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. 5, May 2019, pg.51 – 55

A Review Paper on Analysis of Security Techniques of VANET

Aaditya Barak
Research Scholar
University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak
aaditya.barak5@gmail.com

Vikas Sindhu
Assistant Professor
University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak
vikassindhu7@gmail.com

Abstract: The vehicular ad hoc network is the decentralized type of network in which vehicles can join or leave the network when want. In such type of network routing, security are the major issues which affect network security. The security attacks are classified into active and passive. The various security algorithms are designed to increase security of the network. The DDOS attack is the active type of attack which reduces network performance to great extent. In this paper, various techniques are analyzed for the isolation of DDOS attack are reviewed.
Keywords: DDOS, VANET, Active and Passive

Introduction

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 here by integrating these functions. The warnings related to environmental hazards, traffic and road conditions, and transmitting local information amongst vehicles is provided using the Vehicular Ad-Hoc Networks. 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 which might help the driver in avoiding the specific route as well as saving the time. The vehicles spread the warnings across the other vehicles through proper communication [1]. In case of emergency situations, the VANETs have proved to be beneficial due to their easy configuration as well as quick deployment. For asking any kind of help from other vehicles, a vehicle can send messages to other vehicles and can also inform the concerned authorities regarding problems they are facing on that road. For offering convenience and providing road safety VANETs are used in almost all areas [2]. It is however, to be made sure that

there are no invalid messages being sent across the network and the network is not being utilized in a malicious way. There is a possible situation to be present within the network in which the vehicles whose permanent identity is known can travel with low fuel reserve and ask for help. 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. The RSUs are referred to as the fixed entities as well as the mobile entities are the vehicles. There can be one-hop communication amongst vehicles in VANETs or multi-hop in which the vehicles can act as routers and retransmit the messages [3]. So, here the vehicles can communicate directly with each other of can pass messages amongst a series of vehicles. The nature of the message is an important factor which determines the type of communication. The one-hop communication can be provided if the vehicles wish to communicate on individual basis. If the vehicle requires a certificate authority (CA) to travel along with it, a message is broadcasted and [assed across the network. This stops once the RSU is reached and this type of communication is known as multi-hop type of communication. There are 3 domains in which the architecture of VANET is divided. They are In Vehicle domain, ad-Hoc Domain and the Infrastructure Domain. Within the In-Vehicle domain, the On-Board Unit (OBU) and the Application Units (AUs) are present [4]. When interacting with the OBU, the AUs perform various functions as they are the user devices. The ad hoc network comprises of the OBU's which are present in the vehicles as well as the RSUs which are present along the roadside. When within a proper range, the OBUs and RSUs easily communicate with each other in a wireless manner. An ad hoc domain is formed as the vehicles connect to RSUs in an ad hoc manner according to their requirements. There are RSUs and CA present within the Infrastructure Domain. There is a connection between the CA and the RSU. The RSU here acts as a proxy for the CA. When the packet is to be forwarded from one OBU to another, the multi-hop communication is required in between the OBUs and the RSUs which will help them reach the RSU [5]. The information related to link is used within the network for transferring the packets from source to destination in the case of topology based routing protocols. There are three broader classifications of these protocols. On the basis of shortest path algorithms most of the proactive routing protocols are built. All the information gathered from various nodes is kept in the form of tables as they are table-based [6]. The tables created are shared amongst the neighbors and in case any changes occur, each node updates its routing table as per those changes. The overhead which is created by the proactive routing protocols is overcome by the on-demand or reactive routing protocols. Only the routes which are currently active are maintained here using this type of protocol. The characteristics of both reactive as well as proactive routing protocols are combined in the case of hybrid routing protocols. This helps in providing more scalable and efficient routing protocols [7]. The protocols involved in the hybrid category are mainly zone based which means that the number of nodes are divided into various zones for making route discovery and providing a reliable maintenance. The disadvantages observed in the proactive and reactive routing protocols are removed here by proposing new hybrid protocols. VANET suffer from various attacks [8]. Denial of Service Attack is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user. Sybil Attack is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity. It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route. The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicles so that vehicles can choose another route [9]. In vehicular network each vehicle has unique identifier which is used to verify the messages whenever the accident occurs by sending the wrong messages to other vehicles which causes Node Impersonation Attack. In Application Attack, the main motive of attacker is to content that are related to safety and non-safety related applications. Safety applications play very important role as they provide warning messages to other users [10]. In this attack the attackers alter the contents of the actual message and send wrong messages to other users. A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from utilizing the desired assets.

