Sybil Node Detection and Prevention Approach on Physical Location in VANET

Priyanka Soni
Punjab Technical University
Department of Computer Science,Rimt-IET
College, Gobindgarh, Punjab

Abhilash Sharma
Punjab Technical University
Assistant Professor of Department of
Computer Science, Rimt-IET
College, Gobindgarh,Punjab

ABSTRACT

VANET is a vehicular ad hoc network. This is a part of mobile ad hoc network. 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. Like prankster attack, denial of service attack, blackhole attack, alteration attack, fabrication attack, man in the middle attack, timing attack, illusion attack etc. In this we will use GPSR protocol to remove the Sybil attack. In GPSR protocol 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.

Keywords

VANET, sybil attack, GPSR, ,ITS

1. INTRODUCTION

1.1 VANET

Vehicular Ad-Hoc Network is the network in which communication has been done between road side units to cars, car to car in a short range of 100 to 300 m. Existing authentication protocols to secure vehicular ad hoc networks raise challenges like as certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper proof devices. Vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. This data may be used as the basis of control decisions for autonomous vehicles. If this information is corrupted, vehicles may present unnecessary or erroneous warnings to their drivers, and the results of control decisions based on this information could be even more disastrous. Information can be corrupted by two different mechanisms: malice and malfunction.

1.2 Attacks in vanet

1.2.1 Denial 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. For example, in the event that a malignant needs to make a colossal load up on the roadway, it can make a disaster and use the Dos strike to keep the forewarn from landing to the approaching vehicles.

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.

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.

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, personality.

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.

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.

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 mean time. This assault is extremely unsafe on the grounds that an one hub can issue its different areas in the meantime and this making security hazard. 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. A notoriety framework's powerlessness to a Sybil assault relies on upon how affordably personalities can be created, the extent to which the notoriety framework acknowledges inputs from substances that don't have a chain of trust connecting them to a trusted element, and whether the notoriety framework treats all elements indistinguishably. Confirmation demonstrates substantial scale Sybil assault can be completed in an extremely shoddy and effective path in sensible frameworks like Bit Torrent Mainline DHT.

An entity on a peer to peer network is a bit of programming which has entry to nearby assets. An element promotes itself on the shared system by showing a character. More than one character can relate to a solitary element. At the end of the day, the mapping of characters to substances is numerous to one. Elements in shared systems use different characters for purposes of repetition, asset offering, dependability and trustworthiness. In shared systems, the personality is utilized as a deliberation so that a remote element can be mindful of characters without essentially knowing the correspondence of personalities to neighborhood substances. Of course, every unmistakable character is normally accepted to compare to a particular neighborhood element. Actually numerous characters may relate to the same nearby element.

1.3 Prevention of sybil attack

Validation techniques can be utilized to avoid Sybil assaults and reject disguising unfriendly elements. A near by element may acknowledge a remote personality taking into account a focal power which guarantees a coordinated correspondence between a character and a substance and may even give a converse lookup. A personality may be accepted either straightforwardly or in a round about way. In immediate acceptance the neighbourhood substance questions the focal power to accept the remote characters. In circuitous approval the nearby element depends on officially acknowledged characters which thus vouch for the legitimacy of the remote character being referred to. Character based approval strategies by and large give responsibility to the detriment of namelessness, which can be an undesirable tradeoff particularly in online gatherings that wish to allow restriction free data trade and open dialog of delicate subjects.

2. RELATED WORK

Dongxu Jin et al [1] "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 unmodifiable physical estimations of the guide messages rather than key-based materials, which measurement take care of the Sybil assault issue, as well as additionally lessens the overhead for the identification.

