legitimate wireless communications, and to degrade the overall QoS(Quality of Service) of the network. To detect a particular class of jamming attack, the jammer sends only when valid radio activity is signaled from its radio hardware. This detection model is based upon the measurement of error distribution [11]. Therefore Jamming attack can be classified into four different types based on its behavior; Constant, Deceptive, Random and Reactive jamming.[4]

a) Constant jamming sends random generated data on the channel without checking the state of the channel (Idle or not).

b) The Deceptive jammer introduces a stream of random data constantly without keeping gap between successive packets transmission.

c) Random jamming differs between jamming and sleeping mode to safeguard energy.

d) Reactive jamming jams only when it understands activity on the channel otherwise it stays idle. While all jamming attacks can harm the network performance equally, the main distinction is the detection difficulty.

2.1. Challenges

Due to the high mobility of VANET and the quick change of its topology, defending VANET against jammers has been a solid problem [3]. Jammers need not observe any protocols and their mobility is not limited. A jammer can be standing on base or driving randomly down the roads. Moreover, adversaries have full control of when to start jamming and when to go into a sleep mode to conceal its existence. All these reasons have made jamming problem a challenge to solve and detect.

3. SECURITY REQUIREMENTS

In order to give a secure and dependable vehicular network, a number of security requirements must be considered [25][13]. A secure VANET system should satisfy following requirements.

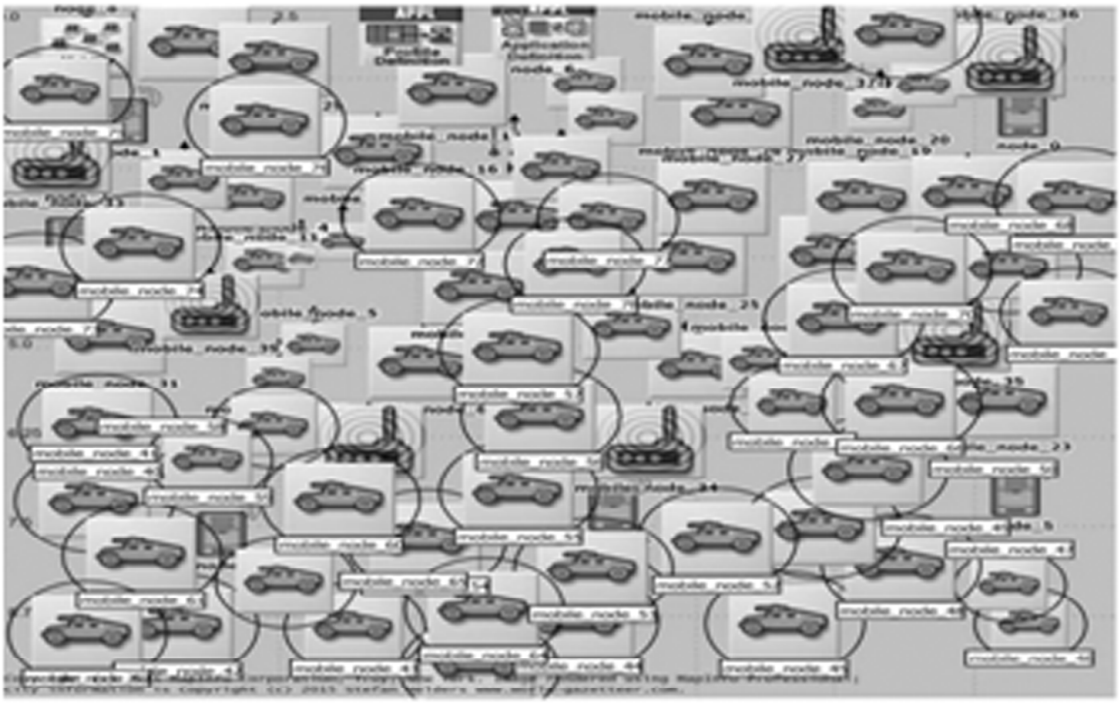

Figure 2: Jamming Attack scenario

3.1. Authentication

Despite the lack of need for confidentiality, network nodes must be authenticated. It is to be able to send messages through the network. Before reacting to messages and events a vehicle must verify the legitimacy of the messages and its sender, therefore there is a need for authentication. Without authentication, legitimate and malicious users can include false messages into the network and confuse other vehicles by give out false information. With authentication, vehicles can simply drop messages from unauthenticated users.

