Detection of Sybil Attacks & Nodes in Vehicular Ad Hoc Networks based on Road Side Units

Mrs.K.Valarmathi[1] Mrs.A.Vijayasarathi[2] S.Devaki[3]
[1]Head of the Dept. [2]Assistant Professor [3]M.Phil Student
[1,2,3]Department of Computer Science
[1,2,3]Trinity College for Women, Namakkal

Abstract— Through the fast growth of wireless technologies, Privacy of personal place information of a vehicle ad-hoc network (VANET) users is attractive a more and more important issue. Services provided by Location based services to VANETs users can breach by Sybil attacks. by malicious vehicles claim multiple identities at the same time. The avoidance of these attacks, which could arise in otherwise out of the Road Side Units (RSUs) reporting have a challenge to detect, as it should gather a cooperation between the ability to identify the real identity of the malicious vehicle, and avoidance of vehicle users starting being tracked by malicious entity. These papers propose a solution to stop and detect Sybil attacks in VANETs. The classification of attackers is based on two types of authentication techniques. The first uses discovery tags embedded in the vehicle to confirm them to the RSU and obtain short lifetime certificates. The second uses certificates to confirm vehicles to their neighbors. The vehicular network is divided into diverse zones brought under the control of dissimilar guarantee authorities (CAs), forcing a vehicle to change its diploma at what time touching from a zone to another. One important characteristic of the projected solution is that it prevents attackers from tracking the mobility of the vehicles. Avoid false negatives is also addressed using observers in vehicle nodes. A set of duplication scenarios also are performance to evaluate the presentation of the proposed solution. In last, these articles summarize the assessment between our proposed approach prevent the network from various hurtful property. Later we propose improvement in RSU support certificate base detection mechanism.

Key words: Vehicular, Communication, Transportation, Vehicle

I. INTRODUCTION

In support of current two decade vehicles are not only realms of Mechanical engineers but gaining attention of computer engineers also. At the present next generation vehicles would have equipped with some kind of hardware named On Board Unit that allow them to communicate with other vehicle as well as roadside-units and they form a statement network so as to we identify vehicular ad-hoc network (VANET). The main aim of VANET is to make roads safer and competent by providing timely in sequence to the other drivers and concerned authorities this is called as gifted Transportation System (ITS). Growths of such type of networks have buy number of security issue those are related to mobile and wireless communication with user time alone. Since of the open nature of VANET they are vulnerable to various types of attacks. Attackers also classify as inside attacker and external attacker. A few of the attacks which may weaken VANET are as follows:

A. Sybil Attack

It's be category of attack in which a hateful driver creates many fake identities to make illusion that there is very heavy traffic nearby him so the traffic following him may choose alternate route and attacker would get empty route for himself. These are some attack that may be performed in a VANET environment by an attacker. Various solutions have been given by authors for these attacks. In this paper we shall consider only Sybil attack in detail. We briefly describe some and regret bounds are derived for general correlation structures among the sniffers, and remain of the schemes to detect Sybil attack in VANET and describe the comparative study of these detection schemes.

Sybil attack is an extremely critical protection issue in vehicular ad-hoc network. Sybil attack was first introduced by Douceur [11] in peer-to-peer networks. Author has given various methods to detect Sybil attack. In Sybil attack one malicious vehicle have control over other Sybil nodes and may have control over other networking protocols also.

For example in presence of Sybil nodes result of some voting based protocols may be deviated and Sybil nodes may also launch Denial of Service attack to impair the normal operations of data dissemination rotocols. Sybil attack can be detected by using three types of techniques [12] a) Radio resource testing, based on an assumption that a radio cannot send or receive simultaneously on the same channel. b) Identity registration, based on that each vehicle should have a unique identity as issued by some centralized authority. c) Position verification, based on the malicious node creates some fake identities at different position so on the basis of the physical position of the node. Some authors propose schemes that are centralized in nature and some propose schemes those are not centralized in nature. Schemes those are centralized in nature have a centralized trusted authority and that authority issues some form of certificate unique for each vehicles but the schemes those are not centralized in nature use other form of techniques to detect Sybil attack for example resource testing or position verification etc. proposed a scheme that is centralized in nature i.e. there is centralized authority authors call it Department of Motor Vehicle (DMV), they may issue a pool of pseudonyms for vehicles, by which a vehicle can be uniquely identified but this identity can be made hidden so that vehicles' privacy can be preserved. Authors also use support of RSU which authors consider a semi trusted unit. Some authors also gave social based Sybil attack defense.

