International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

# Mitigation of Sybil Attack Using Location Aware Nodes in VANET

**Dalbir Singh[1], Manjot Kaur[2]**

[1]Research Scholar, Department Computer Science & Engineering, CGC, Gharuan

[2]Assistant Professor, Department Computer Science & Engineering, CGC, Gharuan

**Abstract:** ***VANETs also called as intelligent transportation system (ITS) in which vehicles communicate to provide timely information. Their aim is to provide security, information and management of network. Instead of their many advantages vehicular network is prone to various attacks. In this research removal of Sybil attack in which node creates its multiple identities and it can be affected by various ways. In previous work Sybil attack is prevented by using the timestamp. Every node has some time stamp to communicate with RSU in which identities are verified. If multiple identities exist then there must be an attacker. On high traffic roads there are number of vehicles for which RSU cannot process all vehicles and also vehicles have high mobility due to which timestamp may be collapse or may miss by vehicle. In previous work three methods were used to find the physical measurement of message that were Time of Arrival (TOA), Angel of Arrival (AOA), and Received Signal Strength (RSSI). In this work, we are using GPSR, Which Reduce the Chances of Attacks.***

**Keywords:** VANET, ITS, RSU, TOA, RSSI.

## 1. Introduction

VANET is self- configuring like MANET. These networks have mobile devices as vehicles and do not require any infrastructure to communicate. Each node can move in any direction without any constraint but movement should be within the link. A vehicular ad-hoc network system (VANET utilizations moving autos as center points in a framework to make a convenient framework) [1]. A VANET changes each one participating auto into a remote switch or center point, permitting interfacing with one another with an extent between 100 to 300m. Due to the mobility vehicle moving very fast and when they go out of range or drop out the network they join another network range and updating their entries in particular network by sending hello messages. Vehicles are associating with each other to make a versatile Internet [2].

### 1.1 Types of Communication in VANET'S

#### 1.1.1 Inter-vehicle communication

The inter-vehicle communication configuration uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers [3]. In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not behind. There are two types of message forwarding in inter-vehicle communications: native broadcasting and intelligent broadcasting. In native broadcasting, vehicles send broadcast messages periodically and at regular intervals [4].

#### 1.1.2 Vehicle-to-roadside communication

The vehicle to roadside communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity [5]. Vehicletoroadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions [6].

#### 1.1.3 Routing-based communication

The routing-based communication configuration Is a multi-hop unicast where a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reached [7]. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source [8, 9].

### 1.2 Attacks

There are various kinds of attack that can affect the entire system or can degrade the performance of system. The attacks can be categorized into following types [10].

#### 1.2.1Denial of Service attack

This strike happens when the aggressor increments control of a vehicle's benefits or jams the channel of correspondence utilized by the Vehicular Network, so it makes tangle to send separating information to its end of the line. It additionally expands the threat to the driver, on the off chance that it needs to rely on upon the application's data [11].

#### 1.2.2 Message Suppression Attack

An assailant specifically dropping packets from the system, these bundles may hold discriminating data for the beneficiary, the aggressor stifle these parcels and can utilize them again as a part of other time[12].

The objective of such an assailant would be to keep enrollment and protection powers from looking into crashes including his vehicle and/or to abstain from conveying crash

reports to roadside access focuses. Case in point, an aggressor may smother a blockage cautioning, and use it in an alternate time, so vehicles won't get the cautioning and compelled to hold up in the activity [13].

#### 1.2.3 Fabrication Attack

An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personalities [14].

#### 1.2.4 Alteration Attack

This assault happens when aggressor modifies current information, it incorporates deferring the transmission of the data, replaying prior transmission, or changing the genuine section of the information transmitted. For example, an aggressor can modify a message telling different vehicles that the current street is clear while the street is congested [15].

#### 1.2.5 Replay Attack

This assault happens when an aggressor replay the transmission of a prior data to exploit the circumstances of the message at time of sending.

#### 1.2.6 Black hole Attack

When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node [16].

#### 1.2.7 Grey hole Attack

This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcast.

#### 1.2.8 Sybil Attack

In this attack, attacker creates various personalities to simulate different hubs. Every hub send messages with various characters, thusly different hubs understand that there are numerous hubs in the system in the meantime. This assault is extremely unsafe on the grounds that a one hub can issue its different areas in the meantime and this making security hazard [17].

The Sybil assault in PC security is an assault wherein a notoriety framework is subverted by producing personalities in distributed systems. In a Sybil assault the aggressor subverts the notoriety arrangement of a distributed system by making a substantial number of pseudonymous personalities, utilizing them to pick up an excessively huge impact [18].

