ISSN (e): 2250 – 3005 || Volume, 06 || Issue, 12|| December – 2016 ||
International Journal of Computational Engineering Research (IJCER)

Sybil attack in VANET

Amit A. Mane[1]
[1]M.E Student of Dept. of Electronics & Telecommunication, Vidyalankar Institute of Technology, Mumbai

ABSTRACT
Sybil attack can counterfeit the traffic scenario by sending false messages with multiple identities, which often causes a traffc jam and even leads to vehicular accidents in vehicular ad-hoc network (VANET). It is very difficult to be defended and detected, especially when it is launched by some conspired attackers using their legitimate identitiess. Since few years, Vehicular Ad hoc Networks deserve much attention. VANET technology uses moving cars as nodes in network to create a mobile network it turns every participating car into a wireless router or nodes, allowing cars approximately hundred to three hundred meters of each other to connect and in turn, create a network with a wide range. The development of wireless communication in VANET implies to take into account the need of security. In VANET, many attacks depends on possibility of the attacker generate multiple identities to simulate multiple nodes. Moreover, due to the limited communication range of a vehicle, the cooperation between nodes is essential. This necessity of cooperation shows the vulnerability of the need of fake nodes detection. In this paper we are checking Sybil attacks in VANET.

Keywords: *VANET, Sybil Attack, Security, DMV, RSU.*

I. INTRODUCTION

Mobile Ad Hoc Networks have undergone incredible growth of popularity during the last years. One of the example of these networks is Vehicular Ad-hoc Network (VANET). The use of wireless communication in VANET implies an always increasing number of potential applications in these networks such as driving assistance, road traffic information or emergency braking alert. All these applications need to exchange data with other vehicles that may be related to the driver safety. The need of confident communications between such critical applications becomes obvious. One possible threat is the creation of multiple fake nodes broadcasting false information. This attack is known as the Sybil attack. Several security schemes based on keys management have been proposed for intrusion detection. Sybil attacks refer to a malicious node illegitimately taking on multiple identities. In wireless networks, mobile nodes usually discover new neighbors by periodically broadcasting beacon packets, in which they claim their identities and positions. However, given the invisible nature of wireless communication, a malicious node can easily claim multiple identities without being detected. Identity authentication does not help prevent Sybil attacks in VANETs, since a malicious driver can still get additional identity information by non-technical means such as stealing, or simply borrowing from his friends. The goal of detecting Sybil attack is to ensure that each physical node is bound with only one legal identity. We refer to a vehicle as a node in the context of VANETs. We refer to a physical node claiming multiple identities as a malicious node and, correspondingly, the malicious node's fabricated identities as Sybil nodes. Further we emphasis in section [2] Architecture of VANET, in section [3] Threats to VANET, in section [4] analysis of defense mechanism, in section [5] comparison, in section [6] Conclusion, in section [7] References.

II. ARCHITECTURE OF VANET

There are two types of nodes in VANET; mobile nodes (On board Unit) and static nodes (Road Side Unit).An OBU consist of mobile network module and processing unit for on-board sensors and warning devices.

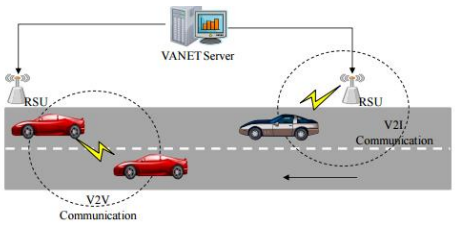

Fig 1. Inter vehicle communication and the components

The RSUs can be mounted on locations such as intersections, parking lots or gas stations. They can play a significant role in many applications such as a gate to the Internet.
Figure 1 shows a typical VANET. A vehicle is enabled with an onboard communication unit for vehicle to vehicle communicaton and vehicle to Infrastructure communication, and sensors and database units to collect environmental information(for example, vehicle location,vehicle speed,tire pressure).The communication unit of the access points are called RSU, which are connected to a VANET server by a wired network. The VANET server records all the data forwarded by the RSUs, and processes the data together with information from other data sources, for example, vehicle manufacturers, police,traffic management centers, and weather information centers.

