International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:4, No:5, 2010

Denial of Service (DOS) Attack and Its Possible Solutions in VANET

Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan

***Abstract*—**Vehicular Ad-hoc Network (VANET) is taking more attention in automotive industry due to the safety concern of human lives on roads. Security is one of the safety aspects in VANET. To be secure, network availability must be obtained at all times since availability of the network is critically needed when a node sends any life critical information to other nodes. However, it can be expected that security attacks are likely to increase in the coming future due to more and more wireless applications being developed and deployed onto the well-known expose nature of the wireless medium. In this respect, the network availability is exposed to many types of attacks. In this paper, Denial of Service (DOS) attack on network availability is presented and its severity level in VANET environment is elaborated. A model to secure the VANET from the DOS attacks has been developed and some possible solutions to overcome the attacks have been discussed.

***Keywords*—**Vehicular Ad hoc Network (VANET); security; availability; security attack; Denial of Service (DOS).

I. Introduction

VEHICULAR Ad-hoc Network (VANET) is a kind of networks in which vehicle nodes can communicate in multihop fashion with each other on the road [1]. VANET applications have been broadly categorized into safety and non-safety applications. Safety applications are very important in nature as these are directly related to users and their lives. These applications provide warning-related information to drivers such as post-crash notification on a particular road [2]. Simply, VANET is concern with safety of human life while these people are moving on the roads. Non-safety applications are to comfort the drivers and passengers, and to improve the traffic system. Traveling map, parking availability, and weather information are the examples of these applications.

Generally, the purpose of both applications categories is to provide correct information to users/drivers on the roads. However, for safety applications, the information not only needs to be correct but also securely transmitted from a source to a destination. Hence, security is an important issue where little interruption, such as intermittent disconnections can create problem to the users. This is particularly crucial if critical life information is being communicated between a sender and a receiver. To achieve this, network availability is a basic requirement. As identified by [2], availability is one of the major security requirements. It is defined as when any node wants to access the other node in the network or to access the infrastructure, the network should be accessible to user.

Corresponding author is with the Department of Computer and Information Sciences. Universiti Teknologi PETRONAS. Bandar Seri Iskandar 31750,Tronoh,Perak, Malaysia. e-mail:halabi@petronas.com.my

The inaccessibility or unavailability may be contributed from any fault or any kind of attacks, such as Denial of Service (DOS). This paper is divided into six sections; Section II describes the possible attacks in VANET. Section III explains the DOS attack and its levels with possible use cases. In Section IV we discuss some possible solutions and proposed model to secure the network. Analysis and discussion is provided in Section V and conclusion in Section VI.

II. Possible Attacks in VANET

Due to the nature of open wireless medium used in VANET, there are a number of possible attacks by which the VANET is exposed to. Hence, the chances for possible attacks are so high. The purpose of the attackers is to create problem for legitimate users, and as a result services are not accessible, thus denial of service. Some of the DOS attacks are mentioned below.

A. Sybil Attack

Douceur [3] is the first author who described Sybil attack. In this attack type, a node sends multiple messages to other nodes and each message contains a different fabricated source identity in such a way that the originator is not known. The basic goals of the attacker are to provide an illusion to other nodes by sending wrong messages and to enforce other nodes on the road to leave the road for the benefits of the attacker [4].

B. Node Impersonation

Impersonation is an attempt by a node to send a modified version of a message received from the real originator for the wrong purpose and claim the message as come from the originator. To overcome this problem, a unique identifier is assigned to each vehicle node in VANET, which will be used to verify the real message originator. Police may use it to identify the driver as it is associated with driver's identity [5]. It is important to protect this identifier so that it can not be misused by the attacker.

C. Sending False Information

In this type of attack, wrong or fake information was purposely sent by a node to other nodes in the network to create a chaos traffic scenario, which it may lead to misinterpretation of the actual situation [6]. With the falsified information, the users would likely to leave the road, thus it makes the road free for the attacker to use it for his own purposes.

D. ID Disclosure

Disclose the identity of other nodes in the network and track the current location of the target node. Global observer monitors the target node and sends a 'virus' to the neighbors of the target node. When the neighbors are attacked by the virus, then they take the ID of the target node, as well as the target's current location. Rental car companies are using this technique to track their cars [7].

