International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 04, April – 2017, PP – 63-70

A Review paper on VANETs

Nitika Phull[1], Dr. Tanupreet Singh Preet[2]
[1]*Assistant Professor,*
Chandigarh University,
[2]Professor,
ACET, Amritsar

Abstract : Vehicular ad hoc networks (VANETs) have great potential to improve road safety and increase passenger convenience in vehicles. On the other hand, since they use an open medium for communication, they are exposed to several threats that influence the reliability of these features. Our aim is to provide a privacy-aware trust-based lightweight security model that works in the VANET environments. The messages sent in the network require trusted software components to ensure that a particular safety message is based on real events and not injected from a malicious vehicle.

1. Introduction

1.1 Introduction to VANET

Vehicular adhoc networks (VANETs) are classified as an application of mobile adhoc network (MANET) the primary benefits of VANETs are the potential in giving explorers comfort and they enhance road safety and vehicle security while protecting drivers' privacy from attacks perpetrated by foes. As of late VANETs have emerged to turn the consideration of researchers in the field of wireless and mobile communications.

Vehicular adhoc network are wireless networks where every one of the vehicles from the nodes of the network. It is for the driver comfort and road safety, the inter-vehicle communication give them. Vehicular specially appointed network is subclass of mobile impromptu networks which gives a distinguished approach to canny transport system. It is autonomous and self-organising wireless communication network, where every one of the nodes in VANET includes themselves as servers or client for exchanging and sharing information. The network architecture of VANET can be classified into three categories pure cellular, pure specially appointed and hybrid. Application and uses for VANET [1:

- **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 utilise a combination of GPS and digital maps are utilised 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.

1.2. V2V Communication

Possible Deployment in regards to the C2C-CC reference architecture together with the advances in heterogeneous communication technologies, vehicular networks potentially have two fundamental sorts of communication scenarios: car-to-car (C2C) communication situation and car-to-foundation (C2I) communication situation. These sorts of communication scenarios permit various deployment options for vehicular networks. Vehicular network deployment can be integrated into wireless hot spots along the road. Such hot spots can be operated exclusively at home or at office, or by wireless Internet service suppliers or an integrated operator [2].

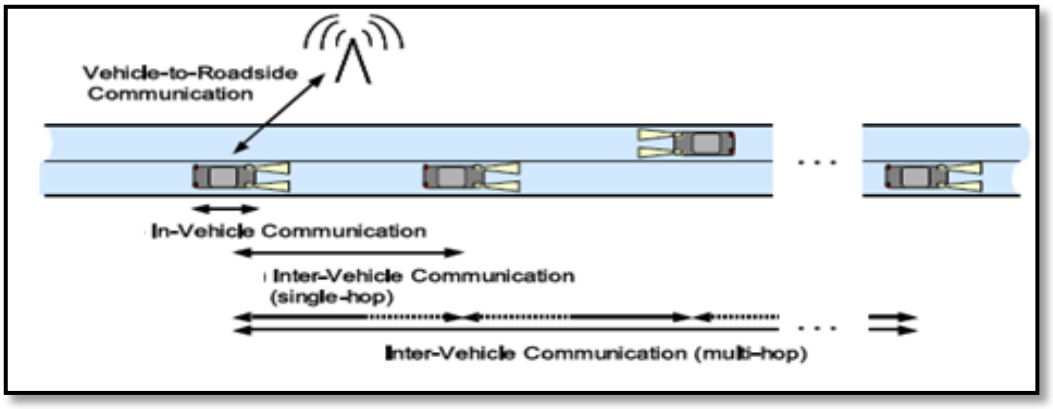

Figure 1.1: Communication architecture [2]

Vehicles can even communicate with other vehicles directly without a communication infrastructure, where vehicles can cooperate and forward information on behalf of each other. Based on their specific characteristics, the technologies for vehicular communication can be categorised in the following three categories.

- In-vehicle communication
- Vehicle-to-roadside/vehicle-to-infrastructure communication
- Inter-vehicle communication (single- and multi-hop)

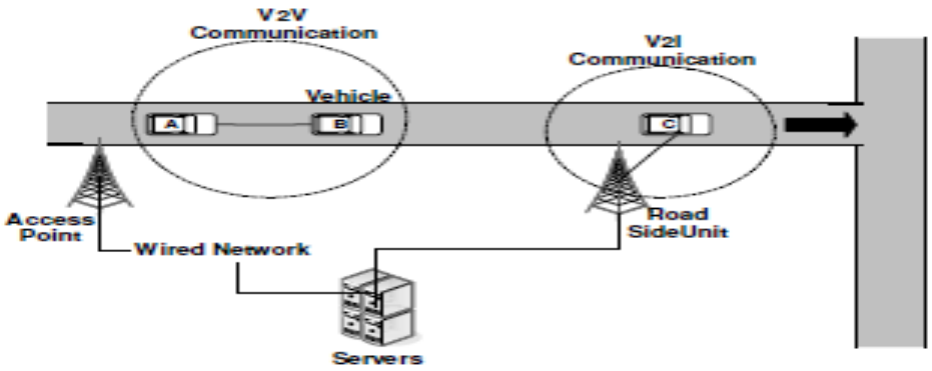

Figure 1.2: Domains of vehicular communication

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 utilised 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. Hence a system needs to be introduced which enables message to be unknown to the common nodes additionally recognition by central authorities in cases like accidents.

