Various Techniques for Secure Routing in VANETs: A Review

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

Usvir Kaur
Assistant Professor
Department of Computer
Science and Engineering
Sri Guru Granth
Sahib World University,
Fatehgarh Sahib

ABSTRACT
The vehicular adhoc networks is the type of network in which no central controller is present and due to which vehicle nodes may join or leave the network any time. In the vehicular adhoc network, vehicle to vehicle and vehicle to infrastructure type of communication is possible in the network. Due to self configuring nature of the network, many malicious nodes may join the network which is responsible to trigger various type of active and passive attacks. In this paper, techniques which are proposed to isolate and Sybil attack in the network are reviewed in terms of description and outcomes.

Keywords
VANET,SYBIL,ACTIVE and PASSIVE

1. INTRODUCTION
Vehicular Adhoc networks (VANETs) are classified as an application of mobile Adhoc network (MANET) [1]. 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 and they enhance road safety and vehicle security while protecting driver's privacy from attack. As of late VANETs have emerged to turn the consideration of researchers in the field of wireless mobile communications [2]. It is autonomous and self-organizing wireless communication network, where every one of the nodes in VANET includes themselves as servers or client for exchanging and sharing information [3]. Vehicular ad-hoc networks are responsible for the communication between moving vehicles in a certain environment. VANET is basically a form of MANET [4]. VANET is a mix of sensor networks and ad hoc networks. They use wireless channel, Satellite channel and transmission for communication. In VANET, vehicles act as nodes which can be exchange data between each other. VANET is mainly aimed at providing safety related information and traffic management [5]. The various types of communication in VANET are of following [6].

- Vehicle – to – Vehicle
- Vehicle – to – Infrastructure
- Inter roadside communication [7]

A variety of attacks have been identified and detected in the network. Keeping in mind the end goal to provide a secure communication, one needs to confront the security challenges. Active and Passive attacks are the two main types of attacks. A passive attack would not disturb the normal operation of mobile ad hoc network, while data have been exchanged from the network. The attacker don't damage to the network specifically. Be that as it may, they can get information for future harmful attacks. Active attacks can be either internal or external. In external attack, the attacker concentrates on to cause congestion in the network. For this reason, they proliferates fake information or to disturb the nodes from giving services.

A Sybil attack comprises of sending multiple messages from one hub with multiple identities. At the point when any hub makes multiple copies of itself then it makes confusion in the network. Claim all the illegal and fake ID's and Authority. It can make collision in the network. This sort of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication yet not internal attacks. There is balanced mapping amongst identity and substance in the network [8].

2. LITERATURE REVIEW
In **K. Rabieh, M. Younis (**2015), [9] the roadside units (RSU) need to know the number of vehicles in their vicinity to be used in traffic management. However, an attacker may launch a Sybil attack by pretending to be multiple simultaneous vehicles. This attack is server when a vehicle collides with others to use valid credentials to authenticate the Sybil vehicles. If RSU are unable to identify such an attack. They proposed a Cross –layer scheme to enable the RSU to identify such Sybil vehicles. Since Sybil vehicles do not exist in their claimed locations, our scheme is based on verifying the vehicles location**.**

In **R. Kaur, M. Kaur (**2015), [10] a novel technique has been proposed to detect and isolate Sybil attack on vehicles resulting in proficiency of network. It will work in two phase .In first phase RSU registers the nodes by identifying their credentials offered by them. if they are successfully verified, second phase starts and it allots identification to vehicles thus, RSU gathers information from neighboring nodes and define threshold speed limit to them and verify the threshold value is exceed the defined limit of speed. A multiple identify generated by Sybil attack is very harmful for the network and can be misused to flood the wrong information over network .simulation results show that proposed detection technique increases the possibilities of detection and reduces the percentage of Sybil attack.

In **W. Han, B. Zang (**2009), [11] they proposed a solution to detect the Sybil attack based on the differences between the normal motion trajectories of vehicles and the abnormal

ones. In our approach ,each node can accomplish the attack detection independently with the limited assistance from the infrastructures of VANET .we improve the feasibility of our approach with limited infrastructures at the early deployment stage of VANET .in addition the independency and feasibility of our algorithm are more robust than the existing solutions that rely on collaboration of neighboring nodes. Simulation results show that the proposed method outperforms the existing solutions in terms of robustness, detection rate, overhead efficiency, and lower system requirements.

In M. C. Surugiu, et.al (2015), [12] the security solution exposed is based on the vehicle position when sending messages, the time when emission occurs, and existence of certification authorities in the area at the starting moment of information transmitted. This guarantees a secure message transmission in the VANET environment. These networks are formed by equipping vehicles with short range wireless communication devices. Development of applications and protocols for VANET network pose particular security issues, induced by the devices being used, vehicles sporadic connectivity, and the high degree of relevance given by their geographical location discovery.

In T. Song, et.al, (2010), [13] they proposed a cluster – based directional routing protocol (CBDRP)for highway scenarios, in which the header of a cluster selects another header according to the moving direction of vehicle to forward packets. Simulation results shows the CBDRP can solve the problem of link stability in VANET, realizing and rapid data transmission.