III. Denial of Service (DOS) Attack

In wireless environment, typically the attacker attacks the communication medium to cause the channel jam or to create some problems for the nodes from accessing the network. The basic purpose is to prevent the authentic nodes from accessing the network services and from using the network resources. The attack may result in devastation and overtiredness of the nodes' and network's resources. Ultimately, the networks are no longer available to legitimate users. In VANET, DOS shall not be allowed to happen, where seamless life critical information must reach its intended destination securely and timely. In summary, there are three ways the attackers may achieve DOS attacks, namely communication channel jamming, network overloading, and packets dropping [8]. There are three levels of DOS attacks as described below.

1) Basic Level: Overwhelm the Node Resources

In this DOS basic level attack, the goal of the attacker is to overwhelm the node resources such that the nodes can not perform other important and necessary tasks. The node becomes continuously busy and utilizes all the resources to verify the messages.

a) Case 01: DOS Attack in V2V Communications

As shown in Figure 1, an attacker sends a warning message "*Accident at location Y*". A victim node behind the attacker node receives this message. However, the sending of the same message is repeated continuously, thus keeps the victim node busy and thus completely denied for accessing the network.

Fig. 1 DOS attack in vehicle-to-vehicle communications

b) Case 02: Launch DOS Attack in V2I Communications

In this case, the attacker launches attack to Road Side Unit (RSU) as depicted in Figure 2. When RSU is continuously busy to verify the messages, any other nodes want to communicate with the RSU will not be able to get any response from it, thus the service is unavailable. Hence, sending critical life information in this situation is full of risk.

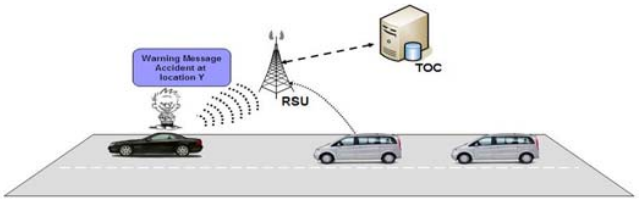

Fig. 2. DOS attack in vehicle-to-infrastructure communications

2) Extended Level: Jamming the Channel

This is a high level of DOS attack in which attacker jams the channel, thus not allowing other users to access the network. The following are two possible cases.

a) Case 01: Attacker sends high frequency channel and jams the communication between any nodes in a domain, as depicted in Figure 3. These nodes cannot send or receive messages in that domain, i.e services are not available in that domain due to this attack. When a node leaves the domain of attack, only then it can send and/or receive messages.

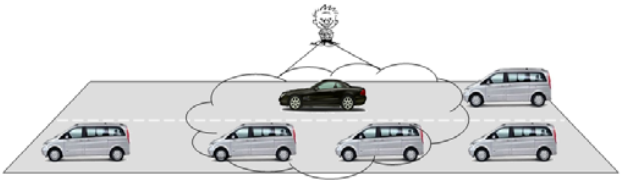

Fig. 3. A domain of jammed channel for vehicle-to-vehicle communications

b) Case 02: The next stage of attack is to jam the communication channel between the nodes and the infrastructure. Figure 4 showed the situation where the attacker launches an attack near the infrastructure to jam out the channel, leading to network breakdown. In this way, sending and/or receiving messages to/from other nodes is not possible and would fail due to network unavailability.

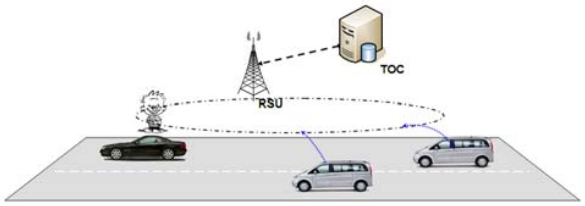

Fig. 4. Jam the channel between vehicle-to-infrastructure

3) Distributed Denial of Services (DDOS)

DDOS attacks are more severe in the vehicular environment because the mechanism of the attack is in distributed manner where the impact is dispersed in the network. In this kind of attack, the attackers launch attack from different locations. There are two possible cases as follow.

a) Case 01: Attacks are launch from different locations and each may use different time slots for sending the messages. The nature of the messages and time slots may vary

from node to node of the attackers. The aim of the attacks is to achieve network unavailability by bringing the network down at a target node. As depicted in Figure 5, there are three attackers' nodes (black color cars) send some messages to a target node in front (grey color car). After some time, the target node cannot communicate with any other nodes in the network.