3.2. Availability

Availability requires all services that the network offers to be available when needed by legitimate users. One harmful attack is DOS(Denial of Service).

3.3. Integrity

Assurance of integrity means secure communication. Real information must not be altered during communication. It covers these attacks.

- Alteration
- Replay
- Masquerading

3.4. Confidentiality

Confidentiality assure that information only be access by legitimate parties. For group communication confidentiality requirement is useful in which only members of group are allowed to access the information

3.5. Privacy

Driver's privacy is an important issue in vehicular communication. The personal and private information of drivers should be kept confidential others. Since the vehicle information such as location, speed, time and other car data are sent via wireless communication, there should not be possible to infer the driver's identity from this information.

3.6. Non repudiation

When a node sends out a message, it should not be able to later deny sending that message. In case of accidents, or investigations, problem-causing drivers should be reliably identified, to correctly address the sequence and contents of communicated messages. This can be done by signing outgoing messages with an anonymous key exclusively related to the sender and also a timestamp associated to the message preventing the user to claim that a particular message has been replayed.

After reviewing the security requirements that VANET should satisfy when deployed, it can be concluded that security is very important in VANET. Moreover, securing all communication and assuring attack-free environment is not an easy job due to the high movability and the topology of the network. Hence, research is still on going to secure more areas of VANET communications.

4. RELATED WORK

- Denial of service (DOS) attack and its possible solutions in VANET [19]: Authors give an explanation of the need to obtain network availability all the time in order to guarantee security. Then they explained different possible attacks in VANET including DOS attack. The DOS attack was then introduced and

its severity was presented. Authors classified DOS attacks into three categories: 1) Basic Level (overwhelm node resources). 2) Extended level (jamming the channel). And 3) Distributed Denial of Services (DDOS). A proposed solution was given based on relying on exploiting the On-Board-Unit (OBU) that each vehicle is furnished with. OBU is expected to make a decision as to avoid a DOS attacks using one of the proposed techniques (switching channels, technology or use frequency hopping [17].

- A New Anti-Jamming Strategy for VANET [9]: Authors have studied the security problems that VANET can encounter. In particular they focused on jamming-style DOS attacks. Anti-jamming[14] is a vital operation in WSN(Wireless Sensor Network) The paper discussed the effectiveness of defense mechanism against jamming and proposed a new direction to utilize RSU to make VANET defense more achievable. Authors defined a scheme called as Hideaway strategy which uses the PSR (packet send ratio) to decide if a network is jammed and in consequence all nodes should go into silent mode. The paper didn't describe detection and supposed it is out of the paper scope.
- Security Challenges, Issues and their Solutions for VANET [7]: R. Raw et al. studied the security requirements and challenges to implement the security measure in VANET. Different attacks and their solutions were discussed. Upon surveying the security requirements, authors concluded that confidentiality is not needed in VANET. The conclusion was based on the assumption that packets on VANET do not contain any confidential data. The paper provided a tabulation measurement of different attacks, technology, security requirements, and solutions used for defense [2].
- Jamming Attack: Behavioral Modelling and Analysis [6]: The paper studied jamming attack intensively. It categorized jamming attack into active and reactive jamming. Authors assessed the impact of different categories of jammers using NS2 simulation. The data was analyzed to show that reactive jamming is more difficult to identify than other attacks because of the intelligent behavior. The paper contribution gave an idea to use the behavioral modeling and analysis tools to understand jamming attacks behaviors to develop an efficient defense strategy.
- A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS(Intelligent Transport System) Services [23]: This paper proposed a new hybrid routing protocol to provide protection for VANET. The protocol is called Position Based Secure Routing Protocol (PBSRP) which is composed of different elements of MFR (Most Forward within Radius) and B-MFR (Border node based) routing protocols. This protocol resides three phases.

