International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 6, Number 4 (2013), pp. 431-440

http://www.irphouse.com

Efficient and Feasible Methods to Detect Sybil Attack in VANET

Mukul Saini[1], Kaushal Kumar[2] and Kumar Vaibhav Bhatnagar[3]

[1]School of Information and Communication Technology, Gautam Buddha University, Greater Noida.
[2]School of Information and Communication Technology, Gautam Buddha University, Greater Noida.
[3]School of Information and Communication Technology, Gautam Buddha University, Greater Noida.

Abstract

Large scale node to node systems face security threats from malfunction or hostile remote computing elements. Node to node system commonly relies on the existence of multiple independent remote entities to mitigate the threat of hostile nodes. Sometime single faulty node can produce various identities leading to control of substantial fraction of the system. These attacks are called Sybil attacks. Since few years, Vehicular Ad hoc Networks deserve much attention. VANET is a technology that 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 rely on having the attacker generate multiple identities to simulate multiple nodes. The recent gain of interest for wireless communication in Vehicular Ad hoc Network (VANET) implies an always increasing number of applications in this kind of network. All these applications need to exchange data with other vehicles. The communication security problem must be taken into account due to the critical goal of safety related applications such as emergency brake. Moreover, due to the limited communication range of a vehicle, the cooperation between nodes is essential. This necessity of cooperation shows the vulnerability of these networks and

the need of fake nodes detection. In this paper we are checking Sybil attacks in VANET by power level of signal coming from same node.

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

1. Introduction

Mobile Ad Hoc Networks have undergone incredible growth of popularity during the last years. One of the most practical 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 and intruder nodes revocation. Sybil attacks refer to a malicious node illegitimately taking on multiple identities. In wireless networks, mobile nodes usually discover new neighbours 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 attacks 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] Detection schemes, in section [5] Future work, in section [6] Conclusion, in section [7] References.

2. Architecture of VANET

2.1. Department of Motor Vehicle (DMV)-

DMV is the trusted party that maintains vehicle records, and distributes certified pseudonyms to vehicles when they apply/renew their registration. The DMV has enough resources to generate pseudonyms quickly and store all the vehicle-related information and is referred to when any authoritative clarification is necessary. However, excessive communication can cause the DMV to become a bottleneck.

2.2. Road Side Unit (RSU)

RSU are wireless access points, provisioned along the road to act as intermediates to the DMV. The RSBs monitor vehicular activity through overhearing, and report suspicious behaviour to the DMV. The RSBs may get compromised, hence the DMV cannot use them for critical functions. However, they can be used to improve the scalability of a system.

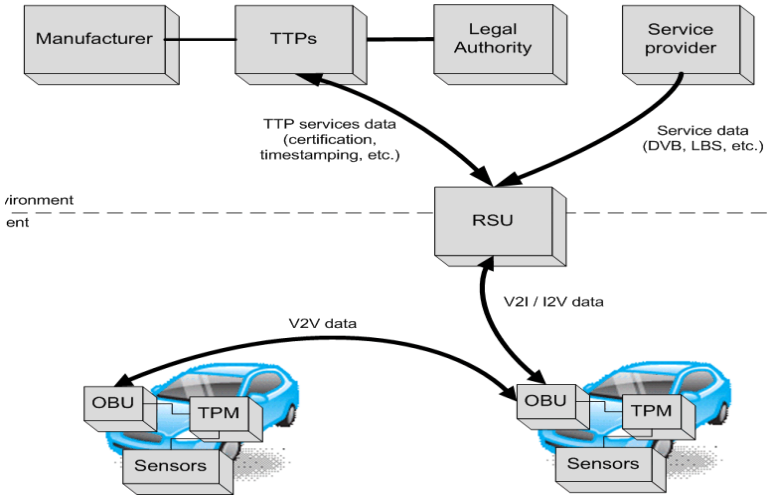

Fig. 1 [18]

2.3. Node/Vehicles-

Vehicles are un-trusted parties. They sense events on the road, and communicate them to other vehicles and agencies in a multi-hop manner. The events are signed with a pseudonym, selected from those that were assigned to them by the DMV. The vision for vehicular ad hoc networks (VANETs) includes the frequent exchange of data by vehicles (or nodes) to facilitate route planning, road safety and e-commerce applications. Network security is clearly important for each of these applications. The traditional approach to network security involves a key management solution that allows for data integrity and the authentication of network \insiders". Besides raising privacy concerns and being unwieldy for a VANET, we believe this approach solves the wrong problem. In a VANET, far simpler attacks than data modification exist, such as for example transmitting fraudulent data about road congestion or vehicle position, and such attacks can be quite damaging.