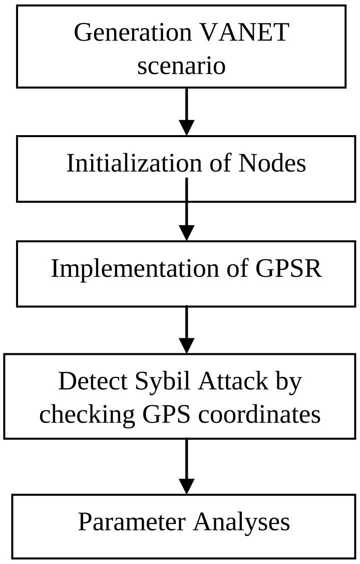
Kumar, P.Vinoth et al [2] "Avoidance of Sybil assault and need group confirmation in VANETs" VANET is a kind of Mobile Ad-Hoc Network which gives correspondence amidst vehicles and road side base stations. The fact is to give wellbeing, development organization, and infotainment organizations. The security of VANET is in concern state from in front of calendar time. VANETs face a couple of security risks and there are different strikes that can provoke human life disaster. Existing VANET systems used recognizable proof count to catch the attacks at the affirmation time in which defer overhead happened. Batch authenticated and key assertion (ABAKA) plan is used to confirm various advances sent from unmistakable vehicles.

de Sales, T.M. et al [3] "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.

Hussain, R. et al [4] “Privacy-aware route tracing and revocation games in VANET-based clouds” The forsean long for dependable, safe, and open to driving background is yet to end up reality since vehicles businesses are trying their waters for VANET (Vehicular Ad Hoc network) organization. In any case by and by, security and protection issues have been the underlying driver of impediment in VANET deployment. As of late, VANET advanced to VANET-based mists as a consequence of assets rich top of the line autos. Before long, Author characterized distinctive compositional structures for VANET-based mists. In this paper, author go for a particular system to be specific VUC (VANET utilizing Clouds) where VANET and CC (Cloud Computing) chip in with one another to give VANET clients (all the more definitely supporters) with administrations.

Hussain, R. et al [5] “Rethinking Vehicular Communications: Merging VANET with cloud computing” Regardless of the surge in Vehicular Ad Hoc network (VANET) research, future top of the line vehicles are required to under-use the on-board reckoning, correspondence, and capacity assets. In this paper, we set forth the scientific categorization of VANET based distributed computing. It is, to the best of our insight, the first push to characterize VANET Cloud structural planning. Moreover we partition VANET mists into three compositional systems named Vehicular Clouds (VC), Vehicles utilizing Clouds (VuC), and Hybrid Vehicular Clouds (HVC)

3. PROPOSED WORK

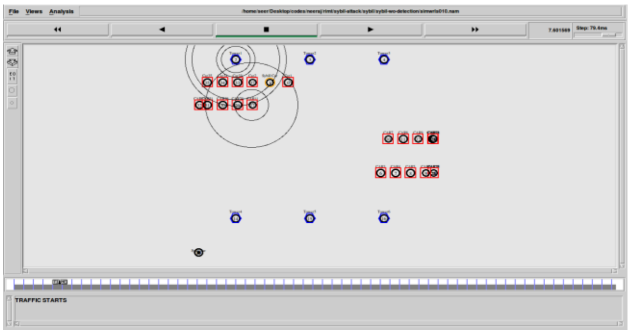

Generation VANET scenario
Initialization of Nodes
Implementation of GPSR
Detect Sybil Attack by checking GPS coordinates
Parameter Analyses

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.

4. RESULTS AND DISCUSSIONS

Table3.1:Simulation Table

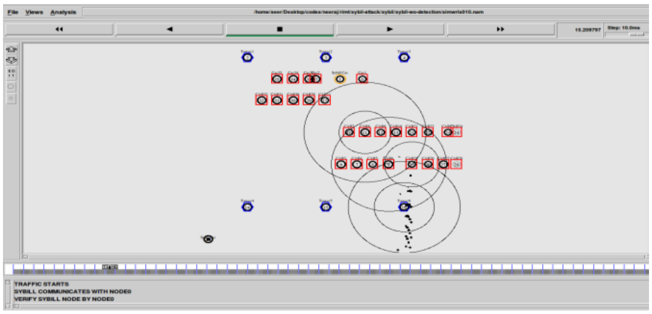
PARAMETERS	VALUES
Routing Protocol	DSR,GPSR
Number of nodes	30
Simulation Time	900sec
Mac Protocol	Mac802.11
Queue Length	50
Radio PropogationModel	Two way Ground
Antenna	Omni
Simulation Area	1000*1000m
Transmission Range	250m