III. THREAT TO VANET

In addition to Sybil Attack some more attack can also exposed in ad-hoc network through intruder.
3.1. Secretly listening to wireless messages: In this attack, an attacker tries to track a vehicle by giving two or more pseudonyms to nearby times and locations. Authors handle this by scattering the time and location of transmission, so that it is difficult to track the message sender.
3.2. Changes messages and re-broadcast: Schemes proposed in literature have solved this by authenticating the entire content of the message.
3.3. Replay messages at a different time and location: These attacks can be avoided by including timestamp and location information in the authenticated messages.
3.4. Impersonate other vehicles: With PKC techniques, impersonating another vehicle is difficult unless the attacker compromises the private keys of the pseudonyms, which are usually well protected.
3.5. Compromise RSBs: RSBs are semi-trusted parties, and may be compromised by the attackers. We assume that RSB compromise can be detected by the department of Motor vehicle, and the compromised RSB eventually revoked. However, attackers can still gain access to all information stored in the RSB.
3.6. Sybil Attack: False information reported by a single malicious vehicle may not be sufficiently convincing. Applications may require several vehicles to reinforce a particular information, before accepting it as truth. However, a serious problem arises when a malicious vehicle is able to pretend as multiple vehicles called a Sybil attack, and suitably reinforce false data. If benign entities are unable to recognize a Sybil attack [2], they will believe the false information, and base their decisions on it. Hence,
addressing this problem is crucial to practical vehicular network systems.

Fig.2 Sybil Attack [19]

As fig. 2 emphasis a hypothetical scenario of Sybil attack in VANET, node A creates multiple identities on the road and broadcast the bogus information to other vehicles.
3.7. Node Impersonation attack: In VANET each vehicle has a unique id and with the these ids each vehicle get identified in the VANET network. It becomes most important when an accident happens. In node impersonation attack an attacker can changes his/her identity and acts like a real originator of the message. An attacker receives the message from the originator of the message and changes the contents of the message for his/her benefits. After that an attacker sends this message to the other vehicles.

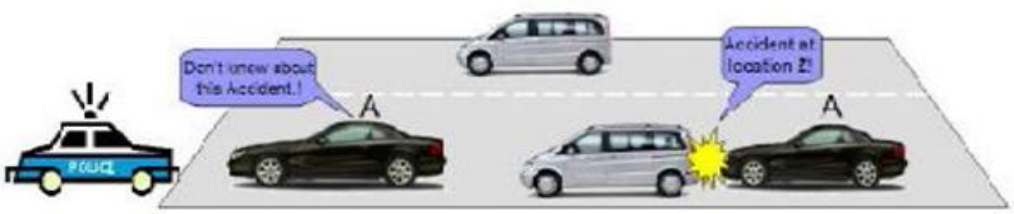

Fig. 3 Node Impersonation attack [19]

IV. ANALYSIS OF DEFENSE MECHANISM

We have different classification of defense mechanisms in VANETs as: (1) resource testing method, (2) position verification based method, and (3) encryption and authentication based methods. At the following we express some selected works in each domain to consider the problems for implementing each mechanism.

4.1. Defense Based on Resource Testing

Resource testing methods test vehicle's resources, such as radio resources [5], computational and memory resources and identification resources. In radio resource testing methods, each node sends a message for all of the neighboring nodes and then randomly selects a channel for listening to the response message. If the selected neighbor is real, it sends the response in the same channel; otherwise it cannot send the response message for its different Sybil entities at the same time on different channels and so Sybil attack is detected. Radio resource testing is based on the assumption that it is not possible for a device to send and receive on more than one channel at a same time. But in VANETs, attackers may have multiple channels and so this method is not applicable for vehicular network.Vehicles with MAC and IP addresses that are not recorded in a list identify as fakes[6]. This method is not sufficient for VANETs because a malicious vehicle may have multiple identities that are not belonging to any of vehicles in the network and it is possible to each of them be registered in the list. Moreover operation of broadcasting the registered identities for legitimate vehicles violates privacy of drivers. For computational resource testing, vehicles which fails to solve a puzzle are identified as fakes [6]. Malicious vehicle and its Sybil entities have shared resources such as memory, computational resources, IP and so on. We therefore can detect them with message tracking, monitoring vehicles and finding which vehicles are using shared resources for sending messages and processing of the received signal. This method requires special tools for network monitoring and message tracking. The goal of using resource testing based methods is not to prevent this attack. Rather, the aim is undermining this attack and restricting fake identities. But in many cases, attacker can obtain sufficient IDs for its purpose and so a successful attack occurs. Therefore these methods are not sufficient for using in VANETs [7].

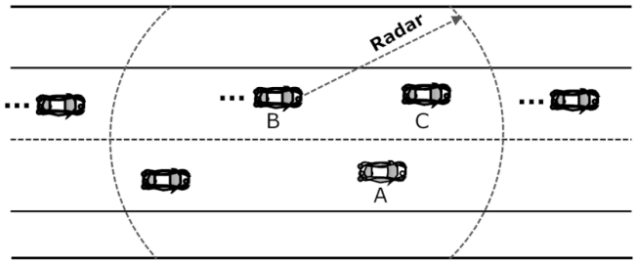

Figure 4. A possible Sybil Attack. A obtains C's position as Lc. A claims to victim B that its position is Lc, and its ID is IDa. B detects a vehicle is at Lc then concludes that it is the position of A [6].