- **Location Awareness:** For the best possible location awareness GPS system is required to handle the VANET application. On the off chance that there is no Proper system for location identification, delay is there automatically.
- **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. Collision drives the stick problem. To conquer this problem delay ought to be less [4].

1.4 Types of Attacks

Since mobile ad hoc network is multi-hop in nature, it strictly relies on the cooperation between the nodes. So the guarantee of cooperation of nodes is required. 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. Fundamentally, there are two types of attacks.

a. Passive 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. The types of passive attacks are eavesdropping and traffic analysis.

1. **Eavesdropping Attack:** Eavesdropping attack is the technique for collecting information by snooping on transmitted data on legitimate network. This information may incorporate the location, public key, private key or even password of the nodes. The attacker snoops the data interchanged in the network without modifying it. It is more vulnerable for MANET malicious nodes that can intercept the shared wireless medium.
2. **Traffic analysis:** The principle task of this attack is to monitor and analyse which sort of the transmission is going on. Its point is to engage in convention or to provoke transmission between nodes. For this reason, the attacker may utilise a few methods, for example, time-correlation monitoring, traffic rate analysis, and so forth [5].

b. Active Attacks

In this attack, an attacker dependably tries to change or destroy the data or normal operation on MANET. 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. In internal attacks, the attacker needs to get the normal access to participate in the network activities. The active attacks are namely dropping, modification, fabrication, etc [7].

1. **Dropping attacks:** The communication between two nodes outside the transmission range relies on upon intermediate nodes to forward the packets. Be that as it may, formerly these intermediate nodes does not fill in not surprisingly i.e. they begin to drop the packets during the communication so as to spare their limited sources, for example, bandwidth, energy, and so on. Such sorts of nodes are called misbehaving nodes or non agreeable nodes. Because of this, it may likewise reduce the network performance by causing data packets to be retransmitted furthermore new routes to the destination to be discovered.
2. **Modification attacks:** The attacker rolls out a few improvements to the routing message. Because of movability of nodes in the network, the malicious node participate in the packet forwarding process and later on launch the message modification attacks. The case of message modification attacks are impersonation attacks and packet misrouting [6].
3. **Fabrication attacks:** In fabrication attacks, the attacker forges network packets. There are two types of fabrication attacks namely active forge and forge reply. The attackers send faked messages without getting any related message on account of active forge. In forge reply, the attacker sends fake route reply messages in response to related authenticate route request messages.
4. **Black hole:** In a black hole attack a malicious node advertises itself as having a valid route to the destination node despite the fact that the route is spurious. With this intension the attacker consumes or intercepts the packet without forwarding it. The attacker can totally suppress or modify the packet and generate fake information, which may cause network traffic diversion or packet drop.
5. **Gray hole:** In Gray hole Attack there is a node in the built up routing topology that selectively drops packet with certain probability causing network distraction. Gray hole may drop packets originating from (or

destined to) certain particular node(s) in the network while forwarding every one of the packets for different nodes. Another sort of gray hole may carry on maliciously for quite a while period by dropping all packets yet may change to normal conduct later. A gray hole may likewise exhibit a conduct which is a combination of the above two [7].