In T. Zhou et al. 2011, [14] P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks. The author proposed a lightweight and adaptable protocol whose main purpose is to identify Sybil assaults and deny malicious vehicles promptly after detection. In perspective of these requirements, they partition the vehicles into gatherings, and discharge the gathering data to RSBs. Such data permits RSBs to identify suspicious conduct, yet is not sufficient for RSBs to track vehicles, because RSBs cannot distinguish a vehicle from a group of vehicles. So, to group the vehicles, they use the one-way hash function to hash the pseudonyms during initialization. From the outcomes, it is shown that scheme having the capacity to identify Sybil assaults at low overhead and delay, while saving privacy of vehicles.

In **K. M. Rabieh et al**. 2011, [15] the author proposed a detection scheme whose idea is based on public key cryptography and aims to ensure security protection, confidentiality and non-repudiation. The author recommend an adaptable security and protection arrangement utilizing brief and validated declarations that must be issued from the national accreditation power keeping in mind the end goal to ensure trust among vehicles. This scheme depends upon architecture through disseminated RSBs along the street and a centralized DMV which decides whether Sybil assault exists or not. Based on PKI, the solution takes advantage of the digital envelope in which a digital signed combination of individual ID, event, and dual signature are encoded with the DMV public key to be exchanged to the DMV. This ensures both security and protection safeguarding of the Vehicle Information and the Personal ID data also.

In **M. Fogue et al**. (2013), [16] the author proposed a protocol named cooperative neighbour position and verification (CNPV) protocol which is based on proactive approach. The scheme maximizes their performance when all the vehicles give correct information and when it gives position errors the performance gets reduced. The scheme detects the node that gives false location information. The author combines the mechanism with two schemes and shows the benefits of these algorithms. The algorithms are eMDR and UV-cast. (I) in eMDR, the receiver vehicle is allowed to forward the message if sender and receiver are present in different streets. (ii)UV-cast algorithm assigns a store carry forward (SCF) tasks to vehicle. The result shows that UV-cast is a good mechanism to reach new areas of the roadmap while eMDR algorithm is more resistant.

In **C. Campolo et al.** (2011), [17] the author proposed a new analytical model which is intended for assessing the telecom execution on CCH in IEEE 802.11p/WAVE vehicular systems. This model expressly represents the WAVE channel exchanging and processes bundle conveyance likelihood as an element of conflict window size and number of vehicles. There are two types of messages over CCH i.e. short status messages (beacons) and WBSS (wave basic service set). The author validated the model by developing an event-driven custom simulation program in Matlab that follows the 802.11p EDCA protocol specifications. Results are carried out for certain set of parameter values and show the probability of successful broadcast delivery.

In **M. Abu-Elkheir et al. (**2011), [18] this paper proposes a position verification scheme that involves the collaborative exchange of one-hop neighbor information of vehicle position announcements to help make the decision. The scheme analyzes accumulated 2-hop neighbors' information in order to check whether vehicle is in its right position. There are three approaches for position verifications that discussed in the paper. Self-trust, honest majority, temporal behavior consistency is such conditions which should be there in vehicular environment. Results are carried out via simulation and future work would involve implementing a realistic VANET propagation model.

Table no: 1

Author	Year	Description	Outcomes
K. Rabieh, M. Younis	2015	The roadside units (RSU) need to know the number of vehicles in their vicinity to be used in traffic management.	Sybil vehicles do not exist in their claimed locations; our scheme is based on verifying the vehicles location**.**
R. Kaur, M. Kaur	2015	A novel technique has been proposed to detect and isolate Sybil attack on vehicles resulting in proficiency of network.	Simulation results show that proposed detection technique increases the possibilities of detection and reduces the percentage of Sybil attack.
W. Han, B. Zang	2009	In this approach, each node can	Simulation results show that the proposed