II. RELATED WORKS

In this article the author detects Sybil attack through cryptographic system. In this method a fixed key infrastructure is used for identifying Sybil attack. For

reviewing the results of this study a Mat lab simulator is used. There is very less delay in detecting Sybil attack in this method, as almost all operations are implemented in Certification Authority, so the proposed method is an efficient method for identifying Sybil attack. The only problem in this proposed method is that, when nodes prompt to other region the method does not work properly. Fake messages and forge nodes are identified by observing their actions afterward of their sending out the messages by using the concept of data-centric Misbehavior Detection Schemes (MDS). In the data-centric MDS, Whether the received information is correct or not is decided by each node and it is made on the basis of consistency of recent received messages.

There is no need of Voting or majority decisions, which makes MDS more reliable to detect Sybil attack. Once the attack is identified, Irrespective of revealing all the hidden ID of suspicious nodes, fine is imposed on those nodes and thus de-motivating them to act selfishly. Thus the computation and communication costs that were indulged in revealing all the hidden ID of suspicious nodes are reduced by this approach and the same is shown in the results.

In this a new timestamp series approach is suggested which is based on road side infrastructure. No special infrastructure or public key infrastructure is required in this approach. The case that two vehicles passes multiple RSUs simultaneously is uncommon, thus considering this assumption and impermanent relation between vehicles and RSU, two Messages having identical timestamp series by same RSU will be taken as a Sybil attack by that vehicle.

As VANET is an emerging research area and so are its security issues. There are many security issues in VANET but here in this section we will be dealing with one of its major security issue the SYBIL ATTACK. SYBIL attack is a malicious attack in which the attacker creates multiple identities and uses them to gain a disproportionately large influence.

SYBIL attack is very grievous as the attacker can play any kind of attack with the system scaling down the efficiency of VANET to a larger extent and thus making it less feasible for practical approach. These forge identities also creates a semblance that there are additional vehicles on the road. Thus the need of ensuring that any confidential information is neither modified nor misused by an attacker.

DMV distributes the global key used for generating coarse grained hash values, to all of the Road-side Boxes (RSB) and preserve the key used for generating fine grained hash values securely and private. RSBs in this research work are the same RSUs in previous methods. After generating sufficient number of fine grained hash values in each subgroup of coarse grained group, all of the pseudonyms in each subgroup (with equal fine grained and coarse grained hash values) should be allocated to one vehicle. DMV assigns a unique fine grained subgroup of pseudonyms to each vehicle at the time of yearly vehicle registration and so this unique mapping is a secure plate number for each vehicle. Sybil attack detection is done in two levels. At the first, RSBs overhear exchanging messages and puts the used pseudonyms for signing a specific event, into a list and with calculation of coarse grained hash values of these pseudonyms, all of the pseudonyms with repetitive coarse grained hash values mark as suspicious and RSB send them.

III. Study of Defense Mechanisms

A. Sybil Attacks Detection

Toward be an well-organized solution toward the prevention of Sybil attacks in mobile networks. To be well used in VANETs, the certificate should not show the real individuality of the vehicles to would only show the pseudonym of the means of transportation instead of its real identity, the latter preserve their privacy. Even if the used certificate should be renewed every short-period of time to prevent attackers from tracking the user and compromising the vehicle security. However, as certificates renewal would generate an additional overhead, the solution to develop should come to a compromise between drivers' privacy and protection from Sybil attacks [13]. Second, when renewing their identities by requesting new certificates, vehicles should be accurately and rapidly identified, preventing them from creating several requests at the Same time to obtain multiple identities from the same RSU. While such a malicious behavior could be detected if two certificate requests have the same timestamp, false positives could be generated. In fact, if the RSU is deployed in road intersections, it could allow a malicious vehicle, which stops close to the RSU, to generate multiple and timely spaced requests and consequently to receive several valid certificates. Therefore the solution to develop should take into consideration the need for defining the RSU positions and prevent vehicles from obtaining multiple valid certificates to prevent them from generating Sybil attacks.

B. Location Privacy Architecture

At the same time as discuss in section I, Vehicular Ad-hoc Network using service of location based in real environment. And VANETs have received a great deal of attention for their promises in revolutionizing the intelligent transportation systems and telemetric services. In a general setting, a VANETs is composed of three components: on board units (OBUs) equipped in mobile vehicles, fixed roadside units (RSUs), and a central trust authority (TA).

1) TA (Certified Trusted Authority)

TA is in declare of the listing of RSUs at the road side and mobile OBUs equipped on the vehicles, and can rev the real OBU identity of a safety message by incorporating with its sub ordinate RSUs. The TA is assumed powered with sufficient computation and store capability.

2) RSU (Road Side Unit)

The RSUs are subordinated by the TA, which hold store units for storing information coming from the TA and the OBUs. The main task of RSUs are (1) issuing a short-time anonymous public key certificate to eaOBU when the OBU requests, and (2) assisting the TA to efficiently track the rOBU identity of any safety message.

