A ROUTE MAP FOR DETECTING SYBIL ATTACKS IN URBAN VEHICULAR NETWORKS

[1] NAGESWARA REDDY KARUKULA, [2] SUNAR MOHAMMED FAROOQ

[1, 2] ASST.PROFESSOR, CSE DEPARTMENT, AVR &SVR CET

ABSTRACT: *Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack, where a node illegitimately claims multiple identities. In urban vehicular networks, the location privacy of anonymous vehicles is highly concerned and anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining excessively large influence. In Vehicular Ad Hoc Networks (VANETs), the vehicular scenario requires smart signaling, smart road maintenance and other services. A brand new security issue is that the semi-trusted Road Side Units (RSUs) may be compromised. The objective of our work is to propose a Threshold ElGamal system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion with the malicious vehicles. By analyzing the packet loss tolerance for security performance by PPI Algorithm demonstration, followed by a discussion on the threshold our method can promote security with low overhead in Emergency Braking Notification and does not increase overhead in and Decentralized Floating Car Data during security promotion.*

Index Terms: Sybil Attack, Qos, Ppialg, Location Privacy, Urban Vehicular Networks, Security

I. INTRODUCTION

Over the past two decades, vehicular networks have been emerging as a cornerstone of the next-generation Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. In vehicular networks, moving vehicles are enabled to communicate with each other via inter vehicle communications as well as with road-side units (RSUs) in vicinity via roadside-to-vehicle communications. In urban vehicular networks where the privacy, especially the location privacy of vehicles should be guaranteed vehicles need to be verified in an anonymous manner. A wide spectrum of applications in such a network relies on collaboration and information aggregation among participating vehicles. Without identities of participants, such applications are vulnerable to the Sybil attack where malicious vehicle masquerades as multiple identities, overwhelmingly influencing the result. The consequence ofSybil attack happening in vehicular networks as shown in fig1 can be vital. For example, in safety-related applications such as hazard warning, collision avoidance, and passing assistance, biased results caused by a Sybil attack can lead to severe car accidents. Therefore, it is of great importance to detect Sybil attacks from the very beginning of their happening. Detecting Sybil attacks in urban vehicular networks, however, is very challenging. The First, vehicles are anonymous. There are no chains of trust linking claimed identities to real vehicles. Second, location privacy of vehicles is of great concern. Location information of vehicles can be very confidential. [1,2]Due to high mobility of vehicles, a moving vehicle can have only several seconds to communicate with another occasionally encountered vehicle. It is difficult to establish certain trustworthiness among communicating vehicles in such a short time. This makes it easy for a malicious vehicle to generate a hostile identity but very hard for others to validate. Furthermore, short conversations among vehicles call for online Sybil attack detection. The detection scheme fails if a Sybil attack is detected after the attack has terminated.

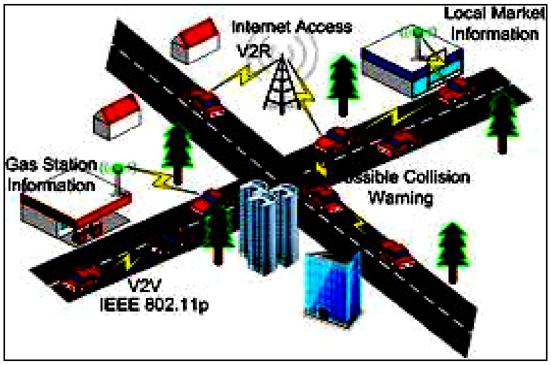


Fig1:vehicular internetwork

II.INTER-VEHICLE COMMUNICATIONS:

