Sybil Attack Encounter Mechanism for Privacy Sensible VANETS

Kalapala Ruth mary Poornima #1, Chinta Naga Manisha#2,

#1, Student, Nimra Institute of Science and Technology, Ibrahimpatnam, Krishna, AP, India

#2, Assistant professor, Nimra Institute of Science and Technology, Ibrahimpatnam, Krishna, AP, India

Abstract: Since few years, Vehicular Ad hoc Networks deserve much attention mainly security and privacy have the most important concerns. In VANET, many attacks rely on having the attacker generate multiple identities to simulate multiple nodes: this is called the Sybil attack. In this paper, we propose a new mechanism to detect Sybil attacks. In proposed system, one mobile node is treated as base station and remaining nodes send their ID and power value to base station. Base station detect the Sybil nodes based on its power value i.e., if power value is less than minimum value. In proposed system, the nodes which are closer to Sybil nodes are selected as senders and Sybil nodes are selected as receivers. If sender sends packets to receivers then there is collision of packets leading to packet drops because identities are present at the same node. If the nodes are very close, then the nodes will be detected as Sybil nodes even if they are not. After detecting and analyzing the attack, throughput and packet delivery ratio was improved.

Keywords: ***Sybil nodes, Sybil attack, VANET.***

I INTRODUCTION

VANET is the most known and near to be realized Ad-hoc networks comprising of vehicles as mobile nodes [1][2]. The VANET makes it possible that vehicles sense their local traffic situation and then share the traffic information quickly with each other. This means vehicles can obtain certain traffic information occurred on their driving route earlier to react against accidental events in advance. For example, traffic congestion can be collectively sensed by vehicles, and cooperatively relayed to other vehicles, toll stations, or the Department of Motor Vehicle (DMV), to facilitate traffic re-routing.

Due to the safety requirements of VANET related applications; we have to deal with the security issues. For example, a malicious vehicle may have vested interests in disseminating false traffic information, forcing other vehicles and vehicular agencies to make incorrect decisions. The cascading impacts of such an attack can be serious. Among various security issues, in this paper, we focus on Sybil attack because it is the root cause of many security problems.

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, they will believe the false information, and base their decisions on it. Hence, addressing this problem is crucial to practical vehicular network systems.

Observe that a Sybil attack may be prevented by requiring vehicles to include a unique identity in transmitted packets. . In this paper, we propose a new mechanism to detect Sybil attacks. In proposed system, one mobile node is treated as base station and remaining nodes send their ID and power value to base station. Base station detect the Sybil nodes based on its power value i.e., if power value is less than minimum value. In proposed system, the nodes which are closer to Sybil nodes are selected as senders and Sybil nodes are selected as receivers. If sender sends packets to receivers then there is collision of packets leading to packet drops because identities are present at the same node. If the nodes are very close, then the nodes will be detected as Sybil nodes even if they are not. After detecting and analyzing the attack, throughput and packet delivery ratio was improved.

II RELATED WORK

Douceur [3] has proven that trusted certification is the only approach that can fully eliminate the Sybil attacks. As the most common solution for defending the Sybil attack, numerous techniques based on public key infrastructure (PKI) have been proposed. As the vehicle can be authenticated with its unique public key and certificate managed by the CA, the Sybil attack can be detected at all times.

SybilGuard [4] 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.

Guette and Bryce [5] suggested a secure hardware based method built on the trusted platform module (TPM). Secure information and related protocols are stored in shielded locations of the module where any forging or manufacturing of data is impossible, and the platform credentials are trusted by car manufacturers; therefore, the communications between TPMs of the vehicles are protected from the Sybil attack. However, as the TPM is an improved variation of a certificate, it still needs trusted authorities that can take the responsibility of managing individual vehicles.

To exploit the fact that one single vehicle cannot present at multiple locations at the same time, Bouassida et al. [6] have proposed a detection mechanism utilizing localization technique based on 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.

Xiao et al. [7] 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 center. 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.

III SYBIL ATTACK

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally. External attacks can be prevented by authentication but not the internal attacks. There should be one to one mapping between identity and entity in WSN. But this attack violates this one-to-one mapping by creating multiple identities. When these nodes want to communicate to their neighboring nodes they use any one of the identities. This confuses and collapses the network.

Each of the defences against the Sybil attack that we have examined has different tradeoffs. Most defences are not capable of defending against every type of Sybil attack. Additionally, each defense has different costs and relies on different assumptions.

IV PROPOSED SYSTEM

Proposed system composed of two main steps – (1) *system initialization*, and (2) *attack detection*. The *attack detection* step is further divided into two stages, namely, detection at node level and detection in cluster routes.

(i) System initialization:

In initialization stage, create a group of mobile nodes. Among the group, one of the nodes is taken as base station. Initially, the base station sends HELLO packets to all the other nodes for topology verification. Here, the nodes with minimum packet drop are chosen as the trust nodes.