3. Threat to VANET

In addition to Sybil Attack some more attack can also exposed in ad-hoc network through intruder.

3.1. Eavesdrop on wireless messages: In this attack, an attacker tries to track a vehicle by associating two or more pseudonyms to nearby times and locations. Authors in propose to handle this by scattering the time and location of transmission, so that it is difficult to track the message sender.

3.2. Modify 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 addressed 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 DMV, 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.

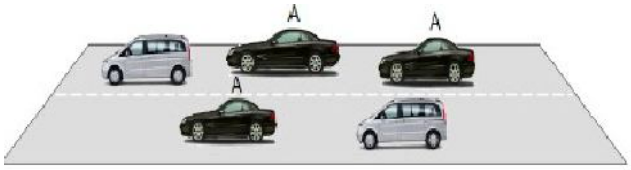

Fig.2 [19]

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 help of these ids each vehicle is 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.

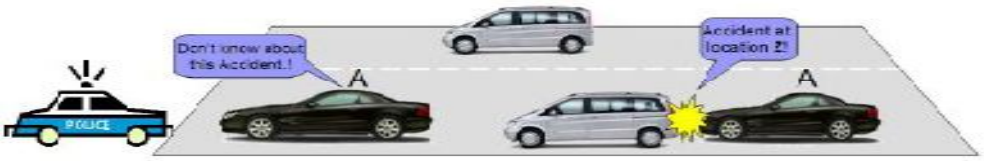

Fig. 3[19]

3.8. Message suppression: In this attacker can selectively drop packets from the network which may contain critical information for the receiver. For example an attacker might remove the congestion alerts it receives in order to prevent the nodes to select an alternative path to destination and force them to wait in traffic. The attacker may use these packets again later to get the benefits. The main objective of the attacker would be to prevent the authorities and RSU to know about the collision.

4. Detection Schemes

4.1. Resources testing: The method propose resources testing as a defences against Sybil attack. This resource testing is based on the assumption that each physical entity is limited in some resource. The method described in uses computational puzzles to test nodes computational resources. The authors show that this approach is not suitable to ad-hoc networks, and hence typically VANET, because the attacker can have more computational resources than an honest node. Instead, they propose a radio resource testing.

4.2. Use of public key cryptography: The authors try to solve the security problem of the Sybil attack with public key cryptography. The authors propose the use of a PKI for VANET (VPKI). They describe a complete solution to provide security of communications and they address the problem of key distribution. They also propose a mechanism for key revocation. As each vehicle may be authenticated with its public key, the Sybil attack is always detected. Nevertheless, deploying PKI for VANET is an heavy and difficult solution that must be tested to assess its possible use in a real world.

4.3. Assuming a given propagation model: Some papers dealing with detection of Sybil attack in wireless networks assume a predefined propagation model. They use the received signal power to deduce some inconsistencies between the power of the

signal and the claimed position. In, a node collects signal strength measurement from other nodes and estimates their new position according to a given propagation model. A node is considered suspect if its claimed position is too far from the evaluated one.

4.4. Secure positioning: Another possibility to defeat Sybil attack is to provide a secure positioning system and the reliability of the position claimed by vehicles. The authors propose methods for determining a transmitting peer's node location using signal properties and trusted peers collaboration for identification and authentication purposes. The method uses characteristics such as signal strength and direction. The authors present a novel approach called verifiable Multi alteration, using distance bounding protocol and base stations to provide secure positioning. They also assume that all network nodes can establish pair wise secret keys.

4.5. Distinguish ability: the authors propose an approach to evaluate the validity of VANET data. Data are correlated and scored; data with the higher score will be accepted. The proposed model notably rely on the fact that nodes are equipped with specific devices allowing to tie a message with a physical sources.

4.6. Signal strength based position verification: position verification scheme relies on monitoring the signal strength of periodical beacons. For clarity of description, we define three categories of nodes' roles: claimer, witness, and verifier. Each node would periodically play all these roles, that is, each node is a claimer, a witness as well as a verifier but at various moments and for various purposes.

4.6.1. Claimer. Each node periodically broadcasts a beacon message at beacon intervals, tb, for the purpose of neighbour discovery. In the beacon message, it claims its identity and position such as GPS position. At this moment, we name the node as a claimer. The goal of our scheme is to verify its claimed position.

