International Journal of Computer Science and Informatics

Volume 2 | Issue 2 Article 11

October 2012

Survey of Various Approaches To Countermeasure Sybil Attack

Karamjeet Kaur
PEC Univ Of Tech., Chandigarh, kaur.karam2411@gmail.com

Sanjay Batish
Dept. of Comp. Science, PEC, University Of Tech, Chandigarh, India, sanjaybatish@gmail.com

Arvind Kakaria
Dept. of Comp. Science, PEC, University Of Tech, Chandigarh, India, arvind_802@rediffmail.com

Recommended Citation

Kaur, Karamjeet; Batish, Sanjay; and Kakaria, Arvind (2012) "Survey of Various Approaches To Countermeasure Sybil Attack," *International Journal of Computer Science and Informatics*: Vol. 2 : Iss. 2 , Article 11.
DOI: 10.47893/IJCSI.2012.1077
Available at: https://www.interscience.in/ijcsi/vol2/iss2/11

Survey of Various Approaches To Countermeasure Sybil Attack

Karamjeet Kaur , Sanjay Batish & Arvind Kakaria

PEC Univ Of Tech., Chandigarh
E-mail : kaur.karam2411@gmail.com, sanjaybatish@gmail.com, arvind_802@rediffmail.com

Abstract **-** Vehicular Ad hoc networks (VANETs) are considered as a promising approach for facilitating road safety, traffic management and infotainment dissemination for drivers and passengers. The development of wireless communication in VANET implies to take into account the need of security. Many attacks rely on having the attackers generate multiple identities to simulate multiple nodes, this is called Sybil attack. In this paper, we discuss various approaches proposed by different researchers to defend against Sybil attack.

I. INTRODUCTION

VANET have attracted a lot of attention during last few years from the research community. As for people living in developed countries sheer volume of traffic can be the daily nuisance. Road safety affects the life of the people; millions of people are killed yearly all over the world. Due to this reason many industries invest a lot in order to enhance the safety of the roads to avoid the road accidents. So VANET is the one of the most promising area that studies the communication among the vehicles. In VANET vehicles are equipped with communication device to enable the direct communication between the vehicles and among vehicles and roadside infrastructure. Two types of communication devices are employed in

VANET i.e. On-Board Unit (OBU) and Road Side Unit (RSU). OBU is installed in a vehicle and RSU are placed on roadside. VANET is to increase driver safety and comfort as well as to facilitate traffic management [1].VANET have many applications such as traffic management , emergency warning message, providing safety to the vehicles.

Security is one of the safety aspects in VANET. Without security, a Vehicular Ad Hoc Network system is open to a number of attacks such as propagation of false warning messages as well as suppression of actual warning messages, thereby causing accidents. Various researchers [2] [3] have pointed out that VANETs are facing number of security threats, which might impair the efficiency of VANETs and life safety of driver as well as passengers. One of these threats is Sybil attack in which vehicle claims to be several vehicles either at the same time or in succession [4].

In this, we summarize the various Defence Mechanisms proposed by different researchers against Sybil attack and then we compare these different mechanisms.

II. SYBIL ATTACK

In this same vehicle masquerades identity of multiple vehicles at same time and sent wrong messages to other vehicles and deliberately mislead the other vehicles and vehicular agencies. As false information reported by single malicious vehicle may not be sufficiently convincing, so it may require several vehicles to reinforce the particular information before accepting it as truth [5]. Hence the problem arises when a malicious vehicle is able to pretend as multiple vehicles and reinforce the false data. If the entity unable to recognize a Sybil attack, they will believe the false information and take wrong decisions based to that information. In Sybil attack an attacker take over complete control over the network and send false information in the network and misguide the passengers.

