Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Inter-Network Cross-Verification Model by Reducing DoS Attacks in VANET

Priyanka
Computer Science & Engineering
Lovely Professional University, India

Harjit Singh
Asst. Professor
Lovely Professional University, India

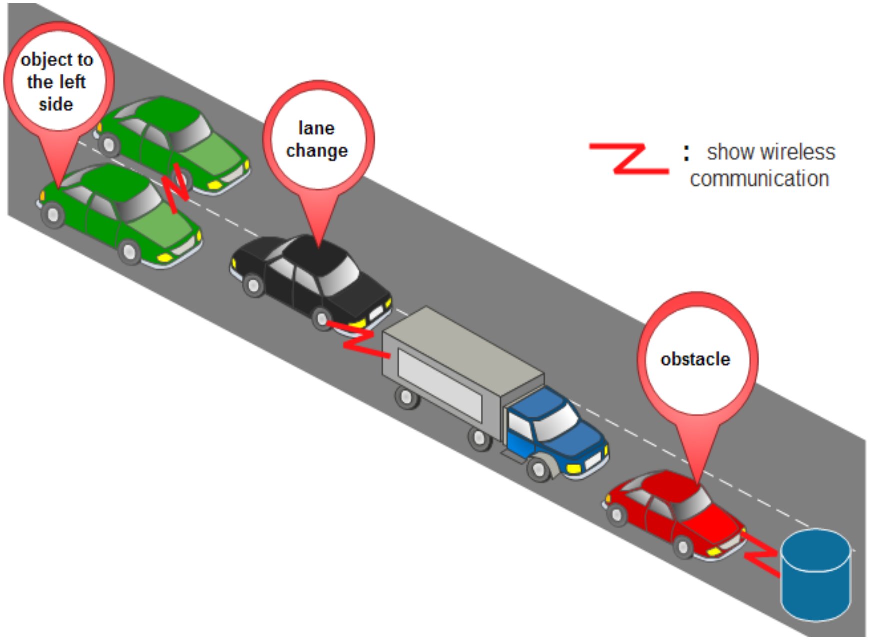
***Abstract** - VANET comes under the category of MANET. In VANET every participating vehicles are treated as the wireless node. VANET helps to improve the (ITS) intelligent traffic system. VANET is a sort of systems in which the vehicles can convey two or more vehicles style with one another on the roadside. The vehicular ad hoc networks have very promising future as they provide with an insight to the safe road environment. Vehicles can communicate with each other when the mobile network is created. There are a variety of security attacks promising in VANET. In this paper we are going to propose a algorithm to reduce the flooding of DoS attacks in VANET. The RRDA algorithm helps in maximizing the security by reducing DoS attacks and increases the response time.*

***Keywords:** APDA (attacked packet detection algorithm), RRDA (request response detection algorithm), VANET (vehicular ad-hoc network), ITS (intelligent transportation system).*

I. INTRODUCTION

VANET is basically a wireless sensor network which is used to create the mobile network. Mobile network is based on mobile vehicles that are represented by wireless nodes on the network. VANET is provides the wireless communication between the vehicles or wireless nodes on the network [2]. The main function of VANET is to provide the safety, security and privacy on the network. In these days VANET becomes more popular in most of the countries [5]. VANET comes under the subcategory of MANET (mobile ad hoc network). VANET stands for Vehicular ad hoc network which uses cars or vehicles as nodes so as to create a vehicular network. A VANET turns each participating vehicles into wireless router or a node and in turn to make a network with a broad range. As the cars or vehicles falls out of warning sign range and fall out of network others cars or vehicles can connect to one another [4] [7]. Vehicular Ad-Hoc Networks (VANETs) is self-organize and self-manage the information in a distributed style. They hold vehicles and roadside units that aid within the organization of the network.

In ITS (Intelligent transportation system) VANET is used as an important element of it. To provide the wireless access in the vehicles, ITS uses WAVE and it is designed with the standard IEEE 802.11p. In vehicular ad hoc network every vehicles or wireless nodes are well furnished with on board radio transductor (ORT). ORT helps in communicating with the other nodes or wireless vehicles on the network [1].



In VANET there are many applications that helps in providing the availability of parking, traffic intensity, beware of accidents. We have distinguished numerous investigates, endeavors that have researched different issues identified with V2I, V2V and VRC territories. Three types of communications used in vehicular ad hoc network are V2I, V2V and VR1 [11].

