Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 8, August 2019, pg.29 – 35

Security Analysis of Vehicular Ad Hoc Networks

Krishna Pal Singh Solanki
M.Tech Scholar
kpss.pal@gmail.com
Sobhasaria Engineering College
Sikar

Anurag Sharma
Assistant Professor
anuragsharma333@gmail.com
Sobhasaria Engineering College
Sikar

Abstract: The wireless ad hoc network is the decentralized type of network and vehicular ad hoc network is the type of wireless networks. In the vehicular ad hoc network vehicles can move freely in the network with the variable speed. The security is the major issue of the network which reduces network performance. In this paper, various security issues related to vehicular ad hoc network is discussed and propose novel technique for the isolation of DDOS attack in VANETs
KEYWORDS: DDOS, VANETs, Hops, AODV

Introduction

A self-configuring type of network that provides vehicle to vehicle and vehicle to roadside communications is known as vehicular ad hoc network. The information is shared across the network through the nodes that represent themselves as servers or clients [1]. The computerized system comprises of various components such as computers, communications, and management technologies as well as the sensor and control innovations. The functioning of a transportation system can be improved by integrating these functions. The warnings related to environmental hazards, traffic and road conditions, and transmitting local information amongst vehicles is provided by using the Vehicular Ad-Hoc Networks [2]. If there is any such condition present where there is traffic jam, road closure or accident casualty the information can be spread across the network. This might help the drivers in avoiding the specific routes as well as saving the time. The vehicles spread the warnings across other vehicles through proper communication. There are vehicles as well as Road-Side Infrastructure units (RSUs) present in the VANETs. The vehicles are able to communicate with each other as well as with the RSUs using VANETs [3]. The RSUs are referred to as the fixed entities and the vehicles are considered as mobile entities. There can be one-hop communication amongst vehicles in VANETs or multi-hop communication in which the vehicles can act as routers and retransmit the messages. So, the vehicles can communicate directly with each other or can pass messages amongst a series of vehicles. The nature of the message is an important factor which determines the type of communication [4]. The one-hop communication can be provided if the vehicles wish to communicate on individual basis. In order to travel within the network, the node or vehicle needs to have a certificate which approves its participation in that network. The basic ad hoc routing protocols cannot be used adequately within the VANETs because of the change is configurations, the mobility patterns, the entering and leaving of various vehicles and various other reasons [5]. The utilization of least communication time while using minimum amount of network resources, is the major objective of routing protocols in VANETs. On the basis of the position accusation and route update technique, the VANETs routing protocols can be categorized [6]. A class of routing algorithm is provided within the position based routing in which the geographic positioning of information is shared amongst the nodes. This can help in choosing the next forwarding hops within the network. Within the clusters that are generated within the network, the cluster based routing protocols are used. The nodes that are similar will form clusters and one cluster head will be chosen which will help in broadcasting the packet to the cluster present. There is an occurrence of delay and overhead within the highly mobile VANETs even when there is high scalability of these networks. In order to share the traffic, weather and any emergency related information from the roads, the broadcasting routing is utilized within VANETs. The important information can be delivered and the announcements can be made amongst the vehicles through this protocol [7]. A location based multicasting routing which helps in delivering the packets from source node to the all other various nodes present in a geographical area is known as geo cast routing. The information related to the links which are present within the network is utilized by the topology based routing protocols. This is done in order to perform packet forwarding across the network. VANETs suffer from various attacks. Multiple messages are transmitted by the attacker to various vehicles within Sybil type of attack. Various sources of identity are present within every message present in the network. Wrong messages are sent by the attacker in order to jam the traffic by creating confusion to vehicles [8]. The vehicles are then forced to follow a next path in order to communicate with each other. Thus, mainly the generation of illusion of multiple vehicles so that they are forced to choose another route is the prior objective of the attacker. The information that is relevant to safety as well as non-safety of various applications is attacked mainly by the attacker in application type of attack. Warning messages are provided to users with the help of safety applications. The information present within actual message is altered by the attacker in this attack which results in sending wrong information to other vehicles [9].