Literature Review

Mohamed Nidhal Mejri et.al (2015) [11] proposed in this paper a new detection mechanism which is known as Greedy Detection for Vehicular ad hoc Networks (GDVAN). This mechanism is proposed in order to detect the greedy behavior attacks that occur within the VANETs. There are mainly two phases involved within this proposed mechanism which are the suspicion phase as well as the decision phase. This technique is considered as passive technique. The proposed technique can be executed by any node present in the network which is a major benefit of this proposed technique. There is 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 is computed which shows that the proposed algorithm outperforms the already existing techniques in terms of various performance parameters.

Pooja. B, et.al, (2014) [12] presented in this paper that authentication is a fundamental structure for protected and secure correspondence of messages in VANETs. For authenticating messages the IEEE 1609.2 standard uses ECDSA as the standard digital signature calculation. As just authentic users can compute the HMAC signature, DoS attack due to outside attackers is mitigated. On the off chance that the entity is authentic and subjects other vehicle to DoS attack, the second phase is designed to detect the insider attackers. In this phase based on the number of invalid signatures flooded by the attacker, it is compared against a threshold value to identify the inside attacker. Subsequently DoS attack is mitigated due to inside and also outside attackers. Test results show that the proposed scheme alleviates DoS attack as well as performs better with negligible computational overhead.

Munazza Shabbir, et.al, (2016) [13] presented in this paper that vehicular adhoc networks are 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 is a critical need. One of the significant attacks that exhausts the network by illegitimately utilizing the greater part of its assets is 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 is proposed.

Nirav J.Patel, et.al, (2015) [14] studied in this paper that the vehicular Ad-hoc networks (VANETs) require trusted vehicles to vehicles communication. VANET is multidimensional network in which the vehicles continuously change their locations. Secure routing is imperative during the routing process to incorporate mutual trust between these nodes. Most of the time, the fake information is broadcast by the malicious node among other nodes. As the malicious nodes attempt to disrupt route discovery or data transmission in the network in that case establishing the trust is become very challenging. Number of researchers is working on secure routing process with trust-based approaches. In this paper a survey of various mechanisms is presented to improve different ad-hoc routing protocols for secure routing process by enhancing the trust among different nodes in VANETs.

Vinh Hoa LA, et.al, (2014) [15] studied in this paper that the vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most attractive topics for researchers and automotive industries due to their tremendous potential to improve traffic safety, efficiency and other added services. Still, VANETs are themselves exposed against attacks that can directly lead to the corruption of networks and it will result in big losses of time, money, and even lives. In this paper a survey have been done on different attacks in VANETs and their solutions by carefully considering other similar works as well as new attacks have been updated and categorized them into different classes. In this perspectives, there is need to construct an intrusion detector for VANETs to alert the attacks in the case performing. This work can be done by applying the system of BRO or MMT tools in considering properties that is possibly collected in attacks.

Kirti A. Yadav, et.al, (2016) [16] reviewed in this paper the research on various routing protocols used in Vehicular Adhoc Network (VANET), with the aim to examine the newly emerged routing strategies. The proposed method also needs to investigate the research direction for security in VANET. Two major aspects have been focused in this paper first is literature survey and other is review along with a conceptual analysis of VANET security aspects. The survey of this paper indicates successful accomplishment of all aspects the security aspect for VANET secured communication requires successful accomplishment of all aspects. The recent survey concludes that there is still further scope for research in security aspects like integrity, non-repudiation, availability. Application/Improvements: This study tries to suggest that understanding the approach of routing and will help to implement a better intelligent transport system with security.

Wenshuang Liang, et.al, (2015) [17] studied the overview of the main aspects of VANETs from a research perspective. In this paper firstly basic architecture of networks have been given, then three popular research issues and general research

methods have been discussed, and ends up with the analysis on challenges and future trends of VANETs. In this paper there is an introduction of the VANETs architecture, including network components, communication types, and layered network architecture. This paper also focuses on VANETs research methodologies and some mobility models and simulator tools are also given. Finally, they provide an analysis on VANETs research challenges and future trends. This paper introduces the vehicular ad hoc networks from the research perspective, covers basic architecture, critical research issues, and general research methods of VANETs, and provides a comprehensive reference on vehicular ad hoc networks.

Bassem Mokhtar, et.al, (2015) [18] presented in this paper that Vehicular Ad hoc networks are special case of ad hoc networks that, besides lacking infrastructure, communicating entities move with various accelerations. Accordingly, this impedes establishing reliable end-to-end communication paths and having efficient data transfer. Thus, there are different network concerns and security challenges in VANETs to get the availability of ubiquitous connectivity, secure communications, and reputation management systems which affect the trust in cooperation and negotiation between mobile networking entities. In this survey paper different main concerns of VANET have been discussed, such as security features, challenges, and attacks of VANETs, and due to different network layers we classify the security attacks of VANETs.