		accomplish the attack detection independently with the limited assistance from the infrastructures of VANET.	method outperforms the existing solutions in terms of robustness, detection rate, overhead efficiency, and lower system requirements.
M. C. Surugiu, R. V. Alexandrescu	2015	The security solution exposed is based on the vehicle position when sending messages, the time when emission occurs, and existence of certification authorities in the area at the starting moment of information transmitted.	Development of applications and protocols for VANET network pose particular security issues, induced by the devices being used, vehicles sporadic connectivity, and the high degree of relevance given by their geographical location discovery.
T. Song, L. Shen	2010	The authors proposed a cluster–based directional routing protocol (CBDRP) for highway scenarios.	Simulation results shows the CBDRP can solve the problem of link stability in VANET, realizing and rapid data transmission.
T. Zhou, R. R. Choudhury,P.Ning, K.Chakrabarty	2011	The author proposed a lightweight and adaptable protocol whose main purpose is to identify Sybil assaults and deny malicious vehicles promptly after detection.	From the outcomes, it is shown that scheme having the capacity to identify Sybil assaults at low overhead and delay, while saving privacy of vehicles.
K. M. Rabieh, M.A.Azer	2011	The author recommend an adaptable security and protection arrangement utilizing brief and validated declarations that must be issued from the national accreditation power keeping in mind the end goal to ensure trust among vehicles.	This ensures both security and protection safeguarding of the Vehicle Information and the Personal ID data also.
M.Fogue,Francisco J,Martinez, Piedad Garrido,M.Fiore, C.F.Chiasserini, C.Casetti, Juan-Carlos	2013	The author proposed a protocol named cooperative neighbour position and verification (CNPV) protocol which is based on proactive approach.	The result shows that UV-cast is a good mechanism to reach new areas of the roadmap while eMDR algorithm is more resistant.
C.Campolo,A.Vinel, A.Molinaro, Y.Koucheryavy	2011	The author proposed a new analytical model which is intended for assessing the telecom execution on CCH in IEEE 802.11p/WAVE vehicular systems.	Results are carried out for certain set of parameter values and show the probability of successful broadcast delivery.
M. Abu-Elkheir, S.A.Hamid, Hossam S.Hassanein,M. Elhenawy,S.Elmougy	2011	This paper proposes a position verification scheme that involves the collaborative exchange of one-hop neighbor information of vehicle position announcements to help make the decision.	Results are carried out via simulation and future work would involve implementing a realistic VANET propagation model.

3. CONCLUSIONS

The vehicle adhoc networks is the decentralized type of network in which V2V and V2I type of communication is possible in the network. In the recent times , various techniques for the detection and isolation of Sybil attack is reviewed and discussed in terms of description, outcome. In the future technique will be proposed for the isolation of Sybil attack in the network

4. REFERENCES

[1] M. Raya, & J.P. Hubaux, "Securing vehicular adhoc networks", Journal of Computer Security, pp.39-68, 2007.

[2] S.Iqbal, S.R. Chowdhury, C. S. Hyder, A.V. Vasilakos, & C.X. Wang, " Vehicular communication: protocol design, test bed implementation and performance analysis", In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly , pp. 410-415, 2009.

[3] B. Xiao, B.Yu., & C. Gao, "Detection and localization of Sybil nodes in VANETs", In Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks pp. 1-8,2006.

[4] Y. Hao, J.Tang, Y. Cheng "Cooperative sybil attack detection for position based applications in privacy preserved VANETs" IEEE In Global Telecommunications Conference (GLOBECOM 2011), IEEE pp. 1-5,2011

[5] S. Chang, Q. Yong, H. Zhu, J. Zhao, X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks", IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011.

[6] S. Chang, Q. Yong, H. Zhu, J. Zhao, X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks", IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011.

[7] B. Lee, E. Jeong, & I. Jung, "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET", International Journal of Security & Its Applications, 7(3), pp.1-10, 2013.

[8] li. Mingxi, Y. Xiong, X. Zhou, Y.Sun, " A Regional Statistics Detection Scheme against Sybil Attacks in WSNs", IEEE Sponsored In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on pp. 285-291, 2013.

[9] K. Rabieh, M. Younis," Cross-Layer Scheme for Detecting Large-Scale Colluding Sybil Attack in VANETs", 2015,IEEE

[10] R. Kaur, M. Kaur," Isolation of Sybil Attack in VANET using Neighboring Information", 2015, IEEE

[11] W. Han, B. Zang," A robust detection of the Sybil Attack in urban VANETs", 2009, IEEE

[12] M. C. Surugiu, R. V. Alexandrescu," Study on the Implementation of Protocols for Providing Security in Average VANETs Intervehiculary Network Communication Systems", 2015, IEEE

[13] T. Song, L. Shen," A Cluster-Based Directional Routing Protocol in VANET", 2010, IEEE

[14] T. Zhou, Romit Roy Choudhury, Peng Ning, Krishnendu Chakrabarty," P2DAP Sybil Attacks Detection in Vehicular Ad Hoc Networks", 2011, IEEE

[15] K. M. Rabieh, Marianne Amir Azer," Combating Sybil Attacks in Vehicular Ad Hoc Networks", Communications in Computer and Information Science, 2011, Volume 162, pp 65-722011

[16] M. Fogue, Francisco J. Martinez, Piedad Garrido, Marco Fiore, Carla-Fabiana Chiasserini, Claudio Casetti, Juan-Carlos," On the use of a cooperative neighbour position verification scheme to secure warning message dissemination in VANETs", 2013, IEEE, ISSN: 0742-1303

[17] C. Campolo, A. Vinel, A. Molinaro, Y. Koucheryavy," Modeling broadcasting in IEEE 802.11p/WAVE vehicular Networks", 2011, IEEE, ISSN: 1089-7798

[18] M. Abu-Elkheir, S. A. Hamid, Hossam S. Hassanein, I Brahim M. Elhenawy, Samir Elmougy," Position Verification for Vehicular Networks via Analyzing Two-hop Neighbors Information", 2011, IEEE, INSPEC Accession Number: 12506231