International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-6)

Research Article | **June 2017**

Detection of Sybil Attack in VANETs

[1]**Kamaljit Kaur,** [2]**Amandeep Kaur**
[1]Asst.Pro. Punjabi University Regional Campus Info &Tech Mohali,
[2]Branch: M.tech CSE

Abstract:

The vehicular adhoc network is the decentralized type of network. The vehicle nodes can join or leave the network when they want. In the such type of network security, routing and quality of service are the three major issues of the network. In the network malicious node is present which is responsible to trigger various types of active and passive attacks. The Sybil attack is the active types of attack in which malicious node change its identification multiple times. In this, paper various techniques are reviewed which are used to isolate malicious nodes from the network.

Keywords: GPS, RSU, CNPV, DMV

I. INTRODUCTION

1.1 VANET

The vehicular Ad-Hoc Network or VANET is a technology that use moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile internet is created. Fixed equipment can belong to the government or private network operators or service providers. It is estimated that the first system that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Advancing trends in ad hoc network scenarios allow a number of deployment architectures for nearby vehicles and between vehicles and nearby fixed roadside equipment.

1.2 Application and uses for VANET [1] are:

- **Safety applications:** Safety applications are most imperative factor to decrease the road accident and loss of life of the occupants of vehicles. There are such a large number of accident happened because of the collision of vehicles.
- **Car speed warning:** With help of these protocols utilize a combination of GPS and digital maps are utilized to judge threat level for driver approaching a curve rapidly.
- **Traffic signal violation warning:** It is additionally intended to send a warning message when driver detects the vehicle is in risk of running the traffic signal. The decision to communicate something specific is made on the premise of traffic signal status and timing the vehicle position and speed.
- **Collision risk warning:** in this system vehicle and RSU distinguish odds of collision between multiple vehicles are not ready to communicate among themselves. The system will gather information about vehicles that are coming in opposite direction and are approaching towards the destination.
- **Lane change warning:** In this application vehicle monitor the position of vehicle inside a roadway lane and warn a driver in the event that it is unsafe to move to another lane.

1.3 Major Issues in VANET

There are some issues in VANET. These are as follow [3]:

- **High Mobility:** Due to high mobility every one of the nodes are not interacted appropriately with each other on the grounds that they need to learn about others conduct first as per learn based scheme. It additionally decreases proficiency of the system.
- **Real-time Guarantee:** VANET applications are utilized for hazard warning, collision avoidance, and accident warning information, so applications include strict deadlines for legitimate message delivery.
- **Privacy and Authentication:** It is required to take after the vehicles for the identification of vehicles from the message they send for authentication of all message transmission, which most consumers won't care for others to think about their personal identification.
- **Location Awareness:** For the best possible location awareness GPS system is required to handle the VANET application..
- **Delay in VANET:** In a VANET delay issue ought to be less for the new path identification. In this system vehicle and RSU detect chances of collision between multiple vehicles are not ready to communicate among themselves. The system will gather information about vehicles that are coming in opposite direction and are

approaching towards the destination. For this, there are numerous safety applications are available in VANET to decrease the road accident and loss of life of the occupants of vehicles.

II. SYBIL ATTACK IN VANET

It comprises of sending multiple messages from one hub with multiple identities. Sybil attack is constantly possible aside from the extreme conditions and assumptions of the likelihood of resource parity and coordination among entities. 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.

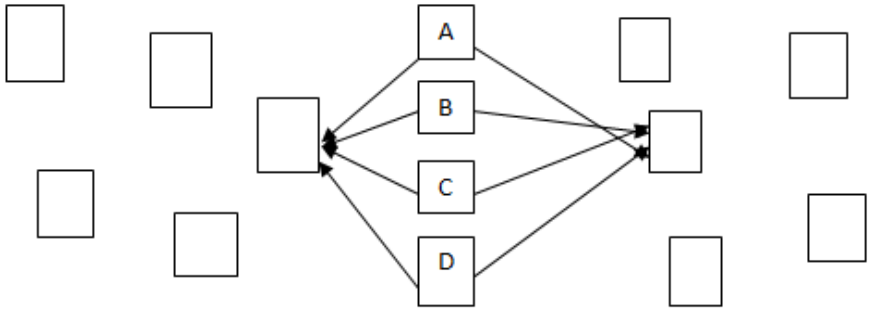

Figure 1: Sybil Attack

As shown in the figure 1, the A,B,C and D are the malicious nodes which trigger attack on the single node. This leads to trigger the denial of service in the network.