Inter-vehicle communications allow a mobile vehicle to communicate with its surrounding environment, mobile or fixed networks. More specifically, vehicular nodes can communicate with their peers either via vehicle-to-vehicle communications or through the fixed roadside infrastructure. The communication and the delivery of information may range from motion data (speed, direction, location, etc.) to Internet media content, through the wide variety of supported applications that operate in a vehicular network. The demands of the applications that operate in the vehicular environment, along with the properties and special traits of the vehicular access networks define the design and the requirements of the security provision, the quality of service provision, and the routing process within the network. While it was first described and formalized by Douceur, the Sybil attack has been a severe and pervasive problem in many forms. In a Sybil attack, an attacker can launch a Sybil attack by forging multiple identifies, gaining a disproportionately large influence. In the literature, there have been many different approaches proposed to detect or mitigate the attack. Many studies have followed Douceur's approach, focusing on how to establish trust between participating entities based on trusted public key cryptographies or certificates in distributed systems, for example, P2P systems,[3,4]sensor networks and mobile ad hoc networks. Although deploying trusted certificates is the only approach that has the potential to completely eliminate Sybil attacks, it also violates both anonymity and location has the problem of key revocation which is challenging, particularly in wireless mobile networks.

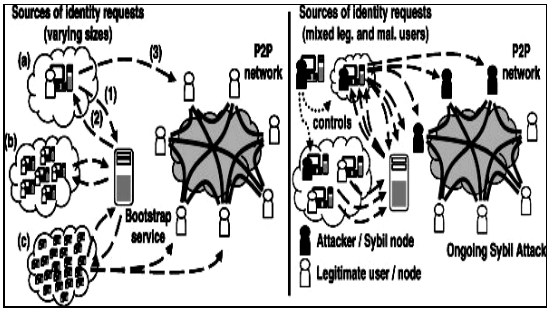


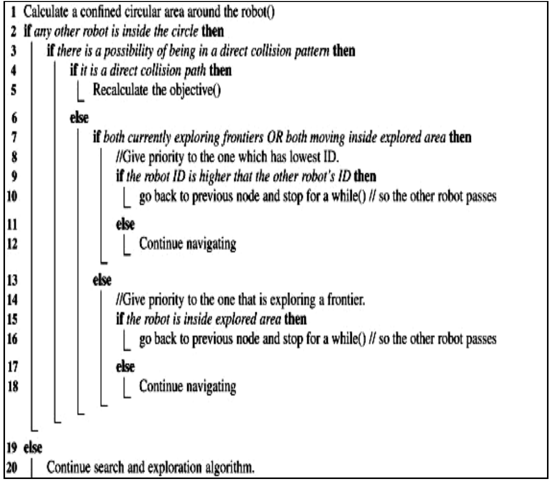
Fig2:sybell node/Attacker in p2p network

As shown in fig2 vehicular networks, this assumption cannot hold since malicious vehicles can easily have more powerful resources than the normal vehicles. Sybil Guard is an interesting scheme studying the social network among entities. In this scheme, human established real-world trust relationship among users is used for detecting Sybil attacks. Since even the attacker can generate as many as Sybil identities, building relationship between honest users and Sybil identities is much harder. Thus, there exists a small "cut" on the graph of trust relationship between the forged identities and the real ones. This is because vehicles are highly mobile. Communications often happen among temporarily met and unfamiliar vehicles. To exploit the fact that one single vehicle cannot present at multiple locations at the same time, Bouassida have proposed a detection mechanism utilizing localization technique based on[5,6] Received Signal Strength Indication (RSSI). In this scheme, by successively measuring the RSSI variations, the relative locations among vehicles in vicinity can be estimated. Identities with the same estimated locations are considered as Sybil vehicles. In practice, the complicated outdoor environments can dramatically affect the wireless signal propagation so that RSSI measurements are highly time variant even measured at the same location.

III.PATH PLANNING IMPROVEMENT ALGORITHM:

Xiao have proposed a Sybil attack detection scheme where the location of a particular vehicle can be determined by the RSSI measurements taken at other participating vehicles. In the scheme, the trust authority distributes a number of pseudonyms for each vehicle. Abused pseudonyms can be detected by RSUs. Since RSUs are heavily involved in the detection process, this scheme requires the full coverage of RSUs in the field. It is infeasible in practice due to the prohibitive cost.