ATTACKS:

Due to the size of the network various attacks are prone in the VANET and become hard to overcome them. The various attacks introduced in VANET are:

1. DENIAL OF SERVICE ATTACK in VANET: This attacks main purpose is to disable the system that provides network services rather than to steal data. This attack prevents the system to respond to the requests [5].
2. SPOOFING attack in VANET: In this attack a device outside the network uses an internal network address to masquerade as a device inside the network [5].
3. DISTRIBUTED DENIAL OF SERVICES attack: this attack is a type of DoS attack which uses multiple mismatched or uncoordinated networks to launch the attack from many simultaneous sources. The attacker introduces software like zombie or drone that directs the computer to launch attack.

II. RELATED WORK

Lobna Nassar, M.et.al. VANET IR-CAS for safety ACN: Information Retrieval Context Aware System for VANET Automatic Crash Notification Safety Application: This paper proposes IR-CAS for VANET fully automatic crash notification safety application. It helps to increase the accuracy and efficiency with its exact or accurate notifications and also helps to increase the decentralization. Different IR models are compared using binary and partial effectiveness measures and the estimation of difficulty is done by calculating the Manhattan distance between crash and severest crash context vectors. [1]

Chan-Ki Park et. Al (2013) Measuring the Performance of Packet size and Data rate for Vehicular Ad-Hoc Networks: In VANET the wireless access in vehicular environments provides the safety service and information to driver as well as to passenger. Currently most of the researchers have been proposed resolution for high speed and rapid topology change or it assumes to packet size. This assumption could not provide the various services for VANETs because of limited size of the packets. In this paper they resolve this problem by analyzing the transmission rate of different packets in VANET using NS2 simulator. The future work from this paper is to develop the channel assign algorithm using multi-channels and MAC protocol for improving the transmission efficiency. [2]

Karan verma et.al. (2012) find an efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. In user datagram protocol (UDP) based flooding that is a form of the Denial of Service attacks, in which the malicious node forms the large number of fake identities. Here is the method that is used to detect and defend against the UDP flooding attack. This method makes use of the storage efficient data structure and Bloom filter method based IPCHOCKREFERENCE detection method. [3]

Yeongkwum kim et. Al. (2013) explains about the security issues in VANET: in VANET security and privacy are the most important factor motivating robust vehicular network designs. Here they discuss about the various threats and attacks in the VANET and in response, provides some security solutions. In this paper they introduce some applications and possible attacks. They provide the brief survey of the security related issues and provide their solutions in vehicular network environment. [4]

Usha Devi Gandhi et. Al.(2014) RRDA (Request Response Detection Algorithm) for Detecting DoS attacks in VANET. In this paper they have worked on detecting the DoS attacks in VANET. Here the attribute of the requesting vehicle is verified and this verification goes through checking no. of packets sent/sec, speed of the vehicle and the maximum capacity of the packet. In this paper they proposed a Request Response Detection Algorithm (RRDA) that helps to detect the DOS after APDA. This algorithm helps in increasing the response time and maximizing the various security attacks in VANET. [5]

Gongjun Yan et al. (2008), in this paper, their main commitment are a novel way to deal with upgrading position security in VANET. To place security in VANETs and attain local security with the aid of on-board radar to discover neighboring vehicles and to confirmed their announced coordinates. Local security is extended to attain global security with the help of preset position-based groups to create a communication network by using a dynamic challenging mechanism to verify remote position information. They accomplish neighborhood and worldwide position security by utilizing the on-board radar to distinguish nearest vehicles and to affirm their declared directions. They process cosine comparability among information gathered by radar and neighbors' reports to channel the manufactured information from the honest information. In view of sifted information, we make a background marked by vehicle development. By checking the history and figuring likeness, we can keep countless assaults and a few mixes of Sybil and position-based assaults. Traded off vehicles are arbitrarily conveyed in the framework. At the point when there are less than 16 traded off vehicles, the time needed to identify them doesn't change with their rate of the activity. On the off chance that there are more than 16 traded off vehicles, the bring down the rate is, the more it takes to discover them on the grounds that they are more sparsely distributed and need more hops to be detected [6].

P. Papadimitratos et al. (2008) analyze threats and recognize security and privacy requirements, and provide a scale of mechanisms to safe vehicular communications systems and present a solution that can be rapidly adopted and deployed [7].

Ali Hamieh et al. (2009) Vehicular Ad hoc Network (VANET) is vulnerable to Denial of Service (DoS) attacks, like jamming attack. The purpose of a jammer is to hinder with legitimate wireless communications, and to mortify the overall QoS of the network. In this paper, they propose a model to detect a particular class of Jamming attack, in which the jammer transmits only when valid radio activity is signaled from its radio hardware. Vehicular ad hoc networks (VANETs) are networks in which wireless mobile nodes establish temporarily network connectivity and perform routing functions under self-organization. Due to their nature, VANET is vulnerable to DoS attacks, such as jamming attack. The goal of a jammer is to obstruct with genuine wireless communications, and to mortify the overall QoS of the network [8].