Distributed Denial of Service Attack (DDOS ATTACK):
An attempt made by an attacker from different locations to stop legitimate users from accessing the required objects from the system is known as Distributed Denial of Service Attack (DDOS) attack. The attacks that are caused from various locations in distributed form by one attacker are known as DDOS attacks. The messages might be transmitted by the attacker within different time durations. On the basis of the vehicles presented by attacker, there is a difference in the nature as well as time duration within which the message is to be transmitted. There is a similar objective as of the DOS attack by this attacker [10]. There are different tools utilized within the DDoS attacks. The basic structure of the tools is same even though they have different names.

Literature Review

Mohamed Nidhal Mejri et al. (2015) [11] proposed a new detection mechanism which was known as Greedy Detection for Vehicular ad hoc Networks (GDVAN). This mechanism was proposed in order to detect the greedy behavior attacks that occur within the VANETs. There were mainly two phases involved within this proposed mechanism which were the suspicion phase as well as the decision phase. The proposed technique was executed by any node present in the network which was a major benefit of this proposed technique. There was no need to modify the IEEE 802.11p standard within this mechanism. With the help of various simulations and experiments the effectiveness and efficiency of the proposed method was computed which showed that the proposed algorithm outperformed the already existing techniques in terms of various performance parameters.

Pooja. B, et al. (2014) [12] presented in this paper that authentication was a fundamental structure for protected and secure correspondence of messages in VANETs. For mitigating the internal and external DOS attackers present within VANETs, a two phase method was proposed in this paper. Through the pair of private and public key, the HMAC signatures were calculated within the principal phase of this method. The comparisons were made with the threshold value for identifying the internal attacker with the help of number of invalid signatures that were flooded by the attacker within this phase. With the help of both internal and external attackers, the DOS attack was mitigated. The experiments were conducted here on the basis of which it is seen through the results that the proposed method performed better in detecting the DOS attack and also provided least computation overhead to the network.

Munazza Shabbir, et al. (2016) [13] presented in this paper that vehicular adhoc networks were turning into a mainstream and promising technology in the modern intelligent transportation world. According to the safety applications of VANETs any information circulating through the network can be life crucial. So the honesty of the information was a critical need. One of the significant attacks that exhaust the network by illegitimately utilizing the greater part of its assets was DDOS attack. In this sort of attack an attacker fakes different identities of nodes i-e utilizes spoofed IP addresses to exhaust the network by circulating bogus messages and making it deny to cater to legitimate solicitations for services. So before the proper deployment of this network practically its security needs should be met. In this paper a DDOS attack detection and after that prevention scheme was proposed.

Nirav J.Patel, et al. (2015) [14] studied in this paper that there was vehicle to vehicle communication provided over the vehicular ad hoc networks. There is a continuous change within the locations of the vehicles within VANETs. During the routing process, there was a need to provide secure routing in order to provide a mutual trust amongst the nodes present in the network. It was very difficult to trust the nodes present in the network as the route discovery or data transmission occurring within the network can be disrupted by these malicious nodes. In order to provide trust-based techniques within these networks, various researchers have proposed many studies. The enhancement of various ad hoc routing protocols had been reviewed in this paper, in order to study the secure the routing processes. On the basis of this review, the various enhancements to be made within the trust-based techniques were also understood.

Vinh Hoa LA, et al. (2014) [15] studied in this paper that there were numerous studies proposed by researchers in order to improve the VANETs. There were various attacks that occur which result in degrading the performance of these networks. Due to this, there was a huge loss observed in terms of time, money and the lives of users. The various types of attacks that can occur within these networks were surveyed in this paper. In order to prevent these networks from various types of attacks, various techniques are proposed which were also presented in this paper. All such techniques were classified into various categories on the basis of the methods used within them. In order to alert the system regarding the attacks arising, there was a need to introduce intrusion detector which is done here. The BRO or MMT tools were utilized here in order to identify the types of attacks that could possibly arise within these networks.

Kirti A. Yadav, et al. (2016) [16] reviewed in this paper the different types of routing protocols that are being applied in vehicular ad hoc networks. The security related scenario was to be generated through the presence of routing techniques within these systems. There was also a need to identify the need of providing security applications to the users involved here. The various security measures being provided in VANET are also studied in this paper. There was a successful achievement required for providing secure scenarios within the VANETs which was done through this survey. Within the security scenarios, there was a need to provide a future scope which could help in ensuring the security, availability as well as non-repudiation of the techniques. It was analyzed through this study that there was a need to provide enhancement in the intelligent transport system in order to provide higher level of secure environment within these networks.