## 2. Related Work

**Kumar, P. Vinoth et al [10]**"Prevention of Sybil attack and priority batch verification in VANETs", VANET is a type of Mobile Ad-Hoc Network which gives correspondence in the middle of vehicles and street side base stations. The point is to give wellbeing, movement administration, and infotainment administrations. The security of VANET is in concern state from ahead of schedule time. VANETs face a few security dangers and there are various assaults that can prompt human life misfortune. Existing VANET frameworks utilized identification calculation to catch the assaults at the confirmation time in which postpone overhead happened. Batch authenticated and key assertion (ABAKA) plan is utilized to verify numerous appeals sent from distinctive vehicles. Yet it doesn't give any need to the appeals from crisis vehicles and a pernicious vehicle can send a false message by satirizing the character of substantial vehicles to different vehicles prompting Sybil assault.

**Dongxu Jin et al [11]** "A Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks" In this paper, past conventions are investigated, and a novel plan to recognize the Sybil nodes in VANETs is introduced, alleviating the impact of a Sybil assault. The proposed Sybil hubs detection scheme, Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in VANETs (PMSD), exploits un-modifiable physical estimations of the guide messages rather than key-based materials, which measurement take care of the Sybil assault issue, as well as additionally lessen the overhead for the identification. The proposed plan does not require settled framework, which makes it simple to execute.

**de Sales, T.M. et al [12]** "A protection saving verification and Sybil location convention for vehicular impromptu systems" In vehicular specially appointed systems (VANETs), the exchange off in the middle of security and validation prompts a hurtful sort of system assault called Sybil assault. The testing is to evade and identify such assault without bargaining client (vehicle) security. Accordingly, this paper proposes a protection preserving authentication and Sybil location convention for VANETs.

**Mingxi Li et al [13] "**A Regional Statistics Detection Scheme against Sybil Attacks in WSNs" The identification of replication assaults in remote sensor systems (WSNs) has been a long-standing issue. Numerous variations of replication assaults were generated, for example, the Sybil assault. In this paper, we proposed a territorial measurements discovery plan (RSDs) against sybil assaults, which is a viable answer for three key issues: firstly, we address the sybil assault by a RSSI-based appropriated recognition instrument; furthermore, our convention can kept the system from a substantial number of hubs disappointment brought on by sybil assaults; Thirdly, the RSDs has been checked can keep up a high identification likelihood with low framework overhead by actualize tests.

**ZiedTrifa et al [14]**"Mitigation of Sybil Attacks in Structured P2P Overlay Networks", the most despicable aspect of malevolent characters under a typical control element, are regularly controlled by an assailant. In Sybil assault, a solitary vindictive client fashions various fake personalities and professes to be different, unique physical hub in the framework. In any case, Sybil assault is a standout amongst the most unsafe assaults that torment current organized Peerto-Peer overlay systems. This assault is utilized to target legitimate associates and subsequently subvert the framework. In this paper, we portray another system to dissect, discover, and moderate Sybil assaults.

## 3. Problem Formulation

Vehicular ad-hoc networks have been used for reliable communication and movement of the vehicles available on the road. Their aim is to provide security, information and management of network. Instead of their many advantages vehicular network is prone to various attacks, like prankster attack, denial of service attack, black hole attack, alteration attack, fabrication attack, man in the middle attack, timing attack, illusion attack etc. In previous work Sybil attack is prevented by using the timestamp. Every node has some time stamp to communicate with RSU in which identities are verified. If multiple identities exist then there must be a attacker. On high traffic roads there are number of vehicles for which RSU cannot process all vehicles and also vehicles have high mobility due to which timestamp may be collapse or may miss by vehicle. In previous work three methods were used to find the physical measurement of message that were Time of Arrival (TOA), Angel of Arrival (AOA), and Received Signal Strength (RSSI). In previous research researcher judge the estimated physical measurement on the bases of three parameter but it may also be the case that message delay occur due to various another reasons like queue problem, congestion problem, accidental problem, so this approach is not accurate due to absence of GPS. According to our work GPSR protocol will be used through which physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If GPS coordinate matched then there is no attack.

## 4. Proposed Work

Firstly, scenario will be generated in which number of nodes will be initialized and then GPSR will be implemented on the bases of which GPS coordinates will be verified at any time. If some node is coming in the range of another node then its verification will be done on the bases of coordinates, in this way malicious nodes will be detected and verification will also be done by the RSU (Road Side Unit). In which RSU keep checking the identities of nodes and compare it with its node table, if two or more than two identities exist then attacker is identified.

