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.187 – 192

Analysis of Sybil Attack Isolation Technique in VANET

Sudha
Research Scholar**,** Swami Devi Dyal Institute of Engineering and Technology, Barwala, Haryana, India
sidkkr27@gmail.com

Mr. Kamal Kumar
Head of Department**,** Swami Devi Dyal Institute of Engineering and Technology, Barwala, Haryana, India
kamalkumar2661987@gmail.com

Dr. Rahul Malhotra
Director Principal**,** Swami Devi Dyal Institute of Engineering and Technology, Barwala, Haryana, India
director@sddgpi.com

Abstract: The vehicular ad hoc network is the decentralized type of network in which vehicle nodes can join or leave the network when they want. The vehicular network is much vulnerable to security attacks which affect network performance. The active attacks are those which reduce network performance in terms of certain parameters. This paper is related to Sybil attack. The techniques which are proposed for the isolation of Sybil attack is reviewed and analyzed in this paper. The techniques are implemented in the network simulators and results are analyzed in terms of certain parameters.
Keywords: Sybil attack, AODV, VANET, Active Attack

Introduction

The Vehicular ad hoc networks are the most prominent research area for the research purposes due to their increase in demand of usage. The vehicles and the elements that are present at the roadside are connected to each other for the purpose of communication and this network is self-configuring in nature. They do not require any fixed infrastructure for them. The transferring and receiving of the information back and forth holds the current traffic conditions of the network. Wi-Fi is the new latest technology used for the purpose of initiating the implementation of vehicular ad hoc networks. For the purpose of communication in VANETs the new Dedicated Short-Range Communication (DSRC) method is proposed [1]. The low latency and high data rate is ensured with the usage of this technique as it provides the short and medium range communications within it. The organizations which are build up in a certain building with less distances, the communication channels are changed more recently, and also the time provided to connect to the vehicles is less use this kind of techniques. With the absence of an automatic intelligent design for building an efficient protocol configuration in VANETs is not

possible. It is due to the fact that there are many problems (NP-problems) arising with it. The areas where highly dynamic topologies and less coverage areas are to be considered, there are various design issues which need to be taken care of [2]. A network in which all the vehicles are represented as the nodes of the network is known as the vehicular ad hoc network. These network communications are built to ensure the network safety and comfort for the driver. An intelligent transport system is provided for the purpose of establishing a vehicular ad hoc network which is anyhow a subset of the mobile ad hoc networks. The vehicles find it very beneficial and so for the purpose of ensuring safety all the vehicles must be provided with this facility [3]. The vehicles and the elements present on the roadside are provided with a wireless communication network. The properties of this network also involve its autonomous nature as well as the self-organizing wireless communication network. For the purpose of exchanging or sharing the information, the nodes present in the VANET act as servers or clients on their own [4]. There are three different categories of the VANET architecture which are pure cellular, pure ad hoc and hybrid. When the topology of the network is changed or there are highly moving nodes or vehicles present in the system, the routing mechanism in VANET is very difficult to perform. A greedy position based routing approach known as the Edge Node Based Greedy Routing (EBGR) is used for the purpose of forwarding the packets to the nodes. These nodes are available in the edge of the transmission range of the source or the forwarding node [5]. On the basis of the potential score of the nearest node, the most appropriate next hop is appointed. There is a minimization of the end to end delay of the packet transmission in the results when compared to the current routing protocols of the VANET. The affect of the traffic lights is measured with the help of the delay-bounded routing protocol. During the crossing of a vehicle through an intersection, the information about the traffic lights is gathered, Along with this, the information related to the traffic load of the road present in the next section is provided [6]. This helps in providing a more accurate assumption regarding the vehicles and the message deliverance in a strategic manner. There is a better usage of the time and a reduction in use of the radio resources which are needed to deliver the message within the time according to the simulation results achieved. For the purpose of assuming the available time and the distance travelled, the linear regression technique is used by the protocol. At a certain moment, there can be switching provided to the delivery strategy which will help in reducing the number of relays by radio [7]. There are two schemes of this protocols used. VANETs security is violated by various types of attacks. The attack occurs when a single node keeps sending multiple messages to other nodes which are pretended to be from different identities [8]. In most of the cases, Sybil attack is possible. It can only be exempted from the extreme conditions and assumptions of chances of resource parity and coordination amongst the entities. A type of confusion occurs in the whole network when a single node starts sending multiple copies of it selves. There is a chance that all the illegal, fake ID's and the authority are claimed. The collision within the network starts beginning which results in causing Sybil attack in the network. Both internal and external attacks can be triggered in this type of attack. [9] However, the external attacks can be avoided by providing authenticities measures. This is not possible with the internal attacks. The identity and entity within a network have one to one mapping. Various messages present in the network are spammed by the attacker in this type of attack. This results in using more bandwidth which further results in increasing the latency of the network [10]. The group user is sent numerous messages by the attackers which have no relation with their work and just help in increasing the load of the network. For the routers which are present in the flooding based protocol, the requests which are to be received here are sent to the attacker directly. A reply for the short node to the destination of a route is created by the attacker once it receives a message. The reply enters the gateway for performing some actions on the packets passing in between them [11]. A gray-hole attack is basically the extension of black-hole attack. In this, the source and monitoring systems are handled using partial forwarding. The selective data packet dropping method is presented as a normal node and this node participates in communication [12]. A node that can behave in a complete normal manner and switch to behaving like black hole which is actually an attacker, is known as a gray hole node. This gray hole node will behave completely normal and so it is difficult to identify the attacker.

