Various Techniques to detect DOS attack in VANET: A Review

Rajwinder Kaur
Research Student
Department of
Computer Science and
Engineering
Sri Guru Granth
Sahib World University
Fatehgarh Sahib

Usvir kaur
Research Student
Department of
Computer Science and
Engineering
Sri Guru Granth
Sahib World University
Fatehgarh Sahib

ABSTRACT

The vehicular adhoc network is the type of network.It is self configuring and decentralized architecture. In the vehicular adhoc network two type of communication is possible which is vehicle to vehicle and vehicle to infrastructure. Due to decentralized architecture of vehicular adhoc networks many malicious nodes may join the network which is responsible to trigger various type of active and passive type of attacks. In the network various when some malicious nodes join the network and that nodes are responsible to trigger DOS type of attack which reduce network performance. Hence Dos attack is harmfull due to inside as well as outside attackers. Experimental results show that the proposed scheme not only alleviates DOS attack but also performs better with negligible computational overhead.

Keywords

VANET,Dos attack,Security,Availability

1. INTRODUCTION

VANET is a self organized many promising applications by exchange of messages between V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) for improvising driving experience. These applications can be classified into safety and non safety related applications.The safety related applications support mostly life critical messages, which are generally broadcasted. Whereas the non safety related applications consist of infotainment related messages to improvise the comfort of driving experience. So, the overall aim of these applications is to provide safe and secure messages to the users.[1] VANET is an application of mobile ad hoc network. VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers.[2] The main objective of VANET is to help a group of vehicles to set up and maintain a communication network among them without using any central base station or any controller. Vehicular ad-hoc networks are responsible for the communication between moving vehicles in a certain environment. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a networkss and is a variant of mobile ad-hoc networks (MANETs). The network consists of infrastructure units such as road side units (RSUs) and wireless communication devices installed on vehicles. VANETs provide Road Side Unit (RSU), known as Vehicle-to-Infrastructure (V2I). [3]

2. LITERATURE REVIEW

R.M. Pai, N. Ajam and J. Mouzna et al. 2014 [1] Authentication is an essential framework for safe and secure communication of messages in VANETs. For authenticating messages the standard uses ECDSA as the standard digital signature algorithm. But the verification time for an ECDSA signature is very high. As a result an inside or an outside attacker could use a fraction of bandwidth and flood the network with invalid signatures resulting in Denial of Service (DOS) attack. As a part of future work, we see that this system tries to mitigate DOS attack only if the attacker floods the system with fals signatures. But if the attacker tries to flood the system with bogus information and valid signatures this system is not so effective. So as a part of future work we will investigate on how to deal with this issue.

R.S. Raw, M. Kumar and N. Singh 2013 [2] Vehicular Ad hoc Networks (VANETs) are the promising approach to provide safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security in VANET got less attention. In this article, we have discussed about the VANET and its technical and security challenges. We have also discussed some major attacks and solutions that can be implemented against these attacks. We have compared the solution using different parameters. Lastly we have discussed the mechanisms that are used in the solutions.we have represented about the opne issues and challeges invalid in VANET.

S. Rehman and T. Zia 2014 [3] VANETs have now been established as reliable networks that vehicles use for communication purpose on highways or urban environments. Along with the benefits, there arise a large number of challenges in VANET such as provisioning of QoS, high connectivity and bandwidth and security to vehicle and individual privacy. This article presents state-of-the-art of VANET and discusses the related issues.

Dr.Ramaprabha and V.Premalatha 2016 [4] VANET turn every participating car into a wireless router or node,allowong cars approximately 100 to 300 meters of each other to connect and in turn create a network with a wide range. VANEt is emergent technologies that they desver of numerous technologies that they desverve ,recently the attention of the industry and the academic institution .

V. H. LA, A. CAVALLI 2014 [5] Vehicular ad-hoc networks (VANETs) technology has emerged as an important research area over the last few years. Being ad-hoc in nature, VANET is a type of networks that is created from the concept of establishing a network of cars for a specific need or situation. VANETs have now been established as reliable networks that vehicles use for communication purpose on highways or urban environments. Along with the benefits, there arise a large number of challenges in VANET such as provisioning of QoS, h igh connectivity and bandwidth and security to vehicle and individual privacy. This article presents state-of-the-art of VANET and discusses the related issues.