  1) Initialization, 2) Optimal node selection, and 3) Secure data delivery phase. Authors also merged a security module by using RSU to RSU key agreement protocol to provide data confidentiality and protect against active and passive attacks. The proposed scheme deals better performance than MFR and B-MFR routing protocols with regard to PDR and end-to-end delay. Authors suggested that the scheme will help many real time applications and it form the system robust.
- Mitigating the effect of jamming signals in wireless ad hoc and sensor networks [22]: Authors aimed to use MPT (Multi Packet Transmission) and MPR (Multi-Packet Reception) to diminish the effect of DOS jamming signal. The main contribution of this paper was that MPR and MPT can be used to importantly to reduce: 1)The probability of successful mitigation for jamming signals. 2)The effect of jamming signals on throughput reduction. 3)The maximum throughput at all jamming signals rate. Authors only discussed theoretical work and stated that the hardware and software to apply the proposed scheme can be performed with moderate complexity due to the electronics advancement.
- VANET Routing on CITY Roads Using Real-Time Vehicular Traffic Information [21]: In this paper authors proposed a new routing protocol called RBVT (Road-Based using Vehicular Traffic) to provide more appropriate routing among vehicles in VANET. The protocol is presumed to outperform existing

routing protocols in city-based VANET. The proposed RBVT uses real-time vehicle traffic information to make road-based paths[12]. The paper proposed two sub protocols called RBVT-R and RBVT-P to work as reactive or proactive protocols. The RBVT guess that each vehicle is provided with GPS, digital maps and navigation system. In RBVT-R the protocol goes through two phases, route discovery and route reply while RBVT-P algorithm has four phases, discover the topology, and disseminate it, computing route, and route maintenance. The proposed protocol accomplishes improvement of 40% better than AODV(Ad-hoc On demand Distance Vector)routing protocol and 30% increase compared with GSR in terms of average delivery ratio and average delay. This paper makes use of the flooding technique between nodes which can cause network overhead. Moreover, the paper didn't point any security issues that VANET can face.

- Detection and Prevention of Physical Jamming Attacks in Vehicular Environment [1]: Authors have studied security problems of Vehicular Ad hoc Network (VANET).VANET routing protocols could enhance system performance by increasing throughput and decreasing data lost. To reduce the effect of interruption, it is significant to detect its existence. In this paper, an enhanced detection mechanism has been suggested. If packet size increased to a specific RTS(Request to Send) threshold, the but packet would have to wait for a specific RTS and CTS(Clear to Send) interval to completely route that packet to its destination node. So the buffer size is considered as102400000. The physical characteristics is modified to Extended Rate. The buffer size and data rate are changed[16] for the prevention of penalties and for increasing the throughput, enhanced AODV parameters are also used in this paper.
- Solution of Detecting Jamming Attacks in Vehicle Ad Hoc Networks [10]: Authors have studied jamming attack on VANET and suggested a new algorithm to detect jamming attack. The proposed detection method is based on the PDR[Packet Delivery Ratio] and its miniature. The PDR value and the rate PDR reduction is used to decide whether a network is jammed as soon as the change of PDR surpasses a threshold. Then warning messages will be provided with high priority. The basic concept is when a vehicle enters a jammed area the parameter Down_ PDR is assumed to detect that it is jammed. When a vehicle is jammed its PDR is high but the rate of PDR reduction is high. Hence, the vehicle is considered jammed. This will lead to broadcast a warning message contains information of its state, direction, jammed time and jammed position.

  The paper provides a new scheme to discover jamming attack in VANET however, it only considers one type of jamming. In real world, jammers can use different methods to block all transmission and have more potential to which were not considered in the paper.
- Machine Learning-based Jamming Detection for IEEE 802.11: Design and Experimental evaluation[20]: In this paper authors have proposed a Jamming detection approach for 802.11 networks. It uses metrics that are attainable through standard device drivers and detect jamming attack via machine learning. The 802.11 network weighs and combines a substantial set of metrics and automatically chooses appropriate thresholds, thereby avoiding the arduous and error prone manual tuning. The metrics are provided to a machine learning algorithm to predict the like hood of a jamming attack. In addition to this approach, cooperative jamming detection can be combined to further increase the accuracy without incurring significant cost.
- Experimental Characterization and Modeling of RF Jamming Attacks on VANETs[18]:In this paper, authors have assessed the performance of 802.11p-based vehicular communication in the presence of RF jamming attacks. In addition to this, the authors identified that the periodic transmission of preamble like jamming signals can hinder successful communication. The impact of reaction delay and interference signals length on the effectiveness of the reactive jammer was also studied. Finally, the behavior of a vehicular platoon under the influence of jamming was predicted with realistic results.