Furthermore, in such a scheme, vehicles should managed by a centralized trusted enter. Each time RSU detects suspicious pseudonyms, it should send all the pseudonyms to the trust center for further decision, which makes the trust center be the bottleneck of the detection. The most relevant work to Footprint is the Sybil attack detection [7] schemes proposed in. In these schemes, a number of location information reports about a vehicle are required for identification. RSU periodically broadcasts an authorized time stamp to vehicles in its vicinity as the proof of appearance at this location. By using PPI Algorithm we improve the path related Vehicles collect these authorized time stamps which can be used for future identity verification.



```
Calculate a confined circular area around the robot()
if any other robot is inside the circle then
    if there is a possibility of being in a direct collision pattern then
        if it is a direct collision path then
            Recalculate the objective()
        else
            if both currently exploring frontiers OR both moving inside explored area then
                //Give priority to the one which has lowest ID.
                if the robot ID is higher that the other robot's ID then
                    go back to previous node and stop for a while() // so the other robot passes
                else
                    Continue navigating
            else
                //Give priority to the one that is exploring a frontier.
                if the robot is inside explored area then
                    go back to previous node and stop for a while() // so the other robot passes
                else
                    Continue navigating
else
    Continue search and exploration algorithm.
```

Trajectories made up of consecutive time stamps and the corresponding public keys of RSUs are used for identification. However, these schemes did not take location privacy into consideration since RSUs use long term identities to generate signatures. As a result, the location information of a vehicle can be inferred from the RSU signatures it collects. In Footprint, authorized messages issued from RSUs are signer-ambiguous which means the information about the location where the authorized message was issued is concealed, and temporarily linkable which means using a single trajectory for long term identification of a vehicle is prohibited. Therefore, the privacy of location information and identity of vehicles are preserved in Footprint.

IV.ATTACKS

1]Denial of Service (DoS):Overwhelm computational or network capacity and Dangerous if users rely on the service and Message suppression attacks at edges as shown in fig

2]Drop congestion alerts

Fabrication: Lie about congestion ahead or lie about identity

Alteration attacks: Replay transmissions to simulate congestion

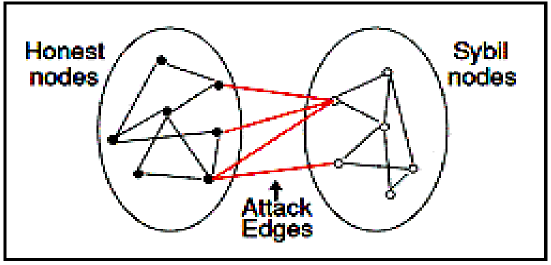


Fig3:attack edges

In order to launch a Sybil attack, a malicious vehicle must try to present multiple distinct identities. This can be achieved by either generating legal identities or by impersonating other normal vehicles. With the following capabilities, an attacker may succeed to launch a Sybil attack in vehicular networks:

4.1 Heterogeneous configuration: malicious vehicles can have more communication and computation resources than honest vehicles. For example, a malicious vehicle can mount multiple wireless cards, physically representing different communication entities. Furthermore, having more powerful resources can also fail those resource testing schemes for detecting Sybil attacks.

4.2 Message manipulation: due to the nature of open wireless channels, the attacker can eavesdrop on nearby communications of other parties. Thus, it is possible that the attacker gets and interpolates critical information needed to impersonate others.

V.DESIGN GOALS:

The design of a Sybil attack detection scheme in urban vehicular networks should achieve three goals:

1.Location privacy preservation: a particular vehicle would not like to expose its location information to other vehicles and RSUs as well since such information can be confidential. The detection scheme should [8] prevent the location information of vehicles from being leaked.

2.Online detection :when a Sybil attack is launched, the detection scheme should react before the attack has terminated. Otherwise, the attacker could already achieve its purpose.

