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

A Review of Impact of Sybil Attack 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- Vehicular ad-hoc network (VANET) is sub class of mobile ad-hoc network (MANET). MANETS are ad-hoc networks and those types of networks which can alter their location and configure it. Security is the main issue in the network during transmission. Various types of attacks occurred in the network. In this paper we will study about Sybil Attack. The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. 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.

Keywords: VANET, Sybil Attack, MANET.

I. INTRODUCTION

1.1VANET

Vehicular ad-hoc network (VANET) is sub class of mobile ad-hoc network (MANET). MANETS are ad-hoc networks and those types of networks which can alter their location and configure it. They use wireless channel, satellite channel and cellular transmission for communication because these are mobile networks which change their position after every interval. In VANETs vehicles can communicate with road side equipment which is also called as vehicle to roadside communication. In VANETs or MANETs it is not necessary that nodes have internet connection. Roadside equipment can have wireless connection by which vehicles can send data. Because of the dynamic nature of mobile ad-hoc network, they are not exceptionally secure, so it is imperative to be take care what information is sent over a mobile ad-hoc network(W., 2011).

Vehicular network give wellbeing, security, and effectiveness to transportation framework and these are new application or services which gave benefit to travelling public to share emergency, security information while travelling. Vehicular networks are now becoming important or necessary part of future because these will be used in intelligent roadside traffic management system. (S. B. , 2006). It is normal that future wise transportation framework will gave different preferences as contrasted with current transportation framework. The few points of interest

Will be enhanced learning based continuous activity flagging frameworks, upgrade wellbeing for movement administration framework and decreased vehicular discharges. Specialists in correspondences designing and movement administration frameworks are locked in for more than every consistently to make suitable Vehicular Ad hoc Networks (VANET) for activity wellbeing frameworks.

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 impromptu system (VANET utilizations moving autos as center points in a framework to make a convenient framework). 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 300 meters (S. B. , 2006). 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. It is assessed that the first frameworks that will incorporate this engineering are police and blaze vehicles to compare with each other for security reason.

1.2 Various type of attackers

- Insiders Vs Outsiders**:** In a network, a member node who can communicate with other node of the network is called as an Insider and can attack in different ways. Outsiders are those who cannot communicate directly with the other nodes of the network have a limited capacity to attack (i.e.., have less variety of attacks) (A.I, 2011).
- Malicious Vs Rational: A malicious attacker uses various methods to damage the member nodes and the network without looking for its personal benefit. On the contrary, a rational attacker expects personal benefit from the attacks (A.I, 2011). Thus, these attacks are more predictable and follow some patterns.
- Active Vs Passive: A dynamic aggressor can create new parcels to damage the network whereas a passive attacker only eavesdrop the wireless channel but cannot generate new packets (i.e.., less harmful).

© 2015, IJARCSSE All Rights Reserved

1.3 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.

- **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 at to the approaching vehicles. Creators in [1] talked about an answer for Dos issue and saying that the current arrangements, for example, bouncing don't totally tackle the issue, the utilization of different radio handsets, working in disjoint recurrence groups, can be a conceivable approach yet even this course of action will oblige adding new and more apparatuses to the vehicles, and this will oblige more sponsors and more space in the vehicle. The inventors in, proposed an answer by trading between assorted channels or even correspondence progresses (e.g., DSRC, UTRA-TDD, or even Bluetooth for short ranges), in case they are open, when one of them (routinely DSRC) is chopped down.

- **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. 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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **Sybil Attack**

In this attack, attacker generates multiple identities to simulate multiple nodes. Each node send messages with multiple identities, in this way other nodes realize that there are many nodes in the network at the same time. This attack is very dangerous because a one node can give its various locations at the same time and this creating security risk.

1.4 Sybil attack

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. 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.
An entity on a peer-to-peer network is a piece of software which has access to local resources. An entity advertises itself on the peer-to-peer network by presenting an identity. More than one identity can correspond to a single entity. In other words, the mapping of identities to entities is many to one. Entities in peer-to-peer networks use multiple identities for

© 2015, IJARCSSE All Rights Reserved

purposes of redundancy, resource sharing, reliability and integrity. In peer-to-peer networks, the identity is used as an abstraction so that a remote entity can be aware of identities without necessarily knowing the correspondence of identities to local entities. By default, each distinct identity is usually assumed to correspond to a distinct local entity. In reality many identities may correspond to the same local entity.

1.5 Security Requirements for VANET

- **Authentication**

Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the greedy drivers or the other adversaries can be reduced to a greater extent. Authentication, however, raises privacy concerns, as a basic authentication scheme of attaching the identity of the sender with the message would allow tracking of vehicles. It, therefore, is absolutely essential to authenticate that a sending vehicle has a certain property which provides authentication as per the application. For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be.

- **Message Integrity**

This is very much requires as this ensures the message is not changes in transit that the messages the driver receives are not false.

- **Message Non-Repudiation**

In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends.

- **Entity authentication**

It ensures that the sender who has generated the message is still inside the network and that the driver can be assured that the sender has send the message within a very short period.
Access control it is required to ensure that all nodes function according to the roles and privileges authorized to them in the network. Towards access control, Authorization specifies what each node can do in the network and what messages can be generated by it.

- **Message confidentiality**

It is a system which is required when certain nodes wants to communicate in private. But anybody cannot do that. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist.

- **Privacy**

This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information Third parties should also not be able to track vehicle movements as it is a violation of personal privacy. Therefore, a certain degree of anonymity should be available for messages and transactions of vehicles. However, in liability related cases, specified authorities should be able to trace user identities to determine responsibilities. Location privacy is also important so that no one should be able to learn the past or future locations of vehicles.