Deepak Raghuvanshi, et al. (2013) [17] presented in this paper that within various applications related to research as well as technology, there is an important role played by the digital images. There was some degree of noise present within the digital images present within digital image processing technology. On the basis of nonlocal means (NL-means) algorithm, the image denoising method was proposed in this paper which was implemented on MATLAB simulator. There was a concept of self-similarity presented within the nonlocal means (NLM) algorithm. There was an aligned pixel within the image that was gathered from internet. Whereas, the image capture from digital media was not aligned properly. Various experiments were conducted in this paper and as per the results achieved it was seen that the performance of NL-means denoising technique is better in comparison to other existing techniques.

Wenshuang Liang, et al. (2015) [18] studied in this paper that there was been huge demand of VANET applications over the recent years. Due to their unique properties, these networks were been deployed both in academic as well as industrial applications. Through the view point of research, an overview of VANETs was presented in this paper. Initially, the most popular research issues being faced within VANETs had been presented in this paper. Further, the general research techniques were discussed in order to analyze the challenges as well as the future enhancements that could be made within these networks. This paper introduced the vehicular ad hoc networks from the research perspective, covers basic architecture, critical research issues, and general research methods of VANETs, and provided a comprehensive reference on vehicular ad hoc networks.

Table of Comparison

Author's Name	Year	Description	Outcomes
Mohamed Nidhal Mejri	2015	They proposed a new detection mechanism which was known as Greedy Detection for Vehicular ad hoc Networks (GDVAN).	With the help of various simulations and experiments the effectiveness and efficiency of the proposed method was computed which showed that the proposed algorithm outperformed the already existing techniques in terms of various performance parameters.
Pooja. B,	2014	For mitigating the internal and external DOS attackers present within VANETs, a two phase method was proposed in this paper.	The experiments were conducted here on the basis of which it is seen through the results that the proposed method performed better in detecting the DOS attack and also provided least computation overhead to the network.
Munazza Shabbir,	2016	In this paper a DDOS attack detection and after that prevention scheme was proposed.	The proposed technique was evaluated by making several comparisons with other already proposed techniques which showed that the proposed approach provided better security approach to prevent network from DDOS attack.
Nirav J.Patel,	2015	The enhancement of various ad hoc routing protocols had been reviewed in this paper, in order to study the secure the routing processes.	On the basis of this review, the various enhancements to be made within the trust-based techniques were also understood.
Vinh Hoa LA,	2014	In order to prevent these networks from various types of attacks, various techniques are proposed which were also presented in this paper.	The BRO or MMT tools were utilized here in order to identify the types of attacks that could possibly arise within these networks.
Kirti A. Yadav	2016	There was also a need to identify the need of providing security applications to the users involved here. The various security measures being provided in VANET are also studied in this paper.	It was analyzed through this study that there was a need to provide enhancement in the intelligent transport system in order to provide higher level of secure environment within these networks.
Deepak Raghuvanshi,	2013	On the basis of nonlocal means (NL-means) algorithm, the image denoising method was proposed in this paper which was implemented on MATLAB simulator.	Various experiments were conducted in this paper and as per the results achieved it was seen that the performance of NL-means denoising technique is better in comparison to other existing techniques.
Wenshuang Liang	2015	Through the view point of research, an overview of VANETs was presented in this paper.	This paper introduced the vehicular ad hoc networks from the research perspective, covers basic architecture, critical research issues, and general research methods of VANETs, and provided a comprehensive reference on vehicular ad hoc networks.

Inferences Drawn from Literature Review

Following are the inferences drawn from the literature review:

1. The vehicular ad hoc network is the decentralized type of network in which vehicular nodes can change their location any time due to which routing is the major issue which needs to get resolved.

2. The vehicular nodes can join or leave the network as per their requirement due to the self-configuring nature of these networks. The malicious nodes enter network and trigger active as well as passive attacks within these networks. A security framework is required which can secure the vehicular ad hoc network.

3. The DDOS attack is the active type of attack which is very easy to detect but difficult to defend due to its dynamic nature. In the previous research no efficient technique is proposed which can detect malicious node in minimal time.

4. According to literature survey, techniques are required which detect malicious nodes from the network which are responsible to find the nodes which spoof credentials of the legitimate node to trigger DDOS attack in the network.