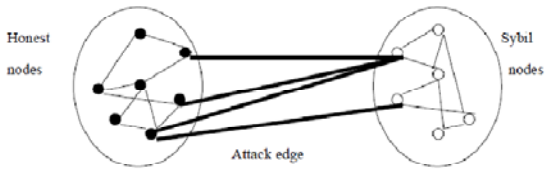

Fig 1

Fig 1 illustrates the Sybil attack problem in which a node illegitimately claims multiple identities. Sybil attack in which a Sybil node pretends to have several identities or a group of malicious node and cooperate together to effect overall network decisions. The bold

black lines show false data and false information between honest and Sybil node [6].

Sybil attack creates an illusion of traffic congestion by claiming multiple identities. it has potential to inject false data in the network via a number of fabricated non-existing vehicles. Sybil attack can further launch a DOS attack by sending the bulk of false information and avoid the true information to reach the destination and can cause the accident or force the driver to take wrong decisions

III. RELATED WORK

Sybil attack was first formalised by Douceur [7] in the context of peer to peer networks. He showed that there is no practical solution for this attack. Deploying trusted certificates is the only scheme that can completely eliminate the Sybil attack but it violates anonymity and Location privacy of nodes, also the assumption that each entity has single identity is very difficult to achieve on the large network.

Resource Testing: This method was proposed by Douceur [7]. In this he assumed that each physical entity is limited in some resources like computation, storage and communication. This approach is not suitable in ad-hoc network because the attacker can have more computational resources than honest nodes.

Radio Resource Testing: This method was proposed by Newsome [8] for detecting Sybil attack in sensor networks. This is based on the assumption that each physical entity has only one radio resource and is able to transmit or receive only on one channel. Entity cannot transmit or receive message on more than one channel simultaneously. This approach is difficult to meet in VANET due to high mobility and impossibility of the pre-deployment of the shared information among vehicles.

Public key Cryptography: Many Researchers [9][10][11] proposed PKI to defend against this attack. Various algorithms are proposed by them. In this one central authority is responsible for giving certificates to each vehicle. Certificate contains public key information, a set of physical attributes of a vehicle. The whole information is recorded by CA. Vehicular Public Key Infrastructure is very heavy to deploy due to the existence of large number of vehicles by different manufactures and countries.

Signal Strength Based Position Verification Scheme: This scheme was proposed by Xiao [12] .This scheme take the advantage of VANET traffic pattern and Roadside base station. The basic idea of this scheme is to estimate a node's position by analyzing its signal strength distribution and to verify whether its claim position is consistent with the estimated position. In this each node play three roles named as (1) Claimer that broadcast beacon messages for the purpose of discovering its neighbours. Beacon messages contain node's identity and its GPS position. (2) Witness is the neighbouring nodes with in signal range that save the corresponding information in their memory. (3) Verifier verifies the claimed position of the vehicle by collecting information from its witness .It calculate mean square error between the estimated position and claimed position. If the estimated position is far different from the claimed position, it is Sybil node. Once the node is detected, the Sybil classification algorithm is performed to check other Sybil nodes generated by same attacker.

Privacy Preserving Detection Scheme: In the previous scheme, every vehicle have to disclose its identity while sending beacon packets as each beacon packet include vehicle identity and GPS information. All this information is in clear text and it is easy for attacker to steal the identity of other vehicles in order to launch Sybil attack. Privacy is one of the most important attribute of a VANET and should not be compromised at any cost. So Sybil attack need to be detected while preserving the privacy of the vehicle.

In this scheme[5], the Department of Motor Vehicles(DMV) provide a pool of pseudonyms for every vehicle in order to hide their unique identity and every vehicle pseudonyms are hashed to particular common value and hash is stored in RSU(Road Side Unit) and DMV. When a vehicle wants to send information to other vehicle it randomly pick any pseudonym from defined pool and then send data using that name. If same vehicle take different pseudonyms from its pool and send wrong information then RSU is able to determine if pseudonym came from same pool or they belong to same entity, if so it suspect a Sybil attack and for further verification and getting the original identity of the vehicle its hashed value sent to DMV and it provide the original unique identity of the vehicle and that suspect vehicle can then be blacklist.