In this paper, the introduction about the vehicular adhoc network is presented with the challenges present in the network. The Sybil attack is explained in detail which is the denial of service type of attack. The literature review is presented for the detection and isolation of malicious nodes from the network

III. LITERATURE SURVEY

Manuel Fogue et al. "On the use of a cooperative neighbour position verification scheme to secure warning message dissemination in VANETs" 2013, the author proposed a protocol named cooperative neighbour position and verification (CNPV) protocol which is based on proactive approach [10]. 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.

Shan Chang et al. "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks" 2012, the author proposed a novel Sybil assault discovery component, Footprint, utilizing the directions of vehicles for distinguishing while still preserving their location privacy [17]. When a vehicle methodologies a road side unit (RSU), it effectively requests an approved message from the RSU as the confirmation of the appearance time at this RSU. The author designed a location-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are endorser questionable so that the RSU area data is hidden from the came about approved message; second, two approved messages signed by the same RSU inside a similar given timeframe (incidentally linkable) are conspicuous with the goal that they can be utilized for ID.

Mervat Abu-Elkheir et al. "Position Verification for Vehicular Networks via Analyzing Two-hop Neighbors Information"2011This 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 [12]. Vehicles can access the connectivity of the neighborhood vehicles and use the logical traffic flow to make judgment on trusting a vehicle position announcement. The scheme analyzes accumulated 2-hop neighbors' information in order to check whether vehicle is in its right position.

Claudia Campolo et al. "Modeling broadcasting in IEEE 802.11p/WAVE vehicular Networks"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 [11]. 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). Beacons carry status information about the vehicle. The motivation to this model is twofold (I) to check out the upcoming standard on the capabilities and constraints.

Khaled Mohamed Rabieh et al. "Combating Sybil Attacks in Vehicular Ad Hoc Networks" 2011, the author proposed a detection scheme whose idea is based on public key cryptography and aims to ensure security protection, confidentiality and non-repudiation [16]. 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.

Tong Zhou et al. "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks"2011, the author proposed a lightweight and adaptable protocol whose main purpose is to identify Sybil assaults and deny malicious vehicles promptly after detection [15]. A baseline method is to forward all the reported events to the DMV and let the DMV analyze the signature of every message. On observing a single event marked with two distinct pseudonyms of the same vehicles, the DMV considers that vehicle as an assailant but the disadvantage of this strategy is the substantial system traffic on the DMV. Accordingly, they propose P2DAP schemes in which RSBs perform the greater part of the DMV's errand to decrease the correspondence overhead.

Soyoung Park et al. "Defense against Sybil attack in Vehicular adhoc network based on road side unit support"2009, proposed a timestamp series approach to defend against Sybil attack in a vehicular adhoc network based on roadside unit support [14]. This approach is probably suitable for initial deployment of VANET where vehicles have network communication and have a basic infrastructure i.e. RSU. It uses digital certificates and do not use public key infrastructure though it is secured.

Tim Leinmuller et al. "Improved Security in Geographic Ad hoc routing through Autonomous Position Verification"2006, the author proposed a detection mechanism scheme that uses various different sensors to rapidly give an estimation of the dependability of other nodes position claims without utilizing specific equipment [13]. As the scheme don't use any specific equipment or infrastructure, he advocate the idea of "Position cheating detection system" that is similar to intrusion detection system like the one developed to detect example selfish nodes in MANETs. Each node calculates a trust value that decides if the nodes are trustworthy or be excluded from routing decisions.