TRAFFIC STARTS

Figure 3.1: Routing

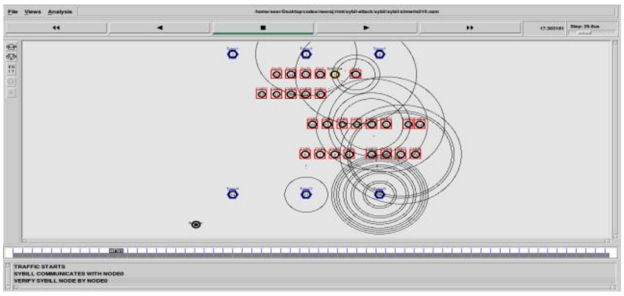
This Scenario is use to represent the routing between the nodes. In routing there is data transmission take place between the nodes.



TRAFFIC STARTS
SYBILL COMMUNICATES WITH NODE0
VERIFY SYBILL NODE BY NODE0

Figure 3.2: Packet with Sybil Attack

This scenario is use to represent the Sybil attack occur in the network. In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.



TRAFFIC STARTS
SYBILL COMMUNICATES WITH NODE0
VERIFY SYBILL NODE BY NODE0

Figure 3.3: 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.

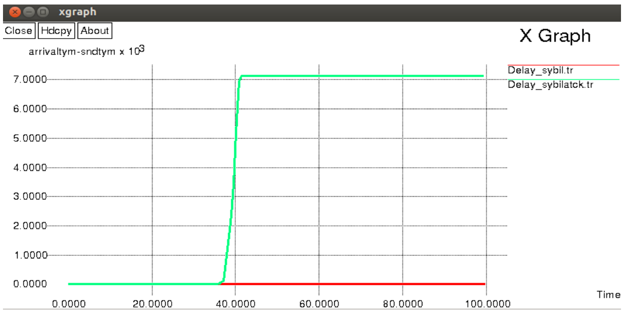


Figure 3.4: Packet Delay

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.

Table 3.2: Packet Delay

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
20	0.0	0.0
40	6.0	0.0
60	6.97	0.0
80	7.1	0.0
100	7.1	0.0

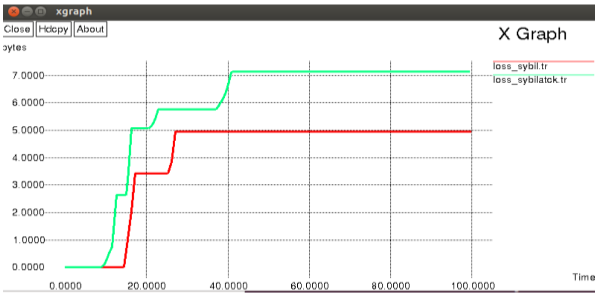


Figure 3.5: Packet Loss

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.

Table 3.3: Packet Loss

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
20	4.2	2.5
40	6.8	4.9
60	7.0	4.95
80	7.2	5.0
100	7.2	5.0

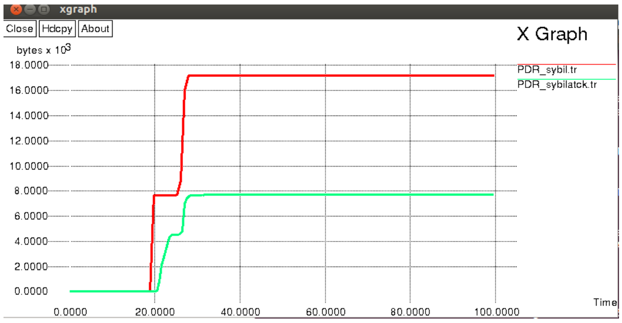


Figure 3.6: Packet Delivery Ratio

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.