Timestamp Series Approach: In this scheme, Park [13] uses only RSU to issues the timestamp to the vehicle when it passing nearby it and each time stamp is digitally signed by issuing RSU. The vehicle contains two things, one is digitally signed timestamp and other is self generated public key. Each vehicle must contain at least two timestamps issued from last two RSU that the vehicle has passed by.RSU periodically broad cast its public key in the form of certificate, every vehicle within it range receive the certificate and vehicle randomly generate its private public key pair and the generate the timestamp request to RSU, by including the previous timestamp+ previous RSU certificate and vehicle's own certificate. After receiving the request from vehicle RSU verify the certificate of the vehicle as

well as the certificate of the previous vehicle, if it found to be valid, only then RSU assign timestamp to the vehicle so that it can carry out the secure communication with vehicles and prevent the Sybil attack If two requests have same timestamp then probability of Sybil attack is there and it can be detected by this proposed scheme

Detection using Neighbouring Vehicles: This scheme protect against the Sybil attack using neighbouring nodes information [14]. The previous Timestamp Scheme based only on RSU to detect Sybil nodes .In this approach every node participate to detect the suspect node in the network. Every vehicle have different group of neighbours at different time interval. A vehicle send several type of messages like beacon packet to ensure its presence, Alert messages to ensure the safety of the vehicle. All nodes within the range of sender receive the packets and form a group of neighbouring nodes. All the Sybil identities originated from an attacker node share the same set of physical neighbours.

Every vehicle after collecting enough beacon packets from neighbouring nodes, it makes a record of group of neighbours at regular interval of time. After significant duration of time these node further exchange their packets with other nodes within its range. After sharing their tables they match their neighbouring table, if some nodes are simultaneously observed with same set of neighbours at different interval of time, then these node are under Sybil attack.

.

IV. SUMMARY

Algorithm	**Description**	**Limitations**
Resource testing[7]	In this, it is assumed that each physical entity has limited number of resources	It is not applicable to Ad hoc networks as the attacker can have more computational resources than honest nodes.
Radio Resource testing[8]	This is based on the assumption that each physical entity has only one radio resource and is able to transmit or receive only on one channel	This approach is difficult to meet in VANET due to high mobility and impossibility of the pre-deployment of the shared information among vehicles.
Public key Cryptography[9][10]	In this one central authority is responsible for giving certificates to each vehicle. Every vehicle uses that certificate to authenticate itself.	Vehicular Public Key Infrastructure is very heavy to deploy due to the existence of large number of vehicles by different manufactures and countries.
Signal Strength Based Position Verification Scheme[12]	The basic idea of this scheme is to estimate a node's position by analyzing its signal strength distribution and to verify whether its claim position is consistent with the estimated position.	The attacker is so clever that he increase the strength of his signal while sending the beacon message with its wrong position in message. When the verifier measure the strength of signal and compare the claimed position both come out to be same and hence no mean square error hence unable to detect the suspect node. Signal Strength based verification accuracy is limited with an error about 10m .If two entities are very close to each other we cannot ensure whether they are neighbouring nodes or Sybil nodes.
Privacy Preserving Detection Scheme[5]	It detects Sybil attack while preserving the privacy of the vehicle. In this scheme[5], the Department of Motor Vehicles(DMV) provide a pool of pseudonyms for every vehicle in	This scheme provides privacy as no vehicle need to disclose its identity. But in this every vehicle need to registered itself to the trusted authorities and it is very heavy to implement as there are very large number of vehicles and its difficult