Literature Review

Hamid Hamed, et.al (2018) proposed a novel approach to detect Sybil attacks. Further, based on the RSUs support, the attackers in VANETs were also aimed to be detected by this research [13]. It is considered to be very rare that the two vehicles pass by multiple RSUs at similar time duration due to the differences of moving dynamics among vehicles. For determining if the Sybil attack occurred or not, two facts were utilized. For detecting the attackers, the proposed mechanism used routine communications among the nodes and RSUs. It was seen through the simulation results achieved that the

proposed system outperformed the existing solutions in terms of various parameters like false positive rate, system requirements as well as detection rate.

D. Srinivas Reddy, et.al (2017) proposed a robust secure mechanism for establishing the faith among several participating entities which was named as cryptographic digital signature [14]. The proposed technique detected the Sybil attacks successfully from the network. Further, the time of vehicle ID was also verified using hash function and XOR operation. So, it was important to revise and extend the efficient communication mechanisms. To design more robust and secured routing protocols and cryptographic techniques within several mobility conditions, the proposed approach was aimed to be extended in future.

Chea Sowattana, et.al (2017) proposed novel mechanism using neighbourhood information. This was known as a distributed detection method [15]. Here, if the position of node was within the intersected region of two communication nodes but no acknowledge was sent to any one of them, a node was considered as Sybil node. Each receiver node's neighbour is voted to be Sybil or not by each other neighbour using the information received related to that neighbour. With respect to the detection rate and false positive rate, the simulations of proposed approach were evaluated in this research. It was seen that with the increase in number of surrounding neighbours, the detection rate was also increased.

Supinder Kaur, et.al (2016) presented a study which discussed the Sybil attack and its impacts caused on VANETs [16]. These networks are highly prone to several kinds of attacks that are triggered by the malicious nodes. This paper aimed to improve the efficiency of VCWC protocol. The wireless communication was made unreliable and the challenges of application were supported by this proposed protocol. Various papers which present the influences of attacks in VANET are reviewed in this study. However, the occurrence of Sybil attack and its effects on the networks were discussed in detail in this review. This study helped in highlighting certain key features of Sybil attack in VANETs.

Anu S Lal, et.al (2015) presented a study in which the basic applications of VANET were highlighted. The VANETs faced two major issues which were related to their security and privacy [17]. To detect Sybil attacks from cooperation of a central authority and RSUs, an improvement in the CP2DAP mechanism was proposed. A collaborative mechanism through which Sybil attacks could be detected was proposed by modifying the hybrid approach. Further, for preventing additional attacks from malicious vehicles, a revocation method was proposed using blossom channel. The disclosure of identity was not needed by the vehicle for detecting Sybil attack. Thus, the privacy was presented.

Ashritha M, et.al (2015) presented that the two major concerns of VANETs are security and privacy. Sybil attacks are very commonly found within these networks which directly affect the privacy of safeguarding mechanisms. This paper aimed to design a secure communication system among the vehicle to RSU and vehicle to vehicle using a hybrid authentication mechanism [18]. There is reduction in the rate of authenticated vehicles with the increment in speed of vehicles as per the second scenario. Faster authentication system and secure routing protocol could be proposed in future for improving the security of system to a greater extent.