4.6.2. **Witness**. All neighbouring nodes, within the signal range of the claimer, would receive the previous beacon message. They measure the signal strength and save the corresponding neighbour information in their memory. Next time they broadcast a beacon message, they will attach their neighbour list, including the signal strength measurements for each received beacon, to the beacon message. We name these nodes performing measurement and reporting measurements as witnesses.

4.6.3. Verifier. After receiving a beacon message, a node waits for a verifying interval, tv, during which it collects enough signal strength measurements concerning the previous beacon message from neighbouring witnesses. tv may be a little longer than the beacon interval tb, since after another interval of tb, each neighbouring witness should have broadcasted a beacon containing the expected measurements. With the collected measurements, the node can locally compute an estimated position of the claimer, for example, by performing MMSE (Minimum Mean-Square Error) on

the collected signal strength and a pre-defined radio model. We call a node performing verification a verifier. To obtain the estimated position, we first calculate the mean square error:

$$MSE(p) = \frac{\sum_{i=1}^{k}(S_r(w_i) - S_m(w_i, p))^2}{k}$$

Sybil attack can be detected if multiple traffic messages contain very similar series of timestamps. These messages can be highly where p is a potential position of the claimer, k is the number of witnesses, Sr is the received signal strength at witness wi, Sm is the calculated signal strength at wi obtained from radio propagation model. By varying p, we can minimize MSE and finally get the optimal estimated position ˆp. If the estimated position of a claimer is far away from its claimed position, we regard this node as a suspect node. Note that due to the unstable and irregular nature of RF (Radio Frequency), we still cannot assert, based on the results of this simple computation , that a Sybil attack is happening.

4.7. Based on Time Stamp Series data propagation: On simple structured roadways that have multiple lanes and have no traffic congestions, vehicles move dynamically at different speeds and move independently. Based on this phenomenon, we discover that it would be rare for arbitrary two vehicles to pass through a few different RSUs far apart from each other always at the same time. Therefore, if a traffic message sent out by any vehicle contains several timestamps issued to this vehicle by the previously passed RSUs suspected as Sybil messages created by a single vehicle. This approach requires that only RSUs can issue timestamps and a vehicle cannot use a timestamp obtained by others. Therefore, in our design,, each timestamp is digitally signed by the issuing RSU and a timestamp obtained by a vehicle contains this vehicle's self-generated public key, which cannot be used by others who do not know the corresponding private key. A vehicle may create multiple requests to obtain multiple timestamps from a single RSU. However, multiple timestamps obtained by a single vehicle in a single transmission range of an RSU must be very close in their timestamps. As aforementioned, traffic messages with these timestamps can be easily detected as Sybil messages.

4.8. Privacy-Preserving Detection of Abuses of Pseudonyms (PPDAP): this scheme assuming that the RSBs have received the keys from the DMV, and can therefore compute coarse-grained hash values of a given pseudonym. Now, when vehicles communicate, the RSBs overhear all the vehicles that are within their communication range. For each event (ti, lj , em), the different pseudonyms used to sign the event are gathered in a list, Li,j,m. When all events with time ti have been collected (say at time ti+1 + _), the RSB goes through each pseudonym p 2 Li,j,m and computes the coarse-grained hash value Hc(p|kc). If 9p, p′ 2 Li,j,m such that Hc(p|kc) = Hc(p′|kc), then the RSB notices that there are at least two pseudonyms of the same

coarse-grained hash value used to sign the event (ti, lj , em). This can be either (i) a Sybil attack where one vehicle is using multiple pseudonyms to report the same event, or (ii) a false alarm, where an event is reported by multiple vehicles, but two or more of them coincidentally have their pseudonyms mapped to the same coarse-grained hash value. The RSB cannot discriminate between (i) and (ii) and it sends a suspicion report to the DMV securely. The RSB suspicion report contains the event (ti, lj , em), the computed coarse-grained hash value , the multiple pseudonyms that hash to and other signatures and certificates accompanying the pseudonyms. on receiving an RSB report, the DMV first verifies the signatures to prevent a compromised RSB from implicating a benign vehicle. If the RSB proves to be bona fide, the DMV computes the fine-grained hash value = Hf (p|kf) for each pseudonym p in the RSB report. If 9p, p′ in the report such that Hf (p|kf) = Hf (p′|kf), the DMV concludes that p and p′ are from the same vehicle that has attempted a Sybil attack. The DMV then figures out the malicious vehicle from the computed secret plate number and takes further actions. Thus, the use of obviates the need for storing the relationship between vehicles and pseudonyms. every Sybil attack is guaranteed to be detected. The burden on the DMV depends on the number of distinct coarse-grained hash values and the number of vehicles reporting one event. If the number of coarse-grained hash values is much larger than the number of vehicles reporting an event, then false alarms are much less likely. However, the number of vehicles reporting one event can be very large. If we increase the number of coarse-grained hash values accordingly, the compromise of an RSB can adversely affect the anonymity of vehicles.