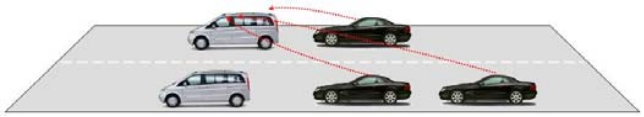

Fig. 5. DDOS in vehicle-to-vehicle communications

b) Case 02: In this case, the target of attack is the VANET infrastruture (RSU) as shown in Figure 6. There are three attackers in the network and launch attack on the infrastructure from different locations. When other nodes in the network want to access the network, the infrastructure is overloaded, thus denial of service.

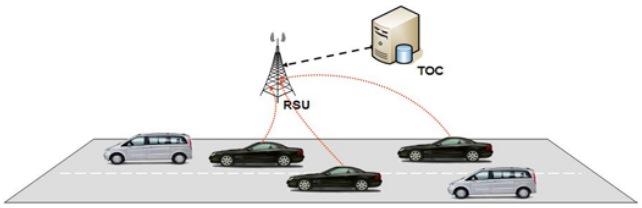

Fig. 6. DDOS in vehicle to infrastructure communications

IV. The Proposed Solution Model to DOS Attack

The proposed model of solution to the DOS attack was based on previous works by [9], [10] and [11]. The model is relying on the use of On-Board-Unit (OBU) that is fitted on each vehicle node, to make decision as to deter a DOS attack. In the case of DOS attack, the Processing Unit will suggest to the OBU to switch channel, technology, or to use frequency hoping technique. Four options are available for the OBU to make decision based on the received attack message. After necessary processing and decision, the information is sent to next OBU in the network. Each switching option is explained in the following.

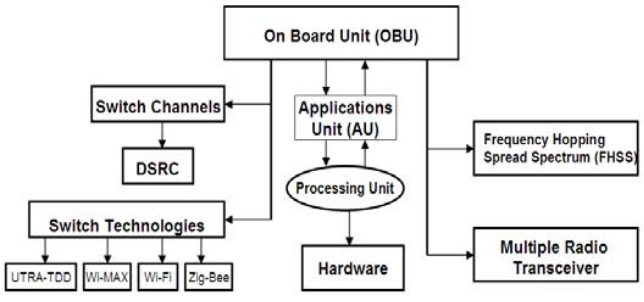

Fig. 7. The proposed model of solution to DOS attacks

A. *Channel Switching*

Dedicated Short-Range Communications (DSRC) provides multiple channels and its transmission ranges from 5.850GHz to 5.925GHz [12]. The DSRC spectrum is divided into seven channels and each channel is 10MHz, as depicted in Figure 8. The data transfer rate that DSRC provides is up to 27Mbps. The role of DSRC is important as it makes nodes and infrastructure communications possible. CH 172 and CH 184 are used for safety related applications, while CH 174, CH 176, CH 180, and CH 182 are used for non-safety applications. Due to the large number of non-safety applications, four channels are assigned to it. CH 178 is assigned to control channel, which generally used for safety related applications, broadcasts messages, and also provides advertise services [13]. With these channels assignment, whenever attackers jam any one of the channels, there are options to move to others channels. In this way, network availability is obtained, thus denying a DOS attack.

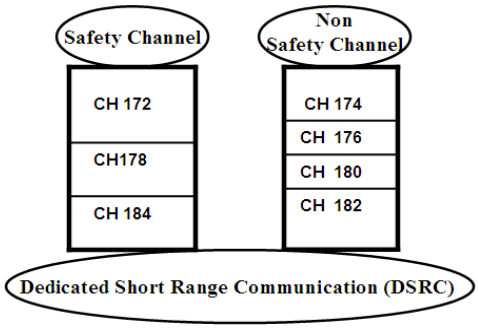

Fig. 8. DSRC and its safety and non safety Channels

B. *Technology Switching*

There are a number of communication technologies that work with VANET, such as UMTS's Terrestrial Radio Access -Time Division Duplex (UTRA-TDD), Wi-MAX ,Wi-Fi, and Zig-Bee. Whenever attacker launches attack, accessing to the network is switched between these technologies, making the attack terminated at a network type. Hence, the services of the overall network remain unaffected. Table I explained the detailed features of these technologies and also did comparison of different parameter (standard, frequency band, data rate, range and primary uses). The features of these technologies provide help to system to switch between technologies. If the intensity of the attack is low then we select low range technology and when the level of attacker/range of the DOS attack is large then we use cellular technology.