Table of Comparison

Authors Names	Year	Description	Outcomes
Mohamed Nidhal Mejri	2015	A new detection mechanism was proposed which is known as Greedy Detection for Vehicular ad hoc Networks (GDVAN).	The effectiveness and efficiency of the proposed method is computed which shows that the proposed algorithm outperforms the already existing techniques in terms of various performance parameters.
Pooja. B,	2014	As just authentic users can compute the HMAC signature, DoS attack due to outside attackers is mitigated.	Test results show that the proposed scheme alleviates DoS attack as well as performs better with negligible computational overhead.
Munazza Shabbir,	2016	In this paper a DDOS attack detection and after that prevention scheme is proposed.	Improvements in accurate detection of attacks were achieved in this research.
Nirav J.Patel,	2014	In this paper a survey of various mechanisms is presented to improve different ad-hoc routing protocols for secure routing process by enhancing the trust among different nodes in VANETs.	The review showed the extensive results which could possibly be achieved when using certain techniques.
Vinh Hoa LA,	2014	In this paper a survey have been done on different attacks in VANETs and their solutions by carefully considering other similar works as well as new attacks have been updated and categorized them into different classes.	This work can be done by applying the system of BRO or MMT tools in considering properties that is possibly collected in attacks.
Kirti A. Yadav,	2016	The research on various routing protocols used in Vehicular Adhoc Network (VANET) was reviewed with the aim to examine the newly emerged routing strategies.	The survey of this paper indicates successful accomplishment of all aspects the security aspect for VANET secured communication requires successful accomplishment of all aspects.
Wenshuang Liang,	2015	In this paper, basic architecture of networks have been given, then three popular research issues and general research methods have been discussed, and ends up with the analysis on challenges and future trends of VANETs.	This paper introduces the vehicular ad hoc networks from the research perspective, covers basic architecture, critical research issues, and general research methods of VANETs, and provides a comprehensive reference on vehicular ad hoc networks.
Bassem Mokhtar,	2015	In this survey paper different main concerns of VANET have been discussed, such as security features, challenges, and attacks of VANETs.	Due to different network layers, the security attacks of VANETs are categorized.

Conclusion

In this work, it is concluded that vehicular ad hoc network is the decentralized type of network in which vehicles can join or leave the network. The malicious nodes enter the network which triggers various type of active and passive attacks. The DDOS attack is the active type of attack which affects network performance. The designed techniques for the isolation of DDOS attack is reviewed in this work. In future novel approach will be designed which detect and isolation DDOS attack in VANET.

References

[1] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," IEEE WONS, volume no. 8, issue 3, pp. 32–41, St. Moritz, Switzerland, 2005.
[2] M. Li, Z. Yang and W. Lou, "CodeOn: Cooperative Popular Content Distribution for Vehicular Networks using Symbol Level Network Coding," IEEE J. Sel. Areas Commun., vol. 29, no. 1, pp. 223-235, 2011.
[3] A. Duel-Hallen, "Fading Channel Prediction for Mobile Radio Adaptive Transmission Systems," IEEE, vol. 95, no. 12, pp. 2299-2313, 2007
[4] S. Haykin and B. Widrow, "Parameter estimation methods," Adaptive and Learning Systems for Signal Processing Communications and Control, Hoboken, NJ: Wiley, volume 4, issue 15, pp- 231-240, 2003.
[5] Hayes, Monson H," Statistical Digital Signal processing and Modeling", Hoboken, NJ: Wiley, vol 12, iss 3, pp. 541-550, 1996.
[6] W. P. Siriwongpairat, T. Himsoon, W. Su, and J. R. K. Liu, "Optimum threshold-selection relaying for decode-and-forward cooperation protocol," Proc. IEEE WCNC, volume 5, issue 2, pp. 1015–1020, 2006.
[7] W Shangguang, F Cunqun, H Ching-Hsien, S Qibo, Y Fangchun," A Vertical Handoff Method via Self-selection Decision Tree for Internet of Vehicles," IEEE System Journal, volume 6, issue 1, pp- 152-163, 2014.
[8] S Michael, M Imad," Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET", IEEE Trans Mobile Comput volume 12, issue 4, 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 Pani\chpapiboon, 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, 2015.
[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, 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, 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", Ijans, Vol.4, Iss. 6, pp- 48-55, 2014.
[16] Rakesh Kumar and Mayank Dave," A Review of Various VANET Data Dissemination Protocols", IJOU, vol.5, Iss. 18, pp- 104-118, 2010.
[17] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie," Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends", IJDSN, volume 16, issue 3, pp- 819-824, 2015.
[18] Bassem Mokhtar, Mohamed Azab," Survey on Security Issues in Vehicular Ad Hoc Networks, ELSEVIER, Vol 5, issue 2, pp- 932-940, 2015.