6. **Worm hole:** A worm hole attack is the place at least two malicious nodes may collaborate to encapsulate and exchange messages between them along existing data routes. The connectivity of the nodes that have set up routes over the wormhole link is totally under the control of the two colluding attackers. A worm hole demonstrates a valid route to the destination however it generally tunnels the packet to its malicious accomplice node. This attack is otherwise called burrowing attack.
7. **Jellyfish attack:** In jellyfish attack the malicious node first intrudes into the forwarding bunch in the network and after that it unreasonably delays data packets for some measure of time before forwarding them. This outcome in essentially high end to-end delay and delay jitter, and therefore degrades the performance of real-time applications [8].
8. **Spoofing:** The spoofing attack happens when a malicious node pretends other node's identity at times. This thusly misguides a non malicious node keeping in mind the end goal to change the vision of the network topology that it can gather.
9. **Sybil attack:** In Sybil attack, attacker pretends to have manifold identities or nodes. A malicious node can act as though it were a multiple number of nodes either by impersonating different nodes or just by claiming false identities. This permits him to forge the outcomes of a voting utilised for threshold security methods for more information.
10. **Eavesdropping:** It is another sort of attack that as a rule happens in the mobile ad hoc networks. It aims to acquire some confidential information that ought to be kept secret during the communication. The information may incorporate the location, public key, private key or even passwords of the nodes. Because such data are imperative to the security state of the nodes, they ought to be avoided the unauthorised access [9].
11. **Byzantine attack*:*** In Byzantine attack there is a compromised intermediate node works alone, or an arrangement of compromised intermediate nodes works in collusion and carry out attacks, for example, creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.
12. **Jamming attack**: It is MAC LAYER ATTACKS Jamming is the specific class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can accomplish this goal by either keeping a real traffic source from sending out a packet, or by keeping the reception of legitimate packets.
13. **State Pollution attack:** In state Pollution attack there is a malicious node gives incorrect parameters in reply, it is known as the state pollution attack. For instance, in best effort allocation, a malicious allocator can simply give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the wireless Ad-Hoc network and the rejection of new node [10].

1.5 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.

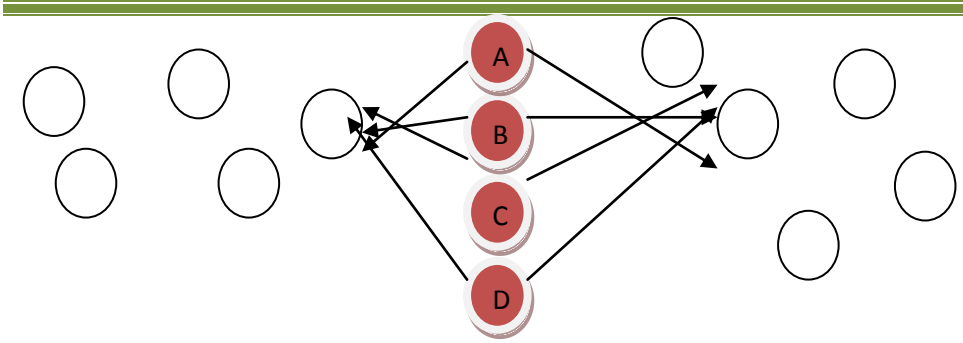

Figure 1.3: Sybil Attack

A, B, C, D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network.

2. 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 [11]. The scheme maximises 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.

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 [12]. 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. (ii) Broadcast apparatus for improving the performance of help in designing. 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.

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 [13]. 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. 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.

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 [14]. 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. The selected mechanism will not completely prevent malicious nodes from using falsified position information; however they will drastically limit the choice of fake positions that will not be detected by our system. As a result, attackers have fewer possibilities for using fake positions. Results are carried out via simulation that 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.

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 [15]. 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. Moreover, this timestamp series approach does not need internet accessibility. As previously proposed schemes required a fixed infrastructure but in this scheme, RSUs is the only component that issues certificates. As vehicles have high mobility, there are fewer chances that two vehicles passing by multiple RSUs at the same time. A Sybil attack is detected when traffic message sent out by vehicle has similar senses of timestamp. To handle with this issue, a vehicle needs to show its previous timestamp to RSU and verify it. They analyzed their approach under various traffic situations i.e. traffic congestion, complex roadways.

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 [16]. 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. In P2DAP scheme, they assign a large portion of the identification to RSBs, and include the DMV just when suspected vehicles need to be confirmed as a Sybil attacker. As RSBs are not trusted elements, the vehicle data accessible to the DMV can't be exchanged to the RSBs. 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.

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 [17]. 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. Certificate Revocation Lists (CRLs) were utilized as a part of conjunction with PKI schemes keeping in mind the end goal to confirm the legitimacy of testaments utilized inside the system. However, he made utilization of the Online Certificate Status Protocol (OCSP), by incorporating it to his proposed plan, to ensure that the used certificates are fresh enough and avoid using already revoked ones.

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 [18]. 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. With the temporal limitation on the link ability of two authorized messages, approved messages utilized for long-term identification are prohibited. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by gathering a continuous arrangement of authorized messages. Using social relationship among trajectories as per the similar definition of two trajectories, Footprint can perceive and therefore dismiss "communities" of Sybil trajectories. It is demonstrated by both analysis and extensive trace-driven simulations that Footprint can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings.

Table of Comparison:

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.
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.
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.
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.
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.
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.
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.
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.

References

[1]. L. Kagal, T. Finin, A. Joshi, Trust-based security in pervasive computing environments, Computer 34 (2001) 154–157

[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]. 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.

[7]. 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.

[8]. 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.

[9]. 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

[10]. 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.

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

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