3.1 Summary of Literature Review:

Author	Year	Description	Outcome
Manuel Fogue	2013	The author proposed a proactive cooperative neighbour position and verification (CNPV) protocol which detects the node that gives false location information.	The result shows that UV-cast is a good mechanism to reach new areas of the roadmap while eMDR algorithm is more resistant.
Shan Chang	2012	The author proposed a novel Sybil attack discovery component, Footprint, utilizing the directions of vehicles for distinguishing while still preserving their location privacy.	. The result shows that Footprint can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings.
Mervat Abu-Elkheir	2011	The author proposed a position verification scheme that involves the collaborative exchange of one-hop neighbour information in order to help a vehicle make better judgements of position announcements.	Results are carried out via simulation which shows that defining the plausibility area yields accurate detection of position falsifications with low false positives.
Claudia Campolo	2011	The author proposed a new analytical model which is designed for evaluating the broadcasting performance on CCH in IEEE 802.11p/ WAVE vehicular networks.	Results are carried out via simulation for set of parameter values and show the probability of successful broadcast delivery
Khaled Mohamed rabieh	2011	The author proposed a detection scheme whose idea is based on public key cryptography and aims to ensure security protection, confidentiality and nonrepudiation.	Certificate Revocation Lists (CRLs) used with PKI schemes in order to verify certificates used in the network. He used Online Certificate Status Protocol (OCSP) to guarantee that the used certificates are fresh enough and avoid using already revoked ones.
Tong Zhou	2011	The author proposed a lightweight and adaptable protocol whose main purpose is to identify Sybil assaults and deny malicious vehicles promptly after detection.	The result shows that scheme have the capacity to identify Sybil attack at low overhead and delay, while saving privacy of vehicles.
Soyoung Park	2009	The author proposed a timestamp series approach to defend against Sybil attack in a vehicular adhoc network based on roadside unit support.	The result is analyzed under different situations and suggests ways to resolve the challenges posed by the situations.
Tim Leinmuller	2006	The author proposed a detection mechanism scheme that uses various different sensors to rapidly give an estimation of the dependability of other nodes position claims without utilizing specific equipment.	A result shows how messages are delivered by Acceptance Range Threshold (ART) and Mobility Grade Threshold (MGT). It evaluates the detection capabilities of our decentralized position verification system.

In this paper, various techniques are analyzed and these techniques are threshold technique, route discovery technique, cryptography techniques which are applied to isolate malicious nodes from the network

IV. CONCLUSION

In this work, it is been concluded that vehicular adhoc network is the decentralized type of network. Due to self configuring nature of the network malicious nodes join the network which is responsible to trigger various active and passive attacks. In this paper, various techniques (monitor mode & Neighbour node) which detect malicious nodes from the network. In future, novel technique (Hybrid technique) will be proposed which malicious nodes from the network which are responsible to trigger Sybil attack in the network

REFERENCES

[1] Raya, M., & Hubaux, J. P. "Securing vehicular ad hoc networks", Journal of Computer Security, 15(1), pp.39-68, 2007.

[2] Iqbal, S., Chowdhury, S. R., Hyder, C. S., Vasilakos, A. V., & Wang, C. X. " 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] Xiao, B., Yu, B., & Gao, C. "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] Hao, Y., Tang, J., & Cheng, Y. "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] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. "Footprint: Detecting sybil attacks in urban vehicular networks", IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011..

[6] Lee, B., Jeong, E., & Jung, I. "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.

[7] Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu, X." 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.

[8] Gañán, C., Muñoz, J. L., Esparza, O., Mata-Díaz, J., & Alins, J. "PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks", Computer Standards & Interfaces, 36(3), pp-513-523, 2014

[9] Balamahalakshmi D., & Shankar M. K. V., "Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks", International Journal of Engine ring Trends and Technology (IJETT) – Volume 12, pp. 578 – 584, 2014.

[10] Manuel Fogue et al. "On the use of a cooperative neighbour position verification scheme to secure warning message dissemination in VANETs" 2013,

[11] Claudia Campolo et al. "Modeling broadcasting in IEEE 802.11p/WAVE vehicular Networks"2011,

[12] Mervat Abu-Elkheir, Sherin Abdel Hamid, Hossam S. Hassanein, Ibrahim M. Elhenawy, Samir Elmougy," Position Verification for Vehicular Networks via Analyzing Two-hop Neighbors Information", 2011, IEEE, 978-1-61284-928-7

[13] Tim Leinmuller, Christian Maihofer, Elmar Schoch and Frank Kargl,"Improved Security in Geographic Ad hoc routing through Autonomous Position Verification"2006, Elsevier, 2973023-3-4-454

[14] Soyoung Park, Baber Aslam, Damla Turgut, Cliff C. Zou," Defense against Sybil attack in Vehicular adhoc network based on road side unit support"2009, Research Pvt. Communications, 900042

[15] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty," P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks"2011, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3

[16] Khaled Mohamed Rabieh, Marianne Amir Azer," Combating Sybil Attacks in Vehicular Ad Hoc Networks" 2011, CCIS 162, pp. 65–72

[17] Shan Chang, Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin (Sherman) Shen," Footprint: Detecting Sybil Attacks in Urban Vehicular Networks", 2012, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 6