C. *Frequency Hopping Spread Spectrum (FHSS)*

Spread spectrum is a famous technology used in GSM, Bluetooth, 3G, and 4G. The purpose of spread spectrum is to expand the bandwidth of a signal by adding some keys/codes so that data packets can be transmitted over a set of different frequency range. Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) are two basic techniques used in spread spectrum communication. FHSS changes the communication channel using some regular interval and follow some pseudo-random sequences. The

objective is to provide security in the network, and when the attacker launches the DOS attack, the network has options to hop into different frequency channels. Two types of hopping techniques are usually used: fast and slow [14]. In slow frequency hopping, one or more data bits are transmitted in single hop. Fast frequency hopping is different from the former as one data bit is divided into multiple hops. This frequency hopping can take advantage of the DSRC channels to achieve secure transmission and importantly to obtain network availability to VANET users.

TABLE I COMPARISON OF DIFFERENT TECHNOLOGIES

Technology	Standard	Frequency Band	Data Rate	Range	Primary Use
UMTS	3G	1800/1900 MHz	2 Mbps	20Km	Cellular Technology
Wi-MAX	802.16 e	Less than 6 GHz	15 Mbps	Cell Radius 1 to 3 miles	Mobile Internet
Wi-Fi	802.16 a 802.16 b 802.16 g	5 GHz 2.4 GHz 2.4 GHz	54 Mbps 11 Mbps 54 Mbps	35-120 meters (indorr to outdoor) 38-140 meters (indoor to outdoor) 38-140 meters (indoor to outdoor)	Fixed Broad Band Wireless Network
Zig-Bee	802.15.4	2.4 GHz	250 Kbps	150 meters	WPAN

When attackers jam the communication channel, the DSRC with its multiple channels provide an ability to hop from one frequency channel to other (as depicted in Figure 9 and Figure 10) to alleviate the attack. Sender and receiver nodes already know the sequence of the hopping and they can exchange the safety messages to each others. Now its make difficult for attackers to launch any attack when the channels/frequencies are rapidly changed.

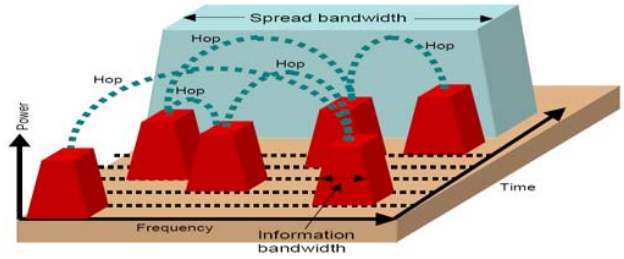

Fig. 9. Frequency Hopping Spread Spectrum [15]

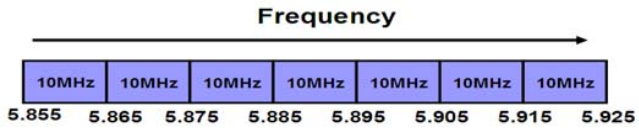

Fig. 10. DSRC frequency band

D. Multiple Radio Transceivers

It is also possible for the OBU to have multiple transceivers for sending and receiving messages, by applying the MIMO design principle. Hence, if there any case of DOS attacks, the system will have the option to move from one transceiver to another, thus eliminating the chance for total network collapse. As a result, part of the network remains in operation, allowing users to access the network and send/receive critical life information between nodes.

V. ANALYSIS AND DISCUSSION

Based on the various possible ways for launching an attack and based on the proposed switching model to overcome the DOS attacks as described in Section IV, Table II was developed summarizing the threat levels with respect to security issue in VANET. The summary was made possible based on the anticipated impacts when various attacks are allowed to occur on a VANET network.