4.2. Defense Based on Position Verification

We know that a vehicle can present t only one position at a time. This method takes the advantage of this fact For position based applications like traffic condition reports , collision avoidance, emergency alert, co-operative driving position based techniques are used for Sybil attack detection. The information about the position should be protect for working these applications in real world, because adversaries like malicious attackers can harm the VANET by obtaining the attacks such as dropping packets, modifying existing packets, inserting false packets and replying packets [6]. As stated in [8 ,9], localization schemas are divided into 2 categories: range-based and range free methods. In Range-based methods the estimated distance between a transmitter and receiver use it to compute the vehicle's position by using next process. We can estimate the distance with the help of three categories: Received Signal Strength Indicator (RSSI) based methods, time-based methods (e.g. Time Of Arrival (TOA) and Time Difference Of Arrival (TDOA)) and Angle Of Arrival (AOA) based methods [10].We can use range based method for estimating the distance and position verification as it has high accuracy in localization.

To prevent many of attacks against vehicle position and also Sybil attack, Yan et al. [11] propose a novel method based on the method i.e 'Seeing of believing'. In this method the author use onboard radar as virtual vehicle eye. The eyesight is limited for low radar transmission range. The vehicle can see neighbor vehicle which is at limited distance and also can hear their GPS coordinates reports. Then what is seen and what is heard get compared by vehicle. It is also possible for the vehicle to confirm actual position of neighbors and separates malicious vehicles from others. This method has certain limitations like : (1) the proposed method requires a new additional hardware that such a device doesn't exist at present [12], (2) the method fails when a target vehicle claims it's at the position of another existing vehicle that both are at the radio range of verifier vehicle [12]..

Sybil attack in this situation is not prevented by using this method and as Shen. P [13] has stated that this method is impractical for the vehicle which is out of radar range.but Yan et al.in [14] gave solution to this problem. He states that radar range in above method, is assumed to be constant, so if a target vehicle is out of verifier vehicle radar range, we can use intermediate vehicles. But using intermediate vehicles leads to some security problems [14]. For gaining trusted and safe position information about target vehicle, it is necessary to use more than one vehicle as intermediates. But if many of intermediate vehicles are starting to act as malicious players, verifier vehicle will be fooled (this problem is possible with collusion attack).
The problem of constant radar range is solved in Yan et al. [14].Authors proposed an onboard radar system which is dynamically configurable. If target vehicle is out of verifier vehicle radar range, radar can dynamically change its range by changing the signal sample size and so verifier vehicle at the most time can get the position information directly rather than using intermediate vehicles. Therefore vehicle positioning system is improved and last problem in Yan et al. [11] method has largely been solved.

4.3. Defense Based on Encryption and Authentication

In this method, Sybil attack can be detected with the help of authentication mechanism and public key cryptography**.** We can use trusted certificates to eliminate Sybil attack. But Public Key Infrastructure is key factor for most of the encryption and authentication methods.The bandwidth and resources consumption increase in public system as it consume more time and memory than symmetric key based systems which increase the message size. Chang et al. [22] proposed a new protocol called as a Footprint. This protocol preserves the privacy of the vehicles in the network. When a vehicle communicates with RSU, receives an authorized message upon reqest from RSU and hence presence of vehicle will be proved at a specific time. Each vehicle collects a set of consecutive authorized messages from RSUs get passed by them for unique vehicle identification. These authorized messages chain together and form a trajectory for the vehicle. To reduce complexity, only the last RSU signs the vehicle trajectory (chained authorize messages). In this Footprint protocol there are two conditions that help vehicles to remain unique in the network. In first condition authorized messages are signer-ambiguous and so after eavesdropping of the authorized messages it is not possible to detect a specific vehicle. In another condition, authorized messages are temporary linkable. This means we can recognize the messages issued by one RSU if they are issued within the same period of time. This condition is very important as sometimes without having knowledge about which RSU has signed the authorized message, malicious vehicle can detect trajectory of the vehicle by gathering authorized messages by the same RSU over the time. With this condition vehicle trajectories cannot be used for a long time. This scheme has some position-hidden features and preserves vehicle privacy.In this scheme the Sybil attack can be detect online. In this scheme the vehicle or RSU plays the role of conversion holder which initialize a conversation amongst vehicle. In this research two methods are proposed based on the type of certificates issued by RSUs.
First method is series of timestamp certificates in Fig. 2. In this method each vehicle receives a set of temporary timestamp certificates. This certificate contains the information about trajectory and time when it is passing through RSUs. Each timestamp certificate constituted of prior and current certificates issued by neighbor RSUs for this vehicle. The main process is to check similarity between aggregated timestamp series of different vehicles. Two similar timestamp series show a Sybil attack.
Second method is temporary certificate in Fig. 3. In this method each RSU has temporary key pairs and certificates for each vehicle for only a limited time and particular local area covering by the RSU. Some RSUs equipped with camera or other devices for physical authentication for issuing first certificate. For each vehicle.After receiving the first certificate and temporary key, the new key pair and certificate which is obtained upon certificate update request gets binds to previous certificates and make chained certificate.Each vehicle uses this certain temporary certificate for a single spatial interval and so Sybil attack with uniqueness of certificate is preserved.