## 5. Results and Discussion

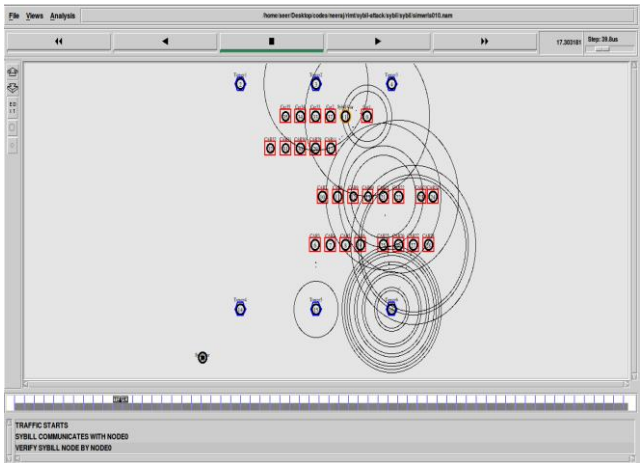


**Figure 6.1:** Removing attack with GPSR

This scenario is use to represent the elimination of Sybil attack occur in the network. This was removed by using GPSR. In GPSR physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If GPS coordinate matched then there is no attack.

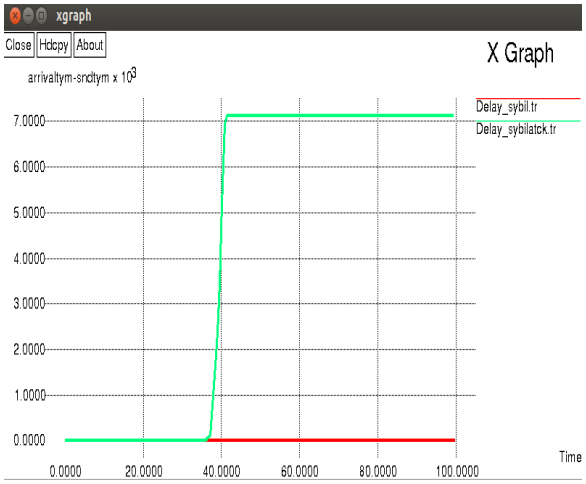


**Figure 6.2:** Delay

This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

$$D = (T_r - T_s)$$

Where, $T_r$ is receive time and $T_s$ is sent time of the packet.

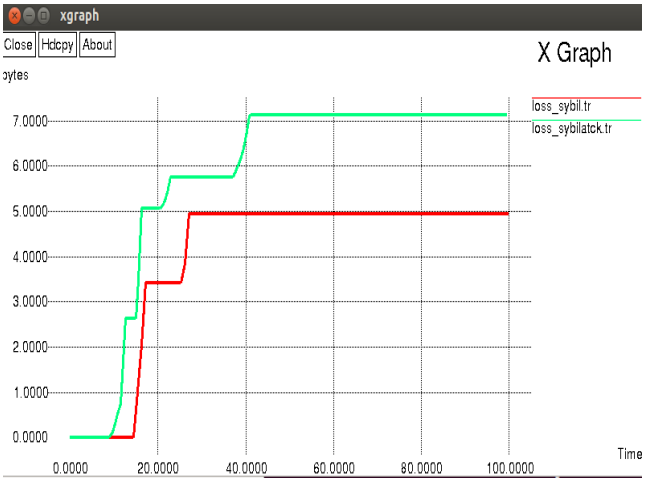


**Figure 6.3:** Packet Loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. The Transmission Control Protocol (TCP) detects packet loss and performs retransmissions to ensure reliable messaging. Packet loss in a TCP connection is also used to avoid congestion and reduces throughput of the connection.

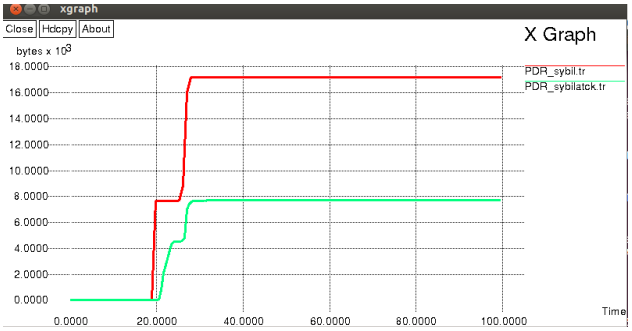


**Figure 6.4:** Packet Delivery Ratio

It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the no. of packet originated from the source.

$$PDR = (P_r / P_s) * 100$$

Where, $P_r$ is total packet received and $P_s$ is total packet sent.