3.Independent detection the essence of Sybil attacks happening is that the decision is made based on group negotiations. To eliminate the possibility that a Sybil attack is launched against the detection itself, the detection should be conducted independently by the verifier without collaboration with others.

VI.VEHICLE TRAJECTORY

Message generation In order to be location hidden, authorized messages issued for vehicles from an RSU should possess two properties. The temporarily linkable property requires two authorized messages are recognizable if and only if they are generated by the same RSU within the same given period of time.

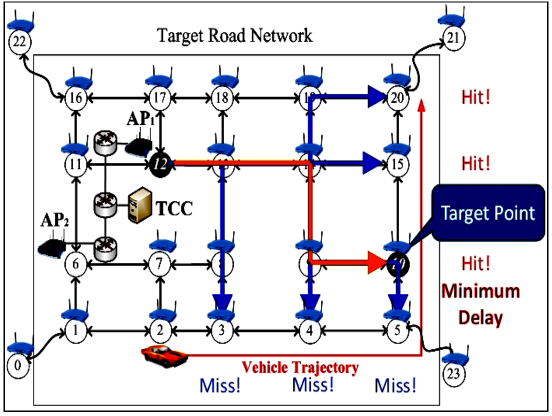


Fig4:vehicle Trajectory

VII.SYBIL ATTACK DETECTION:

1]Vehicular ad-hoc networks rely heavily on node-to-node communication with Potential for malicious data. and

2]VANETs need a method for evaluating the validity of data

3]Nodes search for explanations for the data they receive and accept the data based on highest score first with Nodes can tell “at least some” other nodes apart from one another and second Parsimony argument accurately reflects adversarial behavior in a VANET.

4]Each node builds a world view in an offline mode

A]Rules: two vehicles cannot occupy the same position at the same time, etc.

B]Statistics: vehicles rarely travel faster than 100 MPH, etc.

5]Density combined with mobility supports parsimony

VIII.PRIVACY:

Trade-off between privacy and ability to detect and correct malicious data with Changing keys increases privacy but hinders detection and correction of malicious data and An isolated node regularly reporting its position changes its key. Easy to assume the new key belongs to the same node based on trajectories. Improving security as shown in fig5 Suggestions for changing keys and Change keys at synchronized times and Introduce gaps in data reported near key changes and Change keys when nodes are near one another.

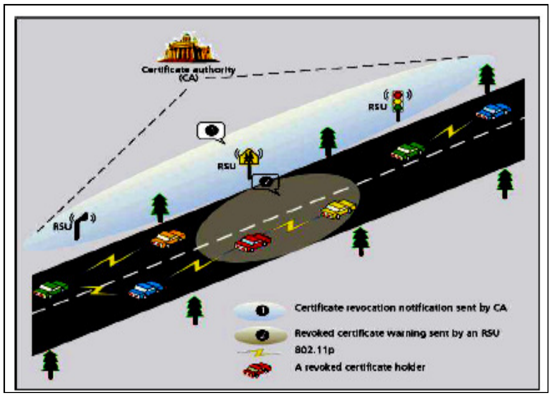

Certificate authority (CA)
RSU
RSU
RSU
Certificate revocation notification sent by CA
Revoked certificate warning sent by an RSU
802.11p
A revoked certificate holder

Fig 5: Security Architecture

Nodes may record an observation if the location of the event is within their observation range the entire duration of the event and Assertions recorded by a node are instantaneously available to all other nodes with Value of data declines the further away from the event it is transmitted, dealing with a small area. Accurate and precise sensor data is important in identifying malicious nodes and data. Finding the most likely explanation in each case will be difficult Manageable when there are only a few malicious nodes and Could be accelerated by having nodes share [9,10] candidate explanations with each other. During a conversation, upon request from the conversation holder, all participating vehicles provide their trajectory-embedded authorized messages issued within specified event for identification. With submitted messages, the conversation holder verifies each trajectory and refuses those vehicles that fail the message verification. After that, the conversation holder conducts online Sybil attack detection before further proceeding with the conversation.RSU Neighboring Relationship and the Freedom of Trajectory Generation can Facilitate Sybil Trajectory Generation. In the Above Figure, Neighboring RSUs (Denoted by Dots) are connected with Dash Line. The Solid Arrows Indicate the Actual Sequence of RSUs a Malicious Meet and the Dash Arrow Presents a Possible Forged Trajectory.