Cheating of the position and ID disclosure can be classified as low level threat since these attacks will not lead to severe network disruption. Medium level threat is the classification for sending false messages and sybil attacks. These two levels of attacks affect the communication but the nodes still can transmit/receive messages and remain as part of the network. However, DOS and DDOS are associated to high level threats. This is because when attacks were launched, the network will not be available to legitimate users, thus denial of service. The network may be reestablished in an attempt to provide continuous services, but it will be only available for short period of time before it breaks down and leads to unavailability of network and its services.

TABLE II SECURITY ATTACKS AND THREAT LEVELS

Attack Threat	Cheating their position	ID disclosure	Sending false info	Sybil attack	DOS	DDOS
Low level	√	√	–	–	–	–
Medium level	–	–	√	√	–	–
High level	–	–	–	–	√	–
Highest level	–	–	–	–	–	√

From another view point and as a consequence from service unavailability, DOS and DDOS attacks directly affect the trust in a VANET network. When the attacks have successfully caused the network to break down, the trust for accessing and using the network services will no longer exist. Furthermore, the nodes may no longer believe on any received messages, thus leading to mistrust of the network and its services by the VANET nodes.

VI. Conclusion

Safety is the primary concern to many road users. The safety requirements can be powerfully supported by many safety applications, such as traffic report and accident notification. VANET application has the opportunity to provide such safety requirements. However, life critical messages must be transmitted from node to node in the VANET network in reliable and timely manner. To achieve this, secure communication and network availability must be obtained in the VANET set up. In this paper we have discussed the different types of attacks that may be applicable to VANET. We have proposed a model to provide solution to DOS and DDOS attacks, which the intention is to ensure network availability for secure communication between the nodes. We found that network availability has been directly affected in the case of DOS and DDOS attacks, where the attacks has led to most severe impact by causing the network to break down. In another view and as a result of an attack, trust in the network may not be developed if the life critical information is altered by attackers before it is really being received by the intended recipient. Therefore, it is important to maintain network availability and to develop thrust in the VANET network, in order for the safety applications to be useful and beneficial to road users.

References

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

[2] J. Jakubiak, Y. Koucheryavy, "State of the Art and Research Challenges for VANETs", 5th IEEE Consumer Communications and Networking Conference, 10-12 Jan. 2008, pp. 912-916.

[3] J. Douceur, "The sybil attack", First international workshop on peer to peer (P2P) system, March 2002, pp. 251-260.

[4] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)**",** WISTP 2008, LNCS 5019, pp.106-116.

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, J-P Hubaux, "Secure vehicular communication system : Design and Architecture Communications" IEEE Magazine, November 2008,vol. 46, pp. 100-109.

[6] P. Klaus, T. Nowey, C. Mletzko, "Towards Security Architecture for Vehicular Ad Hoc Networks", First International Conference on Availability, Reliability and Security (ARES'06), 20-22 April 2006.

[7] H. Moustafa, Y. Zhang "Vehicular Networks techniques, standard and applications", CRC Press, Chapter no.12, pp.336.

[8] J. Blum, A. Eskandarian, "The Threat of Intelligent Collisions", IT Professional, IEEE Computer Society, 2004.

[9] M. Raya, J. Pierre, Hubaux, "Securing vehicular ad hoc Networks" Journal of Computer Security, Vol.15, Issue 1, January 2007, pp. 39-68.

[10] A.Stampoulis, Z. Chai, "A Survey of Security in Vehicular Networks"

[11] R. Prasad, R. Kanjee, H. Zui, Pishro, "DSRC Accident Warning system at Intersection", Technical Report, October 19, 2006.

[12] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, R. Herrtwich, "Design of 5.9GHz DSRC-based vehicular safety communication", IEEE Wireless Communications, Vol.13, No.5, 2006, pp. 36-43.

[13] A. Yahya, O. Sidek, J. Mohamad-Saleh, "Design and Develop Wireless System Using Frequency Hopping Spread Spectrum", Electrical Engineering Department, University Science Malaysia, Engineering Letters, 13:3, 4 November 2006.

[14] W. Stallings, Wireless Communications and Network, 2nd edition, Pearson Prentice-Hall, 2005.