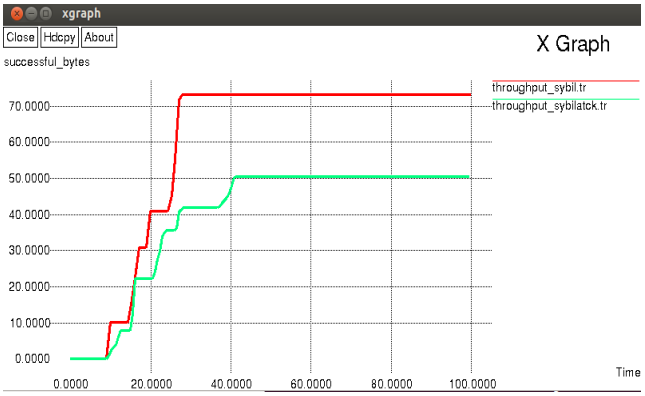


**Figure 6.5:** Throughput

It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation.

## 6. Conclusion

In the purposed work different scenario has been designing for simulation of the vehicular ad-hoc network. According to our work GPSR protocol will be used through which physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If some node is coming in the range of another node then its verification will be done on the bases of coordinates, in this way malicious nodes will be detected and verification will also be done by the RSU (Road Side Unit). In which RSU keep checking the identities of nodes and compare it with its node table, if two or more than two identities exist then attacker is identified. On the basis of various parameters one can conclude that purposed system provides better results.

In the future reference Sybil attack can be avoided by using intrusion detection approach and routing can be done on the basis of location based table for efficient performance during attack on the network.

## References

[1] Sivaraj, R. "QoS-enabled group communication in integrated VANET-LTE heterogeneous wireless networks"*7th International Conference onWireless and Mobile Computing, Networking and Communications (WiMob), 2011*, pp. 17 – 24.

[2] Wagan, "VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination"*International Symposium in Information Technology (IT Sim), 2010*, pp. 607 – 611.

[3] Wagan, Asif Ali, "Security framework for low latency vanet applications", *International Conference onComputer and Information Sciences (ICCOINS), 2014*, pp. 1–6.

[4] Cardote, A Steenkiste, P "On the connection availability between relay nodes in a VANET" *GLOBECOM Workshops (GC Wkshps), 2010*, pp. 181 – 185.

[5] Gongjun Yan, Bista, B.B, Rawat D.B., Shaner, E. F, "General Active Position Detectors Protect VANET Security" *International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011*, pp. 11 – 17.

[6] HsinTeWu, Wei Shuo Li, Tung-Shih Su, Wen Shyong Hsieh, "A Novel RSU-Based Message Authentication Scheme for VANET"*Fifth International Conference onSystems and Networks Communications (ICSNC), 2010*, pp. 111 – 116.

[7] Ebers, S., Hellbuck, H., Pfisterer, D., Fischer, S. "Short paper: Collaboration between VANET applications based on open standards" *Vehicular Networking Conference (VNC), 2013,* pp. 174 – 177.

[8] JieLuo, XinxingGu, Tong Zhao,Wei Yan "MI-VANET: A New Mobile Infrastructure Based VANET Architecture for Urban Environment", *72nd Vehicular Technology Conference Fall (VTC 2010-Fall), 2010*, pp. 1 – 5.

[9] Nafi, N.S., Khan, J.Y. "A VANET based Intelligent Road Traffic Signaling System" *AustralasianTelecommunication Networks and Applications Conference (ATNAC), 2012*, pp. 1–6.

[10] Kumar,Maheshwari. "Prevention of Sybil attack and priority batch verification in VANETs"*International Conference onInformation Communication and Embedded Systems (ICICES), 2014*, pp. 1 – 5.

[11] Dongxu Jin,JooSeok Song "A Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks", *13th International Conference onComputer and Information Science (ICIS), 2014*, pp. 281–286.

[12] De Sales, T.M., "A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks"*International Conference onConsumer Electronics (ICCE), 2014*,pp. 426 – 427.

[13] Mingxi Li, Yan Xiong, Xuangou Wu "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs" *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013*,pp. 285-291.

[14] ZiedTrifa "Mitigation of Sybil Attacks in Structured P2P Overlay Networks" *Eighth International Conference on Semantics, Knowledge and Grids, 2012*,pp. 245-248.

[15] Wei Wei, FengyuanXu "Sybil Defender: A Defense Mechanism for Sybil Attacks in Large Social Networks" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2013, vol*. 24,pp. 2492-2502.

[16] Triki, B. "A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks" *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), 2013*,pp. 1–8.

[17] Mingxi Li, "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs" *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013*,pp. 285–291.

[18] Kafil, P., Fathy, M., Lighvan, M.Z. "Modeling Sybil attacker behavior in VANETs"*9th International ISC Conference onInformation Security and Cryptology, 2012*, pp. 162–168.