3) OBU (on board unit)

The OBUs be install on the moving vehicles, while essentially communicate with each other for sharing local traffic information improve the whole safety driving conditions, and with RSUs for requesting short-time anonymous public key certificate.

4) Observing Security-Related Events

To sense security attacks taking place out of RSUs exposure, and collect security related information useful to determine sybil nodes, an observer component is attached to every vehicle, RSU, and RSC.

Observers in vehicles are active only in inter-zone roads. They are in charge of following actions:

- Sending certificate generation requests to the first crossed RSU of the same zone;
- Reception of certificate revocation lists from RSUs;
- Authentication of neighbors based on signatures of the received messages;
- Generation of reports about used certificates in inter-zone roads;
- Delivery of the generated reports to RSUs;
- Detection of sybil attacks i.e. multiple request from same vehicle at same time (in same zone or different zone).

Observers at each RSUs are in charge of following actions:

- Collecting the identities of vehicles becoming in the coverage of their hotspots, together with timestamps of entry and exit to the covered area;
- Identifying new vehicles entering to the zone, they belong to, for the first time; b) checking signatures of received messages from the vehicles;
- Collecting messages exchanged between neighbors and checking the validity of their signatures;
- Forwarding to the RSC requests for new certificates, received from new incoming vehicles
- Sending to vehicles the list of revoked certificate;

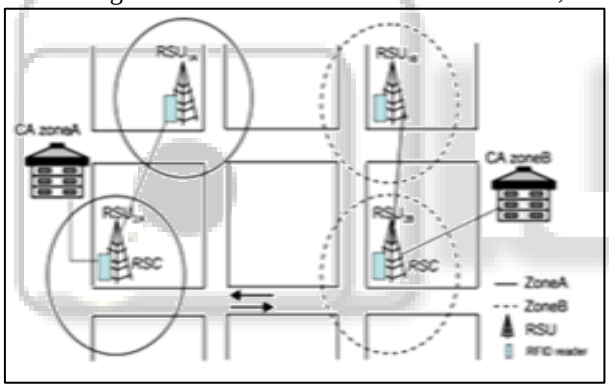

Fig. 1: Proposed Architecture

As it is possible that traffic messages are disseminated through several different multiple hops based on the application in use, the pseudonym PS , RSU certificate Cert_ RS and the signed Event_ Info will prevent any modification or forging of the message.

IV. Evaluation Results

Simulation be established out in NS-2. In organize to decrease the packet overhead, we assume elliptic curve cryptosystem for our basic signature scheme. The synopsis of our simulation parameters is shown in the table below. The key length of elliptic curve digital signature algorithm is 163 bits (21 bytes), and the corresponding signature size is 28 bytes. The estimated signature generation time is 36.82ms, and the verification requires 38.05ms.

Parameters	Values
Simulation distance	600m
The number of vehicles	10, 20, 30,40, 50,60
Average driving speed	50, and 150 km/h
Asymmetric Encryption	ECC with a key of 164bits
Transmission range	170m
Bandwidth	3MB
Packet size	48 and 98 bytes

Table 1: Parameters

For the consistency with signature, we adopt elliptic curve cryptography encryption and decryption with a key of 163 bits for our asymmetric algorithm. The estimated encryption and decryption time are 2.65 and 1.31ms, re-spectively. Generating a request by a vehicle requires one asymmetric encryption (2.65ms). So the total processing time is 2.65ms.

One asymmetric encryption (2.65ms).following figure shows the delay at various speeds with various no. of vehicles.

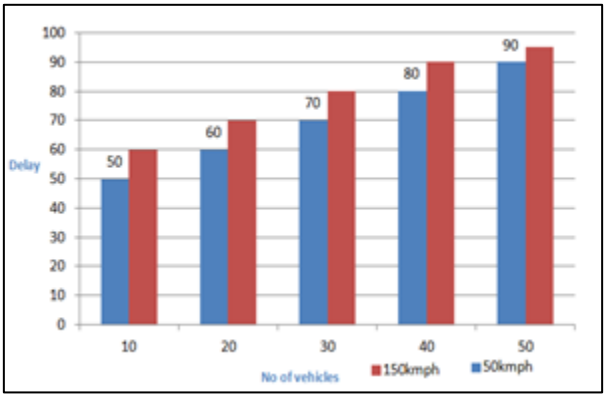

Fig. 2: showing the Delay for various no. of vehicles moving at 50 kmph and 150 kmph.

V. Conclusions

VANETs is silence not protected as well as disposed to different attacks so there is necessity of a accomplished, reliable as well as a tenable protocol which can be capable to rapidly organized and we propose enhancement in RSU maintain certificate base detection mechanism. Since, mostly peer-to-peer systems are disposed to Sybil attacks.