5. Future Work

Users want safety and security on the road in future and it may be possible by implementing secure and safe VANET applications which is a rising technology. This technology is a rich area for attackers who try to change the contents of the safe and non safe applications to misguide the users of the network with their malicious attacks. In this paper we present some possible attacks and their solutions. In future we intend to develop the system for detecting the critical attacks and verifying it through simulation by applying our novel idea on the procedure to protect the safe messages.

6. Conclusion

This paper include various types of attack involve in VANET and their detection mechanism also provided. We showed that only certain areas may contain cheated nodes. As we have characterized such areas, we think that the results given in this paper provide a good framework to elaborate realistic test suites for Sybil attack detection methods and to evaluate them from an objective point of view.

References

[1] Chipcon. Cc1000 radio datasheet. www.chipcon.com/files/ CC1000 Data Sheet 2 3.pdf, 2003.

[2] J. R. Douceur. The sybil attack. In *IPTPS*, pages 251–260, 2002.

[3] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler. The nesc language: A holistic approach to networked embedded systems. In *PLDI*, pages 1–11, 2003.

[4] P. Golle, D. Greene, and J. Staddon. Detecting and correcting malicious data in vanets. In *VANET*, pages 29–37, 2004.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy efficient communication protocol for wireless microsensor networks. In *HICSS*, page 8020, 2000.

[6] J. Hill and D. Culler. Mica: a wireless platform for deeply embedded networks. *IEEE micro*, 22(6):12–24, 2002.

[7] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for network sensors. *ASPLOS*, pages 93–104, 2000.

[8] D. Kotz, C. Newport, R. S. Gray, J. Liu, Y. Yuan, and C. Elliott. Experimental evaluation of wireless simulation assumptions. In *MSWiM*, pages 78–82, 2004.

[9] L. Li, J. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer. A cone-based distributed topology-control algorithm for wireless multihop networks. *IEEE/ACM Trans. Netw.*, 13(1):147–159, 2005. N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In Proc. of the 2003 ACM workshop on Wireless Security (WiSe 2003), pp. 1-10, 2003.

[10] P. Golle, D. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETs. In Proc. of the 1st ACM international workshop on Vehicular ad hoc networks (VANET 2004), pp. 29-37, 2004.

[11] G. Zhou, T. He, S. Krishnamurthy, J.A. Stankovic. Impact of Radio Irregularity on Wireless Sensor Networks. In Proc. of the 2nd international conference on Mobile systems, applications, and services (MobiSys 2004), pp. 125-138, 2004.

[12] S. Capkun and J.-P. Hubaux. Secure Positioning of Wireless Devices with Application to Sensor Networks. In Proc. of Infocom 2005, pp. 1917-1928, 2005.

[13] T. S. Rappaport. Wireless communications, principles and practice. Prentice Hall, 1996.

[14] R.M. Yadumurthy, A. Chimalakonda, M. Sadashivaiah, and R. Makanaboyina. Reliable MAC Broadcast Protocol in Directional and Omni-directional Transmissions for Vehicular Ad hoc Networks. In Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET 2005), pp. 10-19, 2005.

[15] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter. MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks. In Proc. of the 1st ACM international workshop on Vehicular ad hoc networks (VANET 2004), pp. 47-56, 2004.

[16] M. Torrent-Moreno, H. Hartenstein, P. Santi. Fair Sharing of Bandwidth in VANETs. In Proc. of ACM Workshop on Vehicular Ad Hoc Networks (VANET 2005), pp. 49-58, 2005.

[17] G. Korkmaz and E. Ekici. Urban Multi-hop Broadcast Protocol for Inter-Vehicle Communication Systems. In Proc. of the 1st ACM international workshop on Vehicular ad hoc networks (VANET 2004), pp. 76-85, 2004. 8

[18] Jose Maria de Fuentes, Ana Isabel, Gonzalez tabals, Auturo Ribagorda overview of security issue in vehicular Ad-hoc Network

[19] Ajay rawat, Santosh Sharma, Rama Sushil, VANET: Security attack and its possible solution ISSN: 0976–7754 & E-ISSN