Halabi Hasbullah et al. (2013) work on Denial of Service (DOS) attack and its probable solutions in VANET which use the redundancy elimination mechanism. The level of security is basically added by this solution to its already existing solutions of using various alternative options like channel-switching, frequency-hopping, communication technology switching and multiple-radio transceivers to counter affect the DOS attacks. Without using any cryptographic scheme the proposed scheme enhances the security in VANETs. [9]

Jose Maria et al. (2010) provides general idea of current security issues in Vehicular Ad-hoc Networks focusing on road safety communications and identified the security requirements i.e. Confidentiality etc that is present on each VANET setting. There are other context-specific ones i.e. trust assurance over reported data and also described and analyzed the main proposed mechanisms to achieve the security goals. [10]

Ghosh.A.et.al. (2014) Exploring efficient seamless handover in VANET systems using network dwell time: In this paper they provide the more wide-ranging analysis involving beacon frequency, beacon size and the speed of the vehicles. They use a small amount of concept of y-Comm architecture like network dwell time (NDT), time before handover and exit time to provide a support to investigate handover issues. The future work from this paper is to develop complete structure which includes handover policy management mechanism in mobile devices that allows practical flawless handover in the both urban and motorway context. [11]

III. PROBLEM FORMULATION

VANET is one of the most important technologies for creating network of mobile vehicles. Creating instant network and working on it is a challenge in VANET. In the previous researches, they have worked on detecting DOS attack in a VANET network. Though it is efficient, it is divided into two algorithms. In the first one, the attributes of the requesting mobile vehicle is verified [5]. These verifications go through checking number of packets sent per second, speed of the vehicle, and maximum capacity of the packet. For an instant network creation and management it is quite time consuming. To make it a speedier verification process, we are going to propose an internetwork cross verification model, where the vehicles inside the network will be verifying the requesting vehicle rather than requesting RSRT (Road Side Radio Transductor) for verification.

IV. CONCLUSION

The vehicular ad hoc networks have very promising future as they provide with an insight to the safe road environment. If all the vehicles are providing with correct information to all the requesting vehicles then many applications such as road safety, traffic monitoring can be realized into real lives. We have studied the distributed denial of service attacks in our study and reduced the impact of flooding for the same. However, we would further like to take into account various other attacks such as black hole attack and make network secure from the same.

ACKNOWLEDGEMENT

I take this opportunity to express my deep regards and science gratitude for this vulnerable guidance rendered to my guide. Mr. Harjit Singh Asst. Professor, of department of computer science and engineering at Lovely Professional University. I got new knowledge for this kind and valuable guidance for the completion of my thesis work. His consistent support and intellectual guidance made me energize and give up the new idea.

I am thankful to professor, H.O.D of Computer Science & Engineering for this support and providing necessary facility to carry out the work. I am thankful to all my professor and member of the department for their generous help in various ways for the completion of this thesis work.

Finally, I am also thankful to my parents, my friends who have helped me a lot in completion of my thesis work.

REFERENCES

[1] Lobna Nassar, Mohamed S. Kamel, Fakhri Karray *"VANET IR-CAS for Safety CAN: Information Retrieval Context Aware System For VANET Automatic Crash Notification Safety Application ",* Springer Science, 2014.

[2] T.W.Chim, S.M.Yiu, Lucas C.K. Hui "*VANET-Based secure and Privacy-Preserving Navigation (VSPN)",* IEEE , Volume-63, No. 2, February 2014.

[3] Karan Verma, Halabi Hasbullah *"An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VENET"* IEEE 2012.

[4] Yeonkwun Kim, Injoo Kim, *"Security Issues in VANET",* IEEE, 2013.

[5] Karan Verma, Halabi Hasbullah, Ashok Kumar *"An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) stacks in VANET"*, IEEE, 2013.

[6] G. Yan, S. Olariu, , M. C. Weigle, *"Providing VANET security through active position detection,"*. Computer Communications, vol. 31, No. 12, 2883-2897, 2008.

[7] Gandhi.U,.(2014).*"Request Response detection algorithm for detecting DOS attack in VANET"*,Journal of Engineering Science and Technology, 2014.

[8] Park, S., Aslam, B., Turgut, D., Zou, C.C., (2009) *"Defense against sybil attack in vehicular ad hoc network based on roadside unit support"*. In: MILCOM, pp. 1–7.

[9] R. Lu, X. Lin, H. Zhu, and X. Shen, *"An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications,"* IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010.

[10] Arindam Ghosh, Vishnu Vardhan Paranthaman, Glengord Mapp and Orhan Gemikonakli *"Exploring Efficient Seamless Handover in VANET Systems Using Network Dwell Time",* Springer, 2014.