	order to hide their unique identity and every vehicle pseudonyms are hashed to particular common value and hash is stored in RSU(Road Side Unit) and DMV.	to generate large number of pseudonyms for every individual vehicle.
Timestamp Series Approach[13]	In this only RSU issues the timestamp to the vehicle when it passing nearby it and each time stamp is digitally signed by RSU .When vehicle want to send information to any vehicle then firstly it request to RSU to issue timestamp to it, after getting timestamp it send message to other vehicle.	This approach does not work in complex roadways where two vehicles coming from opposite sides, this may result in false detection as both vehicles may receive same series of certificate from same RSU for some significant period of time [14]. If this time is equal to or longer than the observation period, nodes will be falsely detected as Sybil nodes.
Detection using Neighbouring Vehicles[14]	In this approach every node participates to detect the suspect node in the network. Every vehicle have different group of neighbours at different time interval. If every vehicle has same neighbours at different interval then that vehicle is a suspect.	In this addition computations are required to calculate the neighbouring information of the vehicles due to highly dynamic topology of VANET as nodes in neighbourhood of the vehicles change their position rapidly.

.There are a variety of attacks that hinge on the issue of identity. In this paper, we have presented an overview of work related to analyzing or solving the Sybil attack in VANET, in which one entity appears as or controls many different identities. The solutions proposed by various researchers have some holes in them. Some approaches cannot be applied to VANET due to their highly dynamic topology like resource testing, radio resource testing. PKI is difficult to implement. From all the above Timestamp approach and using neighbouring vehicles parameter is best solution for Sybil attack. We will explore our research by using these approaches. We lack an efficient, general solution that scales well to large systems, there are a variety of solutions that can limit or prevent the attack in several individual application domains.

REFERENCES

1. Bai,F.Krishnan,H.Sadekar,V.Holl,G. AND Elbatt, T "Towards characterizing and classifying communication based automotive applications from wireless networking perspective" proceedings of IEEE Workshop on Automotive Networking and Applications 2006.
2. B.Parno and A.Perrig. "Challenges in Securing Vehicular Networks" In Proc of the Fourth Workshop on Hot Topics in Networks , 2005.
3. M.Raya and P.Hubaux "The Security of Vehicular Networks " In Proc of the 3rd ACM workshop on security of Ad hoc and Sensor networks, 2005
4. J.T. Isaac S. Zeadally J.S. Ca´mara, "Security attacks and solutions for vehicular adhoc network",IET communication,2009.
5. Tong zhou, romit roy choudhury,peng ning,krishnendu chakrabarty,"privacy-preserving detection of Sybil attacks in vehicular adhoc network" proc of international conference on mabiquitous, 2007
6. Yu, H. Kaminsky,M .Gibbons, P. Flaxman, "Defending Against Sybil Attacks via Social Networks" In Proc of the 2006 conference on Applications,Technologies,Architecture and Protocols for Computer Communication, 2008
7. J.Douceur "The Sybil Attack" In First International Workshop on peer to peer Systems , 2002.
8. J.Newsome, Elaine Shi , Dawn Song,Adrain Perrig, " The Sybil Attack in Sensor Network:Analysis and Defenses" In Proc of the 3rd international symposium on information processing in sensor networks California USA, 2004
9. Raya. M. And Hubaux," Securing vehicular ad hoc networks", Journal of Computer Security,2007.
10. Golle, P.Greene, D and Staddon, "Detecting and correcting malicious data in VANETs" In Proc of the 1st ACM international workshop on Vehicular ad hoc networks, 2004.
11. Pal.S,Mukhopadhyay A.K and Bhattacharaya P.P, " Defending Mechanisms Against Sybil Attack in Next

Generation Mobil Ad hoc Networks", IEEE Technical Review, 2008.

12. Bin Xiao,Bo Yu and Chuanshan Gao,"Detection and localization of Sybil nodes in VANETS" In proc of workshop on dependability issuses in wireless ad hoc networks and sensor networks, 2006
13. Soyoung Park Aslam,B.Turgut,D.zou and C.C,"Defense against Sybil attack in Vehicular Ad hoc network based on Roadside Unit Support" In Military Communication Conference, 2009.
14. Jyoti Grover,Manoj Singh Gaur,Vijay Laxmi," A SybilAttack DetectionApproach using Neighboring Vehicles in VANET",2011.