IX.QUALITY OF SERVICE:

Although current efforts [ ] have attempted to optimize the available bandwidth to improve latency of messages, QoS support over SecVANETs remains a challenge because of the various factors we discussed earlier. We need to develop adaptive QoS routing approaches that can quickly and efficiently set up new routes when current routing paths becomes no longer available as a result of changes in node velocity, node positioning, network topology or distance between vehicular nodes. Well-defined QoS metrics for SecVANETs in fig6 still need to be agreed upon given the wide variations of performance metrics (including popular QoS ones such as delay and jitter) being used by the VANET community. Initial results by Boban et al. [11] demonstrate that the real QoS challenges are packet delivery ratio and connection duration (rather than typical QoS metrics such as end-to-end delay and jitter [12]) are hard to achieve for unicast-based applications. Although multipath routing improves global QoS [13] metrics we need more in-depth research to investigate the impact of the multipath approach on the available bandwidth and processing load of intermediate vehicular nodes involved in the various paths used. for providing QoS we improve securing VANET as shown in below fig6

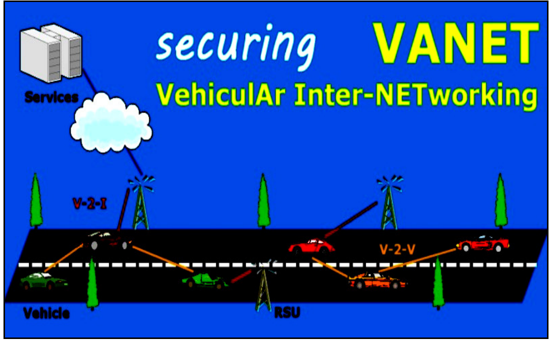


Fig6: securing VANET

X. RESULT ANALYSIS:

Novel broadcasting algorithms are required to minimize broadcast storms that arise as a result of packet flooding. Wireless technology used by VANET is not well suited at handling broadcast Transmissions because of frequent message collisions leading to frequent retransmissions by vehicles. These collisions in turn affect the message delivery rate and increases the delivery time of the messages. Further research is required to investigate intelligent flooding schemes, distributed algorithms that can efficiently handle asymmetric communications among vehicles for different transmission ranges. Considering the scenario where a small fraction of RSUs are compromised and developing cost-efficient techniques to fast detect the corruption of an RSU. Here we delve into designing better linkable signer ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced. A brand new security issue is that the semi trusted Road Side Units (RSUs) may be compromised by providing a Threshold ElGamal system based key management scheme for safeguarding VANET from the

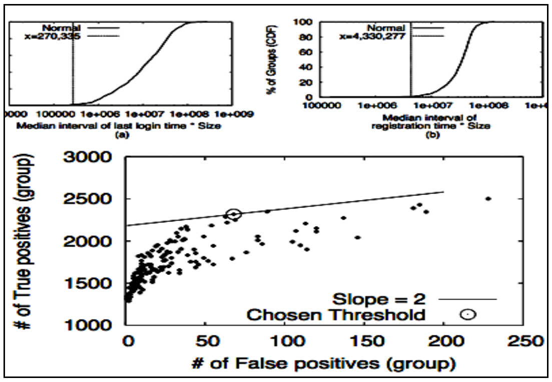


Fig7: Median interaval of last login time

and size and Median interval of
registration time+size
compromised RSUs and their collusion with the malicious vehicles. Providing reliable broadcast messages with minimal overheads for VANETs introduces[14,15]several other technical challenges including: Median interaval of last login time and size and Median interval of registration time+size which is shown in fig7 the selection of the next forwarding node, the maintenance of communications among vehicles as they leave and join a group, hidden terminal problems since broadcast messages do not use the typical Request to Sender/Clear to Sender (RTS/CTS) message exchange.