Mahdiyeh Alimohammadi et.al (2015) studied that several analysts have been focusing on the latest applications of VANET [19]. Within V2V communications of VANET, a secure protocol was proposed as hybrid approach to unravel the two clashing goals of privacy and prevent Sybil attack from harming the network. The batch verification and Boneh-Shacham (BS) short gathering signature scheme were integrated to design a hybrid protocol. It was seen through the experimental results that for V2V communications of VANETS, reliable privacy and detection of Sybil attack were ensured when implementing the proposed mechanism.

Sebastian Bittl, Arturo A. et.al (2015) proposed an analysis of VANET attacks which aimed to spoof the time information. Extreme difference against the administration attacks was seen in case of this attack [20]. The possibility of misusing authentication features was offered by such attacks with the aim of violating the non-repudiation feature of the security mechanism. This research also discussed the methods which could help restrain the effects of security deformities arising in

these networks. A current Car2X mechanism was provided as a hardware solution in order to evaluate the possibility of these attacks to occur in VANETs such that further security measures could be taken.

Khaled Rabieh, et.al, (2015) proposed a novel cross-layer mechanism such that the Sybil vehicles present in the networks could be identified by RSUs [21]. Checking the locations of vehicles was the most important step of this proposed approach since these vehicles do not exist in the locations they claim. For detecting the presence of a Sybil vehicle, a challenge packet was sent to the location claimed by the vehicle with the help of directional antenna. A few Sybil attack alarming mechanisms were also discussed in this research. High detection rate with low probability of false alarm was achieved as per the evaluation results achieved when performing simulations using proposed approach. Further, computation overhead and acceptable communication were needed by this research.

Table of Comparison

Authors' Names	Year	Description	Outcomes
Hamid Hamed,	2018	A novel approach was proposed to detect Sybil attacks. Further, based on the RSUs support, the attackers in VANETs were also aimed to be detected by this research.	It was seen through the simulation results achieved that the proposed system outperformed the existing solutions in terms of various parameters like false positive rate, system requirements as well as detection rate.
D. Srinivas Reddy	2017	A robust secure mechanism was proposed for establishing the faith among several participating entities which was named as cryptographic digital signature.	To design more robust and secured routing protocols and cryptographic techniques within several mobility conditions, the proposed approach was aimed to be extended in future.
Chea Sowattana,	2017	Novel mechanism was proposed using neighborhood information. This was known as a distributed detection method	It was seen that with the increase in number of surrounding neighbors, the detection rate was also increased.
Supinder Kaur,	2016	This paper aimed to improve the efficiency of VCWC protocol. The wireless communication was made unreliable and the challenges of application were supported by this proposed protocol.	This study helped in highlighting certain key features of Sybil attack in VANETs.
Anu S Lal,	2015	To detect Sybil attacks from cooperation of a central authority and RSUs, an improvement in the CP2DAP mechanism was proposed.	The disclosure of identity was not needed by the vehicle for detecting Sybil attack. Thus, the privacy was presented.
Ashritha M,	2015	This paper aimed to design a secure communication system among the vehicle to RSU and vehicle to vehicle using a hybrid authentication mechanism.	Faster authentication system and secure routing protocol could be proposed in future for improving the security of system to a greater extent.
Mahdiyeh Alimohammadi	2015	Within V2V communications of VANET, a secure protocol was proposed as hybrid approach to unravel the two clashing goals of privacy and prevent Sybil attack from harming the network.	It was seen through the experimental results that for V2V communications of VANETS, reliable privacy and detection of Sybil attack were ensured when implementing the proposed mechanism.
Sebastian Bittl, Arturo A.	2015	The possibility of misusing authentication features was offered by such attacks with the aim of violating the non-repudiation feature of the security mechanism.	A current Car2X mechanism was provided as a hardware solution in order to evaluate the possibility of these attacks to occur in VANETs such that further security measures could be taken.
Khaled Rabieh,	2015	A novel cross-layer mechanism was proposed such that the Sybil vehicles present in the networks could be identified by RSUs.	High detection rate with low probability of false alarm was achieved as per the evaluation results achieved when performing simulations using proposed approach.

Conclusion

In this work, it is concluded vehicle ad hoc network is the self configuring network in which various type of security attacks are possible in the network. The attacks are divided into active and passive attacks. The Sybil attack is the active type of attack which affects network performance. The technique of Sybil attack isolation is analyzed in this research work. In future, novel approach will be proposed which isolate Sybil attack in the network.