5. CONCLUSION

VANET is an Intelligent Vehicular Ad-hoc Networking. It uses WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles [8],[15].However Jammer attacks will have an impact on network's performance as a result of jammer interference with the traditional operation. Several researchers try to discover the solutions and did well in their attempts by offering us with various techniques. This paper provides information on identifying jamming attacks and to provide solution to this attack. In this work, we extensively described VANET on various aspects. This paper surveyed different types of jamming problems and solution to evade these jamming problems. The effect of strong reaction method on attentive users of a probable jamming attack in the network may be investigated in future.

REFERENCES

[1] Mahendri, NehaSawal," Detection and Prevention of Physical Jamming Attacks in Vehicular Environment", InternationalJournal of Science, Engineering and Technology Research, 2015.

[2] A. Dhamgaye, and N. Chavhan, "Survey on Security Challenges in VANET", Vol. 2, pp. 88-96, IJCSN 2013.

[3] Rohini Ravat, Dr. Deepti Sharma, "Impact of Jamming Attack in Vehicular Ad hoc Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, April 2015.

[4] Vivek Chand dubey, Vinodkumar, "survey: Secure Routing in VANET", International Journal of Advanced Research in Computer Science and Technology, Vol. 3, Jan. 2015.

[5] R. Dass, R. Sangwan, and I. Girdhar, "Vehicular AdHocNetworks", IJATCSE, Vol. 1, October 2012.

[6] S. Babar, N. Prasad, and R. Prasad, "Jamming Attack: Behavioral Modelling and Analysis", IEEE, 2013.

[7] Sharaf Malebary, Dr. Wenyuan Xu, "A Survey on Jamming in VANET", International Journal of Scientific Research and Innovative Technology. Vol. 2, January 2015.

[8] Vijeta Verma, Vidha Sharma, "Intelligent Vehicular Communication system for collision Avoidance and Evaluation Metrics", International Journal of Advanced Research in Science and Engineering, Vol. 4, March, 2015.

[9] I. Azogu, M. Ferreira, J. Larcom, and H. Liu, "A New Anti-Jamming Strategy for VANET", Globecom2013Workshop, IEEE, 2013.

[10] Nguyen, L. Mokdad, and J. Ben-Othman, "Solution of Detecting Jamming Attacks in Vehicle Ad Hoc NETworks", ACM, 2013.

[11] Hamieh, J. Othman, and L. Mokdad, "Detection of Radio Interference Attacks in VANET", IEEE, 2009.

[12] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET Routing on City Roads Using Real-Time VehicularTraffic Information", Vol. 58, pp. 3609-3626, IEEE, September 2009.

[13] M Abdellatif, "A Brief Summary on the Main Aspects and Challenges of Vehicular AdHoc Networks (VANETs)", INESC Porto, 2010.

[14] Y. Zhu, X. Li, and B. Li, "Optimal Adaptive Antijamming in Wireless Sensor Networks", International Journal of Distributed Sensor Networks (IJDSN2012), Volume 2012.

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", ACM, 2005.

[16] Geetha Priya Tamilarasu, Sumita Mishra, and Ramalingam Sridhar, "Improving Reliablity of Jamming Attack Detection in Ad hoc networks", International Journal of Computer Networks and Information Security, Vol. 3, April 2011.

[17] Swapnil G. Deshpande, "Classification of Security attack in Vehicular adhocNetwork: A Survey", (IJEITCS), Vol. 2, March 2013.

[18] Ascar Punal, Carlos Pereira, Ana Aguiar, "Experimental characterization and Modeling of RF Jamming Attacks on VANET", IEEE, 2014.

[19] 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.

[20] Ismet Aktas, Caj-Julian Schnelke, James Gross, "Machine Learning-based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation" IEEE, 2014.

[21] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information", Vol. 58, pp. 3609-3626, IEEE, September 2009.

[22] J. Sarker, and H. Mouftah, "Mitigating the effect of jamming signals in wireless ad hoc and sensor networks", IET Communications, 2012.

[23] 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.

[24] Y Qian, K. Lu, and N. Moayeri, "A Secure VANET MAC Protocol for DSRC Applications", IEEE Globecom, 2008.

[25] A. Dhamgaye, and N. Chavhan, "Survey on Security Challenges in VANET", Vol. 2, pp. 88-96, IJCSN 2013.