XI. Conclusion

In the past decade, many VANET projects around the world have been undertaken and several VANET standards have been developed to improve vehicle-to-vehicle or vehicle-to infrastructure communications. In this work, we reviewed some of the main areas that researchers have focused on in the last few years and these include security, routing, QoS, and broadcasting techniques and we highlighted the most salient results achieved to date. Secure routing in VANET have been emerging as a cornerstone of Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme. Utilizing social relationship among trajectories, Footprint can find and eliminate Sybil trajectories. The Footprint design can be incrementally implemented in a large city. We hope this taxonomy on VANET simulators will be helpful to future VANET researchers in choosing the optimal VANET simulator best suited for their VANET design goals. Finally, we discussed some of the challenges that still need to be addressed in order to enable the deployment of VANET technologies,

REFERENCES

[1] S. Capkun and JP. Hubaux. Secure positioning of wireless devices with application to sensor networks. In IEEE INFOCOM 2005, volume 3, pages 1917–1928, 2005.

[2] J. Douceur. The Sybil Attack. In First International Workshop on Peer- to-Peer Systems, pages 251–260, 2002.

[3] P. Golle, D. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETS. In ACM international workshop on Vehicular ad hoc networks, pages 29–37, 2004.

[4] Gilles Guette and Bertrand Ducourthial. On the Sybil attack detection in VANET (extended version). Technical report, Heudiasyc Laboratory, University of Compigne, 2007.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S.Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Symp. Operating Systems Design and Implementation (OSDI '02), pp. 299-314, Dec. 2002.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Int'l Symp. Information Processing in Sensor Networks (IPSN '04), pp. 259-268, Apr. 2004.

[7] M. Raya, P. Papadimitratos, and JP. Hubaux. Securing Vehicular Communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 13(5):8–15, 2006.

[8] T. Suen and A. Yasinsac. Ad Hoc Network Security: Peer Identification and Authentication Using Signal Properties. In Systems, Man and Cybernetics (SMC) Information Assurance Workshop, pages 432–433, 2005.

[9] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and Localization of Sybil Nodes in VANETs. In ACM/SIGMOBILE Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, pages 1–8, 2006.
networks.

[10]In Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009, Las Vegas, January 2009. 96. Jerbi, M., Senouci, S.-M., Meraihi, R., & Ghamri-Doudane, Y. (2007). An improved vehicular ad hoc routing protocol for city environments. In Proceedings of IEEE international conference on communication (ICC 2007) (pp. 3972–3979), Glasgow, Scotland.

[11]. Verma, M., & Dijiang, H. (2009). SeGCom: secure group communication in VANETs. In Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009, Las Vegas, January 2009.

[12]. Choi, J., & Jung, S. (2009). A security framework with strong non-repudiation and privacy in VANETs. In Proceedings of 6th IEEE consumer communications and networking conference
2009, CCNC 2009, Las Vegas, January 2009.

[13]AIMSUN User Manual, Version 4.1, TSS-Transportation Simulation System, Barcelona, Spain, 2002. 78. VISSIM 3.5 User Manual, PTV Planung Transport Verkehr AG, Germany, 2000.

[14]. Boxill, S., & Yu, L. (2000). An evaluation of traffic simulation models for supporting ITS development (Technical Report 167602-1). Texas Southern University, October 2000.

[15]. Krauss, S.,Wagner, P.,& Gawron, C. (1997).Metastable states in a microscopic model of traffic flow. Physical Review E, 55(304), 55–97.