References

[1] Adil Mudasir Mala and Ravi kant sahu, "Security Attack with an Effective Solution for DOS attack in VANET", 2013, International Journal of Computer Applications (0975 – 8887), Volume 66– No.22, pp- 1372-1380

[2] Ajay Rawat, Santosh Sharma, Rama Sushil, "VANET: Security Attack and its Possible Solutions", 2012, Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-301-304

[3] Jeong-Ah Jang, "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-of-Sight and/or Traffic-Violation-Prone Environment", 2012, IEEE Transactions on Intelligent Transportation Systems, Volume 13, Issue 4, pp 1-11

[4] Rakesh Kumar, Mayank, "A Comparative Study of Various Routing Protocols in VANET", 2011, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, pp- 643-648

[5] Reena Didcach, "Mobility simulation of Reactive protocol for VANET", 2012, Proceedings published by International Journal of Computer Applications, (IJCA), volume 32, issue 45, pp- 57-61

[6] Parastoo Kafil, Mahmoud Fathy, Mina Zolfy Lighvan, "Modeling Sybil Attacker Behavior in VANETs", 2012 9th International ISC Conference on Information Security and Cryptology, volume 72, issue 26, pp- 3842-3949

[7] Hao Wu, "An Empirical Study of Short Range Communications for Vehicles", 2011, IJSER Cologne, Germany, volume 66, issue 92, pp 83-84

[8] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X., "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks", 2011, IEEE Transactions on Parallel and Distributed Systems, Volume: 23, Issue: 6, pp- 3013-3019

[9] Tong Zhou , Romit Roy Choudhury , Peng Ning , Krishnendu Chakrabarty, "P²DAP -- Sybil Attacks Detection in Vehicular Ad Hoc Networks", 2011, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 29, No. 3, pp- 1123-1131

[10] Reena Dadhich, "Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks", 2012, Proceedings published by International Journal of Computer Applications, (IJCA), volume 32, issue 45, pp- 57-61

[11] Michel Hugo, "Self-Organized Traffic Control", VANET'2010, September 24, Illinois, volume 17, issue 3, pp- 184-195

[12] Isaac J.T., Zeadally S., Camara J.S., Security attacks and solutions for vehicular ad hoc networks", 2010, IET communication, vol. 4, Issue 7, pp.894-903.

[13] Hamid Hamed, Alireza Keshavarz-Haddad, Shapour Golbahar Haghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support", Electrical Engineering (ICEE), Iranian Conference, 2018, Pages: 602 – 606

[14] D. Srinivas Reddy, V. Bapuji, A. Govardhan, S S V N Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Pages: 1 – 5

[15] Chea Sowattana, Wantanee Viriyasitavat, Assadarat Khurat, "Distributed consensus-based Sybil nodes detection in VANETs", 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE), Pages: 1 – 6

[16] Supinder Kaur, Anil Kumar, "Techniques to Isolate Sybil Attack in VANET-A Review", 2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Volume 14, issue 6, pp- 125-138

[17] Anu S Lal, Reena Nair, "Region Authority Based Collaborative Scheme to Detect Sybil Attacks in VANET", 2015 International Conference on Control, Communication & Computing India (ICCC), Volume 8, issue 5, pp- 189-196

[18] Ashritha M, Sridhar CS, "RSU Based Efficient Vehicle Authentication Mechanism for V ANETs", 2015, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO), Volume 43, issue 88, pp- 9713-9729

[19] Mahdiyeh Alimohammadi and Ali A. Pouyan, "Sybil Attack Detection Using a Low Cost Short Group Signature in VANET", 2015, 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Volume 26, issue 39, pp- 6892-6903

[20] Sebastian Bittl, Arturo A. Gonzalez, Matthias Myrtus, Hanno Beckmann, Stefan Sailer, Bernd Eissfeller, "Emerging Attacks on VANET Security based on GPS Time Spoofing", 2015 IEEE Conference on Communications and Network Security (CNS), Volume 14, Issue 19, pp- 4215-4227

[21] Khaled Rabieh, Mohamed M. E. A. Mahmoud, Terry N. Guo, and Mohamed Younis, "Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs", 2015, IEEE ICC, Volume 66, issue 37, pp- 663-676

