Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Sybil Node Detection and Prevention Approach on Physical Location in VANET'S

Priyanka Soni
Dept of Computer Science Engg.,
Mtech Full Time RIMT IET, Punjab India

Abhilash Sharma
Assistant Professor of Dept of Computer Science Engg, RIMT IET, Punjab, India

Abstract- ***Vanet is the branch of networking which deals with the communication of data between different vehicles. The vehicles have been designed with sensors that communicate with RSU and other vehicles available in the range. In the vanet network various attackers perform attack on the network to stop the communication of different vehicles. This attack can make collision between different nodes. The Sybil attack is mainly that interrupts the communication between different vehicles. In the purposed work GPRS algorithm has been introduces for reduction of affect of Sybil attack.***

Keywords-Vanet,V2V, V2R,GPSR.

I. INTRODUCTION

A VANET uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns turn participating car into a wireless router or node which allowing cars 100 to 300 meters of each other to connect and 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 network is created. It is estimated that the first systems that will be this technology are police and fire vehicles to communicate with each other for the purpose of security The connectivity is done among one vehicle to other vehicle and vehicle to road side infrastructure and vehicle or road side infrastructures to the central authority responsible for the network maintenance. The basic tool for message transfer is the short range radios that are being installed in any of the nodes. The short transmission node is used by vehicular node. RSU's are spread sporadically or regularly depending on the deployment of the network in any particular region. In reality spread sporadically.

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 in-formation over multiple hops to a group of receivers. In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not be-hind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in inter-vehicle communications: naïve broadcasting and intelligent broadcasting. In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it.

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. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units.

1.1.3 Routing-Based Communication

The routing-based communication configuration is a multi-hop uni-cast where a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reached. 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 vehicles it received the request from, which is then charged with the task of forwarding it towards the query source.

1.2 Characteristics of VANET

VANET is an application of MANET but it has its own distinct characteristics which can be summarized as:

High Mobility: The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy.

Network topology: Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.

Unbounded network size: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

Frequent exchange of information: The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.
Wireless Communication: VANET is designed for the wirless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication. Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.
Sufficient Energy: The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.
Protection: The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack.

1.3 Routing in VANET

The main concepts of anchor-based routing in sensor networks have been adapted to vehicular networks environments. GSR and SAR integrate the road topologies in routing using those concepts. In these protocols, a source computes the shortest road based path from its current position to the destination. Similar to RBVT, they include the list of intersections that define the path from source to destination in the header of each data packet sent by the source. However, do not consider the real-time vehicular traffic, and consequently, they could include empty roads or roads with network partitions..

1.4 Applications of VANET

According to the DSRC, there are over one hundred recommended applications of VANETs. These applications are of two categories, safety and non-safety related. Moreover, they can be categorized into OBU-to-OBU or OBU-to-RSU applications. Here we list some of these applications.
1.4.1 Co-operative Collision Warning: Co-operative collision warning is an OBU-to-OBU safety application, that is, in case of any abrupt change in speed or driving direction, the vehicle is considered abnormal and broadcasts a warning message to warn all of the following vehicles of the probable danger. This application requires an efficient broadcasting algorithm with a very small latency.
1.4.2 Lane Change Warning: Lane-change warning is an OBU-to-OBU safety application, that is, a vehicle driver can warn other vehicles of his intention to change the traveling lane and to book an empty room in the approaching lane. Again, this application depends on broadcasting.
1.4.3 Intersection Collision Warning: Intersection collision warning is an OBU-to-RSU safety application. At intersections, a centralized node warns approaching vehicles of possible accidents and assists them determining the suitable approaching speed. This application uses only broadcast messages. In June 2007, General Motors 'GM' addressed the previously mentioned applications and announced for the first wireless automated collision avoidance system using vehicle-to vehicle communication (Fig. 2-1, [13]), as quoted from GM, "If the driver doesn't respond to the alerts, the vehicle can bring itself to a safe stop, avoiding a collision".

II. RELATED WORK

Vinoth Kumar, P et al [1] "Prevention of Sybil attack and priority batch verification in VANETs" VANET is a form of Mobile Ad-Hoc Network which provides communication between vehicles and road-side base stations. The aim is to provide safety, traffic management, and infotainment services. The security of VANET is in concern state from early time. VANETs face several security threats and there are a number of attacks that can lead to human life loss. Existing VANET systems used detection algorithm to detect the attacks at the verification time in which delay overhead occurred. Batch authenticated and key agreement (ABAKA) scheme is used to authenticate multiple requests sent from different vehicles. Yet it does not provide any priority to the requests from emergency vehicles and a malicious vehicle can send a false message by spoofing the identity of valid vehicles to other vehicles leading to Sybil attack. Priority Batch Verification Algorithm (PBVA) is used to classify the requests obtained from multiple vehicles in order to provide immediate response to emergency vehicles with less time delay.
Dongxu Jin et al [2] "A Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks" In traffic safety related application of Vehicular Ad-hoc Networks (VANETs), security is a great important issue. Sybil attack is a particular kind of attack where the attacker illegitimately claims multiple identities. In the past years, several approaches have been proposed for solving this problem. They are categorized into PKI-based, infrastructure-based, observer-based, and resource-test-based schemes. In this paper, previous protocols are analyzed, and a novel scheme to detect the Sybil nodes in VANETs is presented, mitigating the effect of a Sybil attack. The proposed Sybil nodes detection scheme, Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in VANETs (PMSD), takes advantage of unmodifiable physical measurements of the beacon messages instead of key-based materials, which dose not only solve the Sybil attack problem, but also reduces the overhead for the detection. The proposed scheme does not require fixed infrastructure, which makes it easy to implement.
Mekliche, K et al [3] "L-P2DSA: Location-based privacy-preserving detection of Sybil attacks" In this paper we propose an approach that uses infrastructures and localization of nodes to detect Sybil attacks. Security and privacy are two major concerns in VANETs. Regrettably, most privacy-preserving schemes are prone to Sybil attacks, where a malicious user pretends to be multiple vehicles. L-P2DSA is an improvement to C-P^2DAP [3], as it allows detecting Sybil attacks while reducing the load on the DMV. This is done due to the cooperation between adjacent RSUs to