Table 3.4: Packet Delivery Ratio

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
20	0.0	7.8
40	4.3	12.5
60	7.9	17.6
80	7.9	17.6
100	7.9	17.6

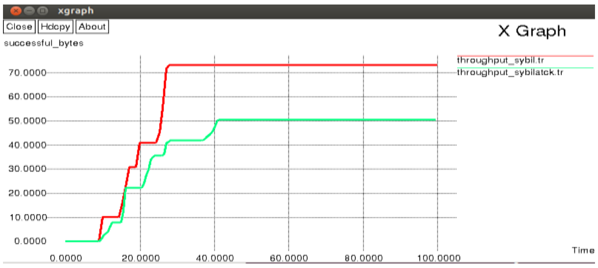


Figure3.7: Packets Throughput

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

Table 3.5: Packet Throughput

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
20	22.0	34.0
40	44.0	60.0
60	51.0	74.0
80	51.0	74.0
100	51.0	74.0

5. CONCLUSION

VANET is a vehicular ad hoc network. This is a part of mobile ad hoc network. 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. GPSR Protocol is use to eliminate the Sybil attack. 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. In final we analyze various types of parameters. On the basis of these parameters we conclude that our system gives us better results.

6. REFERENCES

[1] Kumar, P.Vinoth, Maheshwari, M. “Prevention of Sybil attack and priority batch verification in VANETs”International Conference onInformation Communication and Embedded Systems (ICICES), 2014, pp. 1 – 5.

[2] 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.

[3] de Sales, T.M., Almeida, H.O., Perkusich, A., de Sales, L. “A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks”International Conference onConsumer Electronics (ICCE), 2014,pp. 426 – 427.

[4] Hussain, R.,Abbas, F., Junngab Son, HasooEun "Privacy-aware route tracing and revocation games in VANET-based clouds"9th International Conference onWireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 730 – 735.

[5] Hussain, R, Junggab Son, HasooEun, Sangjin Kim "Rethinking Vehicular Communications: Merging VANET with cloud computing"4th International Conference onCloud Computing Technology and Science (CloudCom), 2012, pp. 606 – 609.

[6] Janech, Lieskovsky,Krsak, E. "Comparation of Strategies for Data Replication in VANET Environment"26th International Conference onAdvanced Information Networking and Applications Workshops (WAINA), 2012, pp. 575 – 580.

[7] Ku, I, You Lu, Gerla, M., Ongaro, F. "Towards software-defined VANET: Architecture and services"13th Annual MediterraneanAd Hoc Networking Workshop (MED-HOC-NET), 2014, pp. 103 – 110.

[8] Azogu, I.K., Ferreira, M.T., Hong Liu "A security metric for VANET content delivery" Global Communications Conference (GLOBECOM), 2012, pp. 991 – 996.

[9] Wanting Zhu, Qing Zhang, Fong, A.C.M. "Performance Analysis of a Hierarchical Structured VANET" IEEE International Conference on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), 2013, pp. 1352 – 1356.

[10] Hao Jiang, Siyue Chen, Yang Yang, ZhizhongJie "Estimation of Packet Loss Rate at Wireless Link of VANET—RPLE"6th International Conference onWireless Communications Networking and Mobile Computing (WiCOM), 2010, pp. 1 – 5.

[11] Yibo Yang, Hongling Li, Qiong Huang "Mobility management in VANET"22ndWireless and Optical Communication Conference (WOCC), 2013, pp. 298 – 303.

[12] Hsin-Te Wu, 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.