The trusted nodes now become the head nodes with a group of its own member nodes. The member nodes send their ID and power value to the head nodes. The head node checks for nodes with power value below the threshold value. If the power value is lesser than the threshold value, those nodes are detected as Sybil nodes. These abnormal nodes are selected as receivers for next detection phase

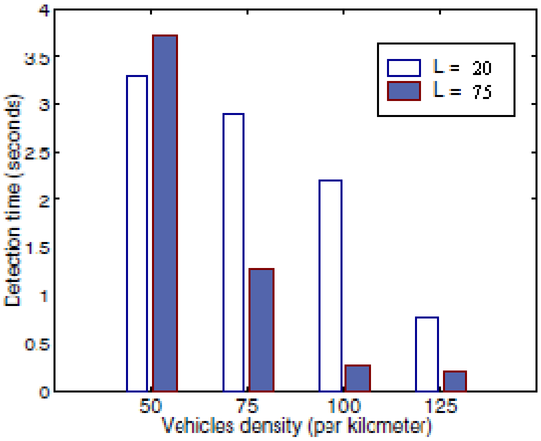
(ii) Sybil Attack Detection:

In this stage initially, we select two nodes closer to Sybil nodes as senders s1, s2. Later, another two Sybil nodes are selected as receivers r1, r2. Now, Packets are sent to s1 and s2 to both receivers. Since both identities are present at the same node, there is collision of packets leading to packet drops. The distance between the receivers is found. If the distance is zero, the node suffers from Sybil attack. If the nodes are very close, then the nodes will be detected as Sybil nodes even if they are not.

The routing procedure in the cluster is checked to verify if there was a hop between the Sybil identities. If there exists a hop between the Sybil identities, then the nodes are not Sybil nodes. If no hops, then the nodes are confirmed to be under attack and they will be removed from the network.

V PERFORMANCE

Let consider Vehicles are placed randomly on the road with the minimum inter vehicle space. Now, we examine the *detection time* which is defined as the time interval from when the malicious vehicle starts the attack to when it is identified by other vehicles. The detection time has a trend to decrease when the offset distance increases because the vacuum space is larger.



So, more vehicles can be employed to identify the attack. An interesting observation is that when vehicles' density is low, the detection time of larger offset distance is longer than that of shorter offset distance. The reason also lies in the longer vacuum space. In the low density scenario, it is hard to identify the attack by only employing S-vehicles. When O-vehicles are used in the confirmation procedure, it takes longer time for them to hear the first message from the malicious vehicle. However, when the density increases, the probability of identifying an attack by only utilizing S-vehicles will be augmented. So, the detection time decreases sharply.

VI CONCLUSION

VANET is the most known and near to be realized Ad-hoc networks comprising of vehicles as mobile nodes. In this paper, we propose a new mechanism to detect Sybil attacks. In proposed system, one mobile node is treated as base station and remaining nodes send their ID and power value to base station. Base station detect the Sybil nodes based on its power value i.e., if power value is less than minimum value. In proposed system, the nodes which are closer to Sybil nodes are selected as senders and Sybil nodes are selected as receivers. If sender sends packets to receivers then there is collision of packets leading to packet drops because identities are present at the same node. If the nodes are very close, then the nodes will be detected as Sybil nodes even if they are not. After detecting and analyzing the attack, throughput and packet delivery ratio was improved.

VII REFERENCES

[1] F. A. I. W. on Vehicular Ad Hoc Networks (VANET), "Fleetnet: Communication platform for vehicular ad hoc networks," in *Zukunftsforum Mobiles Internet 2010*, October 2004.

[2] T. Kosch and M. Strassberger, "The role of new wireless technologies in automotive telematics and active safety," in *8th Symposium Mobile Communications in Transportation*, 2004.

[3] J. Douceur, "The Sybil Attack," Proc. of International Workshop on Peer-to-Peer Systems, pp. 251–260, 2002.

[4] H. Yu, M. Kaminsky, P.B. Gibbons, and A.Flaxman, "Sybilguard: Defending against Sybil Attacks via Social Networks*," Proc.* SIGCOMM, pp. 267-278, Sept. 2006.

[5] G. Guette and C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)," Proc. of WISTP 08, LNCS 5019, pp. 106-116, 2008.

[6] M.S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within Vanet," *Int'l J. Network Security,* vol. 9, no. 1, pp. 22-32, 2009.

[7] B. Xiao, B. Yu, and C. GAO, "Detection and Localization of Sybil Nodes in Vanets*," Proc. Workshop Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks* (DIWANS '06), pp. 1-8, Sept. 2006.

[8] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *Euro Wireless*, 2002.

[9] W. Piers, T. de Paula Figueiredo, HC. Wong and A. Loureiro. Malicious Node Detection in Wireless Sensor Networks. In *IEEE International Parallel & Distributed Processing Symposium*, 2004.