- **Real time guarantees**

It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met.

II. LITERATURE SURVEY

Kumar, P.Vinoth et al [1] "Avoidance of Sybil assault and need group confirmation 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. Batchauthenticated 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. Need Batch Verification Algorithm (PBVA) is utilized to arrange the solicitations got from numerous vehicles to give quick reaction to crisis vehicles with less time delay. This framework likewise to counteract Sybil assault by limiting timestamps gave by RSU at an early stage itself.
Dongxu Jin et al [2] "A Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks" In movement security related utilization of Vehicular Ad-hoc Networks (VANETs), security is an incredible critical issue. Sybil assault is a specific sort of assault where the assailant illegitimately guarantees various characters. In the previous years, a few methodologies have been proposed for taking care of this

© 2015, IJARCSSE All Rights Reserved

issue. They are ordered into PKI-based, base based, spectator based, and asset test-based plans. In this paper, past conventions are investigated, and a novel plan to recognize the Sybil nodesign VANETs is introduced, alleviating the impact of a Sybil assault. The proposed Sybil hubs detectionscheme, 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. The proposed plan does not require settled framework, which makes it simple to execute. To expand the discovery exactness, activity stream hypothesis and wellbeing watchman separation is brought into the plan. The reproduction results demonstrate a 97% recognition rate of Sybilnodes, with just around a 2% mistake rate.

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 preservingauthentication and Sybil location convention for VANETs.

Mingxi Li et al [4] "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. At long last, we run our convention in a model location framework with 32 hubs that the test result affirmed its high effectiveness.

Zied Trifa et al [5] "Relief 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. We inspect in detail this assault, the most difficult issue that at present engenders in organized Peer-to-Peer overlay systems. We distinguish gimmicks and quest for behavioral ascribes that may serve to recognize such assaults. We had the capacity break down them inside and out, utilizing honeypots, which permits us to gather data to recognize Sybil hubs from legit hubs. Moreover, we present an alleviation system that assuages a portion of the impacts of such an assault by infusing a few summonses into the Sybil hub or subvert the correspondence channel.

Wei et al [6] "Sybil Defender: A Defense Mechanism for Sybil Attacks in Large Social Networks" Distributed frameworks without trusted personalities are especially helpless against Sybil assaults, where an enemy makes different counterfeit characters to bargain the running of the framework. This paper presents Sybil Defender, a Sybil protection instrument that influences the system topologies to shield against Sybil assaults in interpersonal organizations. In light of performing a predetermined number of arbitrary strolls inside the social diagrams, Sybil Defender is productive and adaptable to extensive interpersonal organizations. Our examinations on two 3,000,000 hub certifiable social topologies demonstrate that Sybil Defender beats the cutting edge by more than 10 times in both precision and running time. Sybil Defender can adequately recognize the Sybil hubs and locate the Sybil group around a Sybil hub, actually when the quantity of Sybil hubs presented by each one assault edge is near to the hypothetically discernible lower bound. Furthermore, we propose two ways to restricting the quantity of assault edges in online informal organizations. The review consequences of our Facebook application demonstrate that the presumption made by past work that all the connections in informal communities are trusted does not matter to online interpersonal organizations, and it is doable to point of confinement the quantity of assault edges in online informal organizations by relationship rating.

III. APPROACHES USED

DSDV Routing Protocol-

DSDV refer as Destination Sequence Distance Vector. It is a proactive routing protocol in which every node maintains table of information in the presence of every other node in the network. 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.

© 2015, IJARCSSE All Rights Reserved

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.

Type/Characteristics	**AODV**	**DSDV**	**GPSR**	**DSR**
Abbrevation	Ad hoc On Demand Distance Vector Routing	Destination Sequenced Distance – Vectors Routing	Greedy Perimeter Stateless Routing	Dynamic Source Routing
Defination	Reactive routing protocol which establishes a route to a destination when there is a demand.	Stores the whole path from source to destination in the routing table instead of having the next hop stored	every node known its own geographical location using global positioning systems	Every neighbor in DSR maintains the entire network route from source to the destination
Advantage	No extra traffic is Created for communication along existing links.	It guarantees loop free paths. It also reduces infinity problem counts.	Its reliance only on knowledge of only forwarding node immediate Neighbors	Cache route mechanism results in boosting up the data Transmission
Disadvantage	Requires more time to establish a connection	It does not support multipath routing and sometimes wastage of bandwidth happens	It lacks scalability and does not support quick topology changes.	Size of the packets in the DSR routing protocol increases
Throughput	slowly increases initially and maintains its value when the time increases	increases initially and reduces when the time increases	increases initially and reduces afterwards	increases at lower pause time and grows as the time increases.
Packet delivery Ratio	higher than all other protocols	worse in lower pause time and gradually grows in higher pause time.	PDR of GPSR is less than AODV but improves as density of vehicles increases.	higher than that of DSDV

IV. CONCLUSION

This paper concludes that many researchers provide their methodologies to solve this savior attack but still this is one of the major prone in VANETs, because this attack may also be the reason of other attacks like denial of service attack, prankster attack etc. This paper reveals the performance analysis of reactive routing protocols AODV, AOMDV and DSR in comparison with proactive routing protocol DSDV.In future we will give our methodology to overcome this attack and that approach will be improved than the existing approaches.

REFRENCES

[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.

© 2015, IJARCSSE All Rights Reserved

[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.

© 2015, IJARCSSE All Rights Reserved