A. Quyoom, R. Ali and D. Gouttam et al 2016 [6]. Among all these attacks, denial-of-service (DoS) attacks is a major threat to the information economy. In this paper, we proposed an Malicious and Irrelevant Packet Detection Algorithm (MIPDA) which is used to analyze and detect the Denial-of Service (DOS) attack. As a result, the attack is eventually confined within its source domains, thus avoiding wasteful attack traffic overloading the network infrastructure. It also reduces the overhead delay in the information processing,which increases the communication in coming time we are going to detetect of multiple malicious, invalid to request sent and received from muliple vechicles at a time and to analyze and detect the attacker in effcient and effective manner for enviroment.

A. Singh and P. Sharma 2015 [7] . It is the responsibility of RSU to make the network available all the time to every node for secure communication of critical information. For this, network availability occurs as the major security requirement, which may be exposed to several threats or attacks.Among these Denial of Service attack is the major threat to the availability of network. VANET from DOS attack we have proposed Enhanced Attacked Packet Detection Algorithm which prohibits the deterioration of the network performance even under this attack.In future work to assign priority to emergancey vehicles such as ambulancew,fire extinguiseher,etc to verify them in less time as campared to vchicles.

M. N. Mejri, N. Achir and M. Hamdi 2016 [8] Vehicular Networks are an ideal target for various types of rational and non-rational attackers. To cope with, reaction methods against these attacks must exist. In this direction, game theory applied to the security of wireless networks can be a good way of modeling. In this paper we propose a reaction method against DOS attacks in VANET. In this method we have the choice between two proposed reaction games. Design methodology and defined metrics are inspired from game theory models. To the best of our knowledge, no similar games have been proposed before. The simulations showed the efficacy of our proposal measured by the performance of the obtained results. We evaluated our proposed game by simulation.we believe these contibutions to be very useful for solving the DOS attack reaction problem in VANETs.

N.lyamin, A.Vinel, M. jonsson 2014 [9] A method for real time detaction of denial of services attacks in IEEE 8021.11p vehicular ad hoc networks is proposed. Thestudy focused on the jamming of perioidic position.pof attack detcetion and false alarm are estimated for two different attackers models.Our on goning work is focused on rellaxing the assumptions of the presented model and correspondingly enchancing the detection for realistic scenarios.

D.Johnson, A.Menezes, S.Vanstone 2001 [10] The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA).

Author's Name	**Year of Publication**	**Description**	**Outcomes**
R.M. Pai,N. Ajam ,J. Mouzna	2014	Authenticating messages the standard uses ECDSA as the standard digital signature algorithm. But the verification time for an ECDSA signature is very high.	The solutions helps in mitigate the effects of denial service attack against signature based authentication due to both the insider and outside attackers there making the system more safe and secure. But if attackers floods the system with bogus information. so part future work we will investigate on how to deal with this issue.
A.Singh,P.Sharma	2015	It is the responsibility of RSU to make the network available all the time to every node for secure communication of critical information. For this, network availability occurs as the major security requirement which may be exposed to several threats or attacks.	Enhanced Attack packet detection algorithm is more responsive and verification is done with lesser and has increased throughput's In, future intend to assign priority to emergency vehicles such as ambulance, fire extinguisher, etc to verify them in much less time as compared to other vehicles.
A. Quyoom, R. Ali and D. Gouttam	2016	In this paper, we proposed an Malicious and Irrelevant Packet Detection Algorithm (MIPDA) which is used to analyze and detect the Denial-of Service (DOS) attack.	In coming time they are going to apply this algorithm request sent and received from multiple vehicles at a time to analyze and detect the attacks in efficient and effective for secure environment.
R.S. Raw, M. Kumar and N. Singh	2013	We have also discussed some major attacks and solutions that can be implemented against these attacks.	Among all requirement and privacy are major issue in vanets.however confidentially is not requirde in the vanets generally packets on the network do not contain