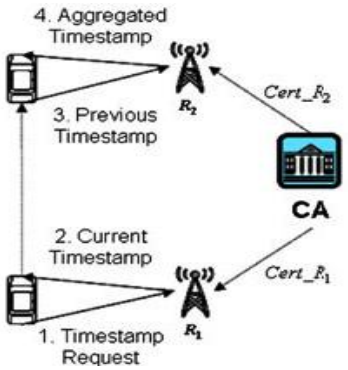

Figure 5.timestamp series based approach [23].

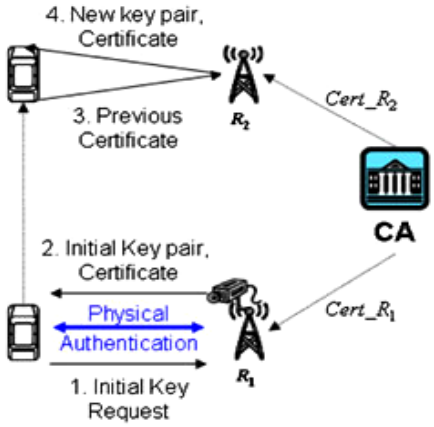

Figure 6. Temporary certificate based approach [23].

Advantage of timestamp series based approach is no requirement of physical authentication for the first visit with RSUs. But temporary certificate approach requires some of RSUs be equipped to extra devices for initial authentication.If we use some of RSUs equipped to physical authentication then first certificate not be issued until the vehicle meets an equipped RSU ans hence network is vulnerable in this time interval.

V. COMPARISON

It is difficult to firmly select a unique mechanism and method. Selection of a good method for detecting Sybil attack depends on the allocated costs, road architecture and number of vehicles in each country. Features of the existing methods can help to choice a suitable method. So In real world a good method meets the following requirements: (1) detection a large percentage of Sybil nodes for eliminating damage in VANET, (2) necessary time for discovering and removing of Sybil entities is an important factor that should be minimal, (3) privacy of drivers should be preserved, (4) doesn't need to additional high priced hardware, and (5) doesn't increase exchanging messages in the network.

We have not proposed resource testing methods, since they are not sufficient methods for Sybil attack detection with high accuracy in VANETs. Many of position verification methods are simple, have less computational complexity than authentication methods and they are distributed in processing. These are positive features for implementation. But they violate privacy and expose position and identifier information of vehicles. Moreover, distributed processing by vehicles in these methods, lead to messaging overhead. All of the authentication methods need an infrastructure for key distribution, revocation and so on. This infrastructure also may be necessary for many of other applications such as secure message exchanging, group communications, etc. In these methods privacy preserving and higher accuracy are positive features although they are complex for implementation and usually have less scalability than position verification methods.

VI. CONCLUSION

In this paper, we have discussed about defense methods against Sybil attack in VANETs. According to the studies in this area, each method has some advantages and disadvantages for implementing. Resource testing methods are not sufficient to implement for Sybil attack detection with high accuracy in VANETs. Authentication methods are more reliable and useful for message integrity, authenticity and privacy and there are suitable methods in this category for practical implementation in urban areas. In contrast, position verification methods are lightweight and easy for implementation and if they have high accuracy for position verification, we can use them for other security purposes such as position verification after receiving location information that periodically broadcast by vehicles for position related applications. So selection between two recent methods is depending on policies, requirements and allocated cost in each country.

REFERENCES

[1]. Lu, R., Security and Privacy Preservation in Vehicular Social Networks, Doctoral dissertation, University of Waterloo, 2012.
[2]. J. R. Douceur. The sybil attack. In *IPTPS*, pages 251–260, 2002.
[3]. Sood, M., & Vasudeva, A., Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network. In Computer 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 ad hoc 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]. 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]. Ajay rawat, Santosh Sharma, Rama Sushil, VANET: Security attack and its possible solution ISSN: 0976–7754 & E-ISSN