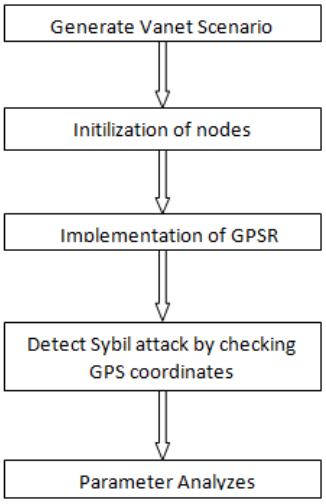
determine the location of suspicious nodes and measure a distinguishability degree between the positions of these malicious nodes. The detection in this manner doesn't need for any vehicle to disclose its identity; thus preserving privacy. The applicability of our contribution is validated through simulation of a realistic test case.

Al-kahtani, M.S.et al [4] "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)" Vehicular Ad hoc Networks (VANETs) are emerging mobile ad hoc network technologies incorporating mobile routing protocols for inter-vehicle data communications to support intelligent transportation systems. Among others security and privacy are major research concerns in VANETs due to the frequent vehicles movement, time critical response and hybrid architecture of VANETs that make them different than other Ad hoc networks. Thus, designing security mechanisms to authenticate and validate transmitted message among vehicles and remove adversaries from the network are significantly important in VANETs. This paper presents several existing security attacks and approaches to defend against them, and discusses possible future security attacks with critical analysis and future research possibilities.

Saggi, Man deep Kaur et al [5] "Isolation of Sybil attack in VANET using neighboring information" The advancement of wireless communication leads researchers to conceive and develop the idea of vehicular networks, also known as vehicular ad hoc networks (VANETs). In Sybil attack, the WSN is destabilized by a malicious node which create an innumerable fraudulent identities in favor of disrupting networks protocols. In this paper, a novel technique has been proposed to detect and isolate Sybil attack on vehicles resulting in proficiency of network. It will work in two-phases. In first phase RSU registers the nodes by identifying their credentials offered by them. If they are successfully verified, second phase starts & it allots identification to vehicles thus, RSU gathers information from neighboring nodes & define threshold speed limit to them & verify the threshold value is exceed the defined limit of speed. A multiple identity generated by Sybil attack is very harmful for the network & 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.

III. METHODOLOGY

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.



DSDV Routing Protocol- DSDV refer as Destination Sequence Distance Vector. It is a proactive routing protocol in which every node maintains a table of information in the presence of every other node in the network [10]. It update the table periodically when change occurred in the network).If any change occur in the network then it broadcasted to every node in the network.

AODV Routing Protocol

AODV refer as Ad hoc on Demand Distance Vector. It is a reactive routing protocol which establishes a route to a destination when there is a demand occurs for the transmission of the data. It does not contain any loop. AODV routing protocol has consist < RREQ, RREP> pair of message to find the route. AODV is only updates the relevant neighboring node(s) instead of broadcasting every node of the network.

DSR Routing Protocol

DSR refer as Dynamic Source Routing. It is also reactive routing protocol as AODV. DSR helps to maintain the source routing, in which, every neighbor in DSR maintains the entire network route from source to the destination.

GPSR- GPSR is a well-known Geographic routing protocol which use the geographic position of the nodes to make the routing decisions, it assumed that every node known its own geographical location using global positioning systems

(GPS).GPSR makes greedy forwarding decisions using only information about routers immediate node in the network topology. When a packet reaches a region where greedy forwarding is impossible the algorithm recovered by routing around the perimeter of the region by keeping state only about the local topology. GPSR uses the greedy approach to find out the immediate neighbors, which works on the principle that the optimal node is the one which is closest to the destination.

IV. CONCLUSION

Vanet network is used for communication between different vehicles available in the city. RSU are available on the roads for transmitting the information about position of other vehicles and safety messages to the vehicles in the range of RSU. In this paper various attacks have been studied that affect the performance of vanet. In this paper different approaches have been described that can reduce the affect of the attacks. In the purposed work GPSR algorithm has been purposed to extract the exact position of the vehicles, so that the predication of attacker node can be done.

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] 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.

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

[6] Wei Wei, Fengyuan Xu "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.

[7] Triki, B. ,Rekhis, S. "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.

[8] 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 (TrustCom), 2013,pp. 285 – 291.

[9] Wagan, A.A., Mughal, B.M., Hasbullah, H. "VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination"International Symposium in Information Technology (ITSim), 2010, pp. 607 – 611.

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

[11] Cardote, A., Sargento, S., Steenkiste, P "On the connection availability between relay nodes in a VANET" GLOBECOM Workshops (GC Wkshps), 2010, pp. 181 – 185.[12] Ravi, K., Praveen, K. "AODV routing in VANET for message authentication using ECDSA" International Conference onCommunications and Signal Processing (ICCSP), 2014, pp. 1389 – 1393.