For designing more effective and practical Sybil defenses, we will future suggested an implementation depending on new detection algorithm. In this article, the challenge troubled to security i.e. Sybil attack has been studied. Then an Intrusion Detection System (IDS) mainly for Sybil attacks is implemented employing new Genetic Algorithm, and then examine with networks of disseminated node configurations.

References

[1] T. Zhou, R. R. Choudhury, P. Ning, K. Chakrabarty "P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks," Selected Areas in Communications, IEEE Journal Vol. 29, No. 3, 582-594, 2011.

[2] M. A. Razzaque, A. Salehi, S. M. Cheraghi, "Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the RoadAhead," Springer Berlin Heidelberg, In Wireless Networksand Securit, 107-132, 2013.

[3] Sood, M., & Vasudeva, A., Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network. In Compute/r Networks & communications (NetCom), Vol. 131, 3-13, 2013.

[4] Karlof, C., Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, Ad hoc Networks Journal (Elsevier,) vol. 1, 293 -315, 2003.

[5] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," In Proceedings of the 3rd international symposium on Information processing in sensor networks,259-268, 2004.
[6] G. Yan, S. Olariu, M. C. Weigle, "Providing VANET security through active position detection," Computer Communications, vol. 31, No. 12, 2883-2897, 2008.
[7] B. N. Levine, C. Shields, N. B. Margolin, "A survey of solutions to the Sybil attack," MA, University of Massachusetts: Amherst, 2006.
[8] A. Boukerche, H. A. Oliveira, E. F. Nakamura, A. A. Loureiro, "Vehicular adhoc networks: A new challenge for localization-based systems," Computer communications, Vol.31, No. 12,2838-2849, 2008.
[9] H. Wang, J. Wan, R. Liu, "A novel ranging method based on RSSI," Energy Procedia, Vol. 12, No. 1, 230-235, 2011.
[10] C.-H. Ou, "A roadside unit based localization scheme for vehicular ad hoc networks," Int. J of Communication Systems Wiley, No. 51, 123-130, 2012.
[11] J. T. Isaac,, S. Zeadally, J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks" Communications IET, Vol. 4, No. 7, 894-903, 2010.
[12] IJSER. K. Ibrahim, "Data aggregation and dissemination in vehicular ad-hoc networks," Doctoral dissertation, Old Dominion University, Norfolk, Virginia, 2011.
[13] P. Y. Shen, "An efficient public key management regime for vehicular ad hoc networks (VANETS)," Masters by Research thesis, Queensland University of Technology, 2011.
[14] G. Yan, W. Yang, J. Li, V. G. Ashok, "Active position security through dynamically tunable radar," In Mobile Ad hoc and Sensor Systems (MASS), IEEE 7th International Conference, 733-738, 2010.
[15] B. Xiao, B. Yu, C. Gao, "Detection and localization of Sybil nodes in VANETs," Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, 1-8, 2006.
[16] B. Yu, , C. Z. Xu, B. Xiao, "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing, Vol. 73, No. 6, 746–756, 2013.
[17] M. Demirbas, Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," In Proc. Of International Symposium on a World of Wireless, Mobile and Multimedia Networks, 564–570, 2006.
[18] S. Zhong, L.E. Li, Y.G. Liu, Y.R. Yang, "Privacy-reserving location based services for mobile users in wireless networks," Technical Report. YALEU/DCS/ TR-1297, Department of Computer Science, Yale University, 2004.
[19] S. Abbas, M. Merabti,, D. Llewellyn-Jones, K. Kifayat"Lightweight Sybil Attack Detection in MANETs," IEEE,Systems Journal, Vol. 7, No. 2, 236-248, 2013.
[20] B. Dutertre, S. Cheung, J. Levy, "Lightweight Key Management in Wireless Sensor Networks by LeveragingInitial Trust. Technical Report," SRI-SDL-04-02, SRI Int'l2004.
[21] S. Capkun, L. Buttyán, J. P. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans Mobile Computing, Vol. 2, No. 1, 52-64, 2003.
[22] S. Chang, Y. Qi, H. Zhu, J. Zhao, X. Shen, "Footprintdetecting Sybil attacks in urban vehicular networks," IEEETransactions on Parallel and Distributed Systems, Vol. 23, No6, 1103-1114, 2012.
[23] S. Park, B. Aslam, D. Turgut, C. C. Zou, "Defense againsSybil attack in the initial deployment stage of vehicular adhoc network based on roadside unit support," Security and Communication Networks, Vol. 6, No. 4, 523–538, 2013.
[24] Lu, R., Security and Privacy Preservation in Vehicular Social Networks, Doctoral dissertation, University of Waterloo, 2012.
[25] J.R Douceur, "The Sybil attack," Proceedings of the International Workshop on Peer to Peer Systems, 251–260, 2002.