Proposed Work

In this research work, the technique will be proposed which can detect and isolate malicious nodes from the network which are responsible to trigger DDoS attack. The DDoS attack is the denial of service type of attack in which malicious node can select some of the nodes which can flood victim node with raw packets. In this work, mutual authentication technique will be proposed for the detection of malicious nodes from the network. The nodes which are not able to prove their identity will be detected as malicious nodes from the network.

Methodology

In the work, technique will be proposed which will detect malicious nodes from the network and to detect malicious nodes following are the steps which will be followed:-

1. In the first step, the network will be deployed with the finite number of vehicle nodes. The fixed bandwidth will be allocated to each vehicle node in the network.

2. The road side units will start analyzing the bandwidth consumption of each vehicle node and node which will use the bandwidth above allocated value will be the malicious node.

3. In the third step, the road side units will check the type of packets the node is sending which is using the bandwidth above the allocated value. When the node will send the data packets to the victim node, it may be the malicious node.

4. In the last step, the nodes which will send the malicious data packets, if that node will receive control packets from any node then that node will be detected as the malicious node which will be responsible to trigger DDOS attack.

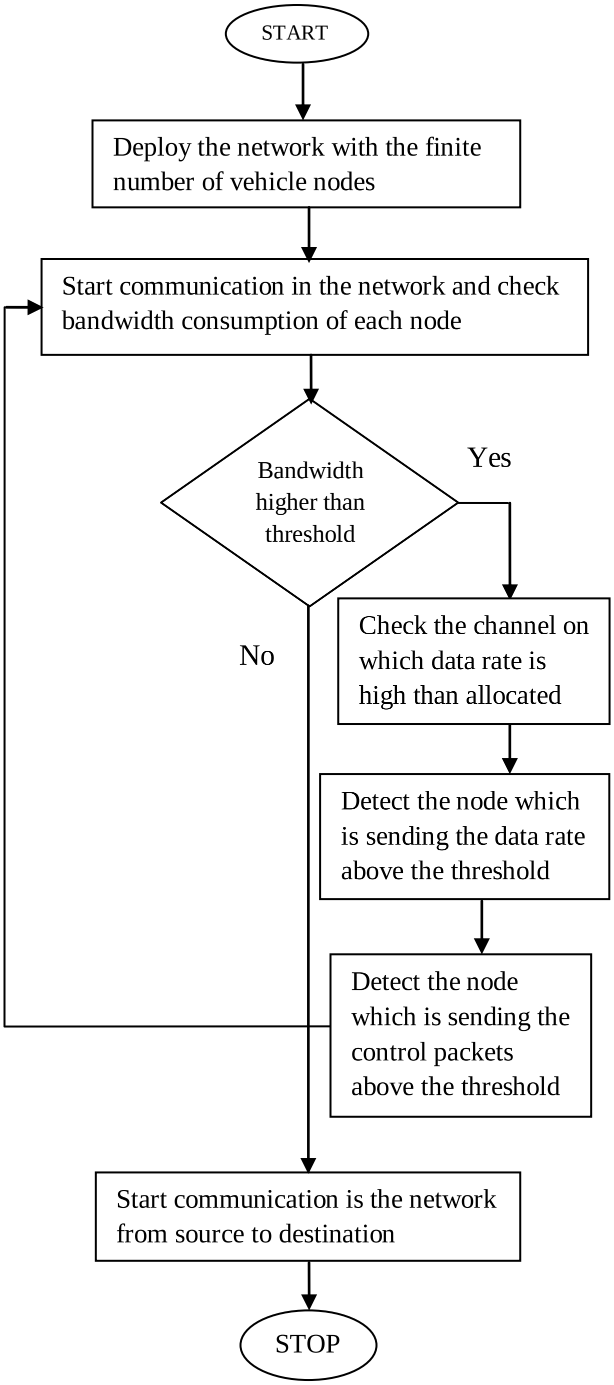
START
Deploy the network with the finite number of vehicle nodes
Start communication in the network and check bandwidth consumption of each node
Bandwidth higher than threshold
Yes
No
Check the channel on which data rate is high than allocated
Detect the node which is sending the data rate above the threshold
Detect the node which is sending the control packets above the threshold
Start communication is the network from source to destination
STOP

Fig 1: Proposed Threshold Flowchart

Conclusion

In this work, it is concluded that vehicular ad hoc network is the decentralized type of network in which vehicle nodes join or leave the network when they want. Due to such nature of the network security is the major issue which needs to get resolve. In this paper, technique is proposed which isolate malicious nodes from the network which are responsible to trigger DDOS attack.