			any confidential data.
S. Rehman ,T. Zia	2013	VANETs have now been established as reliable networks that vehicles use for communication purpose on highways or urban environments. Along with the benefits, there arise a large number of challenges in VANET such as provisioning of QoS, high connectivity,bandwidth and security to vehicle and individual privacy.	This paper preseneted an overview and tutorial of various issues in vanets .Various type of challenges
Dr.Ramaprabha ,V.Premalatha	2016	VANET turn every participating car into a wireless router or node, allowong cars approximately 100 to 300 meters of each other to connect and in turn create a network with a wide range.	In this paper we have done the absolute survey and discussed on vanet.The aim of this paper is to give an overview of vehicular ad hoc networks.
M. N. Mejri, N. Achir ,M. Hamdi	2016	In this paper we propose a reaction method against DOS attacks in VANET. In this method we have the choice between two proposed reaction games. Design methodology and defined metrics are inspired from game theory models.	The simulations showed the efficacy of our proposal measured by the performance of the obtained results. We evaluated our proposed game by simulation.we believe these contibutions to be very useful for solving the DOS attack reaction problem in VANETs.
N.lyamin, A.Vinel, M. Jonsson	2014	A method for real time detaction of denial of services attacks in IEEE 8021.11p vehicular ad hoc networks is proposed.	Our on goning work is focused on rellaxing the assumptions of the presented model and correspondingly enchancing the detection for realistic scenarios.
M.Boban,G. Misek	2008	We analyze some of the most important QoS metrics in VANET. Namely, we determine the upper performance bound for connection duration, packet delivery ratio, end-to-end delay, and jitter for unicast communication in typical highway and urban VANET environments.	The results also confirmed our initial assumptions regarding the locality of interest for applications in VANET communication over large area will not be possible without the use of infrastructure.

3. CONCLUSIONS

Due to decentralize architecture of vehicular AdHoc network many malicious nodes may join the network which is responsible to trigger various type of active and passive type of attacks. In the network various when some malicious nodes join the network and that nodes are responsible to trigger DOS type of attack which reduced network performance.In the recent times, various techniques for the detection and isolation of DOS attack is reviewed and discussed in terms of description, outcome. In the future technique will be proposed for the isolation of DOS attack in the network.

4. REFERENCES

[1] R.M. Pai, N. Ajam, J. Mouzna, “Mitigation of Insider and outside DOS attack against Signature based Authentication in VANETs’’,Asia-Pacific Conference on Computer Aided System Engineering, pp.152-157, IEEE 2014.

[2] R.S. Raw,M. Kumar, N. Singh,“Security challenges, Issues and Their Solution For VANET’’, International Joural of network,Volume.5,No.5,September 2013.

[3] M.A. Khan and T. Zia, “Vehicular Ad-Hoc Networks(VANETs)- Overview and Challenges’’, Journal of Wirelsess Networking and Communication,pp.29-36, 2013,

[4] Dr. Ramaprabha and V. Premalatha 2016,“Security challenges, Issues and Their Solution For VANET’’,International journal of Contemporay Research in computer Science and Technology ,Volume 2,pp.876-879, issue 7 july 2016.

[5] V. H. LA, A. CAVALLI,“Security attacks and solutionl in vehicular Ad Hoc network’’,International Journal of Network Security & Its Applications ,Volume. 4, No.2, April 2014.

[6] A. Quyoom, R. Ali, D. Nandan Gouttam, H.Sharma,“A Novel Mechanism of Detection of Denial of Service Attack in VANET using Malicious and Irrelevant Packet Detection Algorithm’’,International Conference on Computing Communication and Automation ,pp.414-419, IEEE 2015.

[7] A. Singh and P. Sharma,“A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm’’,International

Conference on Computing, Communication and Automation ,IEEE 21-22 December 2015.

[8] M. N. Mejri, N. Achir and M. Hamdi,"A New Security Games Based reaction algorithm Against DOS Attacks in VANETs",13th IEEE Annual Consumer Communications & Networking Conference, 2016.

[9] N. lyamin, A. Vinel , J. loo,"Real Time Deteactin of denial of services attacks in IEEE 802.11p vehcular network ",IEEE Commincation latter, Volume.18, No.1, pp.110-113, january 2014.

[10] D.Johnson, A. Menezes, S.Vanstone, "The Elliptic Curve Digital Signature Algorithm ", International Journal of Informatics Security, Volume 1,No. 1,pp. 36-63,2011.

[11] M. Boban, G. Misek, and K. Tonguz, "What is the Best Achievable QoS for Unicast Routing in VANETs", GLOBECOM Workshops, IEEE, pp.1-10, 4 November 2008

[12] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving", IEEE Transactions on Wireless Communications, Volume 7, pp. 4987-4998, December 2008.

[13] A. Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," IEEE International Conference on Communications , pp.1-5, May 2010.

[14] S. Manvi, M. Kakkasageri, and D. Adiga, "Message authentication in vehicular ad-hoc networks: ECDSA based approach," Future computer and Communication, International Conference ,pp.16-20, April 2009.