References

[1] A.Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," IEEE Wireless On-demand Network Systems and Services, St. Moritz, Switzerland, volume no. 8, issue 3, pp. 32–41, 2005.

[2] M. Li, Z. Yang and W. Lou, "CodeOn: Cooperative Popular Content Distribution for Vehicular Networks using Symbol Level Network Coding," IEEE Journal on Selected Areas in Communication., volume 29,issue 8 , pp. 223-235, 2011.

[3] B.Ayyappan and Dr. P.Mohan kumar,"Vehicular Ad Hoc Networks (VANET): Architectures, Methodologies And Design Issues," IEEE International Conference on Science Technology Engineering and Management (ICONSTEM), volume 95, issue 12, pp. 2299-2313, 2016.

[4] P. Muhlethaler and A. Laouiti, "Vehicle Ad Hoc Networks: Applications And Related Technical Issues", IEEE Communications Surveys & Tutorials , volume 4, issue 15, pp- 231-240, 2008.

[5] Neha Goel,Gaurav Sharma," A Study of Position Based VANET Routing Protocols", International Conference on Computing, Communication and Automation (ICCCA), volume 12, issue 3, pp. 541-550, 2016.

[6] Kanza Bayad, "Comparative Study of Topology-based Routing Protocols in Vehicular ad hoc Network using IEEE802.11p," IEEE International Conference on Electrical and Information Technologies , volume 5, issue 2, pp. 1015–1020, 2016.

[7] Ravendra Kumar Sharma ; Sushil Kumar Saroj, "Sybil attack prevention and detection in vehicular ad hoc network", IEEE International conference on Computing Communication and Automation , volume 4, issue 2, pp- 152-163, 2016.

[8] S Michael, M Imad, " Spatial Distribution And Channel Quality Adaptive Protocol For Multihop Wireless Broadcast Routing In VANET", IEEE Transaction of Mobile Computing volume 12, issue 4, pp- 722–734, 2013.

[9] SY Ni, YC Tseng, YS Chen, JP Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network, Wireless Networks", volume 8, issue 3, pp.153–167, 2002.

[10] S Panichpapiboon, W Pattara-atikom,"A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks", Communications Surveys & Tutorials IEEE volume 13, issue 99, pp- 1–15, 2011.

[11] Mohamed Nidhal Mejri and Jalel Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm For VANETs", Journal Of IEEE Transaction On Mobile Computing, volume 4, issue 7, pp- 53-62, 2016.

[12] Pooja. B, Manohara Pai M.M, Radhika M Pai, Nabil Ajam, Joseph Mouzna, " Mitigation of the Insider and Outsider DoS attack against the Signature Based Authentication in VANETs", IEEE Computer Aided System Engineering , volume 15, issue 2, pp- 639-645, 2014.

[13] Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, Nazar A. Saqib, " Detection and Prevention of Distributed Denial of Service Attacks in VANETs", IEEE Computational Science and Computational Intelligence , volume 8, issue 14, pp- 123-129, 2016.

[14] Nivraj J.Patel, Rutvij H.Jhaveri, "Trust based approaches for secure routing in VANET: A Survey", ELSEVIER, volume 19, issue 71, pp- 194-203, 2015.

[15] Vinh Hoa La, Ana Cavalli, "Security Attacks And Solutions In Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems, volume 4, Issue 6, pp- 48-55, 2014.

[16] Kirti A. Yadav and P. Vijayakumar, "VANET and its Security Aspects: A Review", Indian Journal of Science and Technology, volume 9, Issue 18, pp- 104-118, 2016.

[17] Deepak Raghuvanshi, Deepak Jain, Pankaj jain," Performance Analysis of Non Local Means Algorithm for Denoising of Digital Images", International Journal of Advanced Research in Computer Science and Software Engineering , volume 3, Issue 11, pp- 551-558, 2013.

[18] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends", International Journal of Distributed Sensor Networks, volume 16, issue 3, pp- 819-824, 2015.