IJRRECS/August 2014/Volume-2/Issue-8/2866-2872 **ISSN 2321-5461**

**INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE**

# AN EXPOSURE TOWARDS DEFENDING AGAINST ATTACKS IN VEHICULAR SYSTEMS

**G.Tejaswini[1], V.Ramakrishna[2]**

[1]M.Tech Student, Dept of CSE, Anurag Group of Institutions (formely CVSR College of Engineering), Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Anurag Group of Institutions (formely CVSR College of Engineering), Hyderabad, T.S, India

**ABSTRACT:**

To detect or mitigate the attack many different approaches have been introduced in the literature. To react against the accidental events in advance the vehicles can obtain certain traffic information by their driving route. The recent gain in the interest of wireless communication in Vehicular Ad hoc Network is always increasing the number of potential applications in the network. Different types of attacks can be launched with Sybil nodes in sensor networks. Sybil attacks are always possible except under extreme and unrealistic assumption of resource parity and coordination among entities. Among various security issues, we mainly focus on Sybil attack because it is the root cause of many security problems. By forging multiple identifies, and by gaining a disproportionately large influence an attacker can launch a Sybil attack. Deploying trusted certificates is the only approach which has the potential to eliminate Sybil attacks completely. By means of the trajectories of vehicles in support of recognition while still protecting the anonymity as well as location privacy of vehicles, we put forward a new Sybil attack detection method Footprint. Footprint can mainly confine Sybil attacks and can extremely decrease effect of Sybil attacks in urban situation.

***Keywords: Sybil attacks, Wireless communication, Vehicular Ad hoc Network, Trusted certificates.***

## 1. INTRODUCTION:

The multiplication of false nodes in a wireless network in order to launch various kinds of attack is known as the Sybil attack. While the Sybil attack was the first described and formalized and it has been a severe and a persistent problem in many forms. The Sybil attack consists in sending multiple messages from one node with multiple identities [4]. Hence, several nodes in the network are simulated by the attackers. Due to the critical goal of safety related functions the communication security problem must be taken into account. The widely accepted privacy preserving communication scheme in vehicular network is by using pseudonyms which has left the doors open for security problems such as Sybil attack [8]. A privacy-preserving Sybil attack is introduced for the detection scheme using pseudonyms and a number of pseudonyms for each vehicle are distributed by the trust authority. A message sent from a neighboring vehicle is said to be trustworthy if the content of the message is identical with at least a certain number of messages sent from other neighboring vehicles. A particular group signature schemes are adopted for vehicles to sign on messages so that the anonymity of each vehicle can be achieved by suppressing duplicate messages from the same vehicle [1]. However, if a vehicle generates two signatures on the same message, these two signatures can be acknowledged by the verifier vehicle. The same driving environment is observed by the multiple vehicles will generate different messages with very similar semantics. In this case, the resolved trustworthy messages might be a minority of all observations which results in a biased or no final decision [11]. Sybil attack is one of the most serious attacks to vehicular networks and detects the attack by using footprint scheme in which the route of vehicle is produced and vehicle's place is found from successive messages send by vehicle toward road side unit. Among various security issues, we mainly focus on Sybil attack because it is the root cause of many security problems [3]. We put forward a detection system in support of Sybil attack which is based on public key cryptography and it aims to ensure privacy preservation and confidentiality.

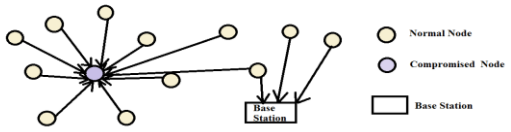


Fig1: Sybil Attacks Diagram

## 2. METHODOLOGY:

The vehicular network has been in use as a promising technology in a ubiquitous environment with the significant development of network technologies and facilities. The recent gain in the interest of wireless communication in Vehicular Ad hoc Network is always increasing the number of potential applications in the network. The vehicles sense their local traffic situation and share the traffic information quickly with each other is possible by the VANET [14]. To react against the accidental events in advance the vehicles can obtain certain traffic information by their driving route. It is simple for a malicious vehicle to intercept, modify or inject data in VANET As data is broadcasted over a shared communication media. Moreover, the cooperation between nodes is essential due to the limited communication range of a vehicle. Other nodes are allowed to discover its neighborhood and to share information by exchanging the data. This shows the vulnerability of networks if no security mechanism is available. Intention of Sybil attacks as shown in fig1 is simply to give an illusion of a traffic jam so that it forces other vehicles to leave the road to gain of the attacker [9]. Sybil attacks are always possible except under extreme and unrealistic assumption of resource parity and coordination among entities. By means of the trajectories of vehicles in support of recognition while still protecting the anonymity as well as location privacy of vehicles, we put forward a new Sybil attack detection method Footprint. The road side unit issues an allowed message for vehicle as proof of its presence and time in footprint when a vehicle encounters a road side unit [7]. The approved messages are utilized to make out vehicles which are positioned at different areas can get dissimilar authorized messages. There is an escape of location privacy of vehicles by unswervingly employing authorized messages since knowing an approved message of a vehicle signed by a meticulous road side unit is corresponding to knowing the information that vehicle has explained up near that road side unit at that time [2]. We intend a location-hidden authorized message generation system for two reasons in footprint. Initially, the signatures on messages are signer-ambiguous which signifies a road side unit is anonymous when signing a message. The road side unit location information is covered in this

method from concluding authorized message. Secondly, two authorized messages concerned from similar road side unit are identifiable if and only if they are concerned within similar period of time [16]. We assume that all road side units are trustworthy in footprint. However, it can help a malicious vehicle to generate fake legal trajectories if a road side unit is compromised. The footprint cannot detect such trajectories in such cases. To quick notice the fraud of road side unit we will develop cost-efficient techniques. We have validated our design and studied its performance in actual complex atmosphere based on continuing practical model. A scalable security and privacy solution was suggested and authenticated certificates which have to be concerned from national certification authority [12]. By analysis and extensive trace driven simulations that Footprint can mainly confine Sybil attacks and can extremely decrease effect of Sybil attacks in urban situation is demonstrated by footprint design which can be incrementally implemented in large city.

## 3. PREVIOUS EFFORTS ON DETECTION OF SYBIL ATTACK:

Since malicious vehicles can easily have more powerful resources than the normal vehicles in vehicular networks. The social network among entities is an interesting scheme studying in Sybil Guard [5]. In this scheme, for detecting Sybil attacks human established real-world trust relationship among users is used. By building the relationship between honest users and Sybil identities is much harder as the attacker can generate as many as Sybil identities. A trusted relationship between the forged identities and the real ones are identified by a small “cut” on the graph [15]. However, it is very challenging to establish such trust relationship among vehicles, so this scheme cannot be used in vehicular networks. This is because vehicles are highly mobile. Communications often happen among temporarily met and unfamiliar vehicles. Here, we propose a detection mechanism utilizing localization technique based on Received Signal Strength Indication (RSSI) as the scheme cannot be used in vehicular networks [10]. The same estimated locations are considered as Sybil vehicles with the identities. The RSSI measurements are highly time variant even measured at the same locations which are complicated as the outdoor environments can dramatically

affect the wireless signal propagation. Here, we have introduced a Sybil attack detection scheme where the location of a particular vehicle can be determined by the RSSI measurements. Since RSUs use long-term identities to generate signatures, these schemes did not take location privacy into consideration [6]. 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. Therefore, the privacy of location information and identity of vehicles are preserved in Footprint. By forging multiple identifies, and by gaining a disproportionately large influence an attacker can launch a Sybil attack [13]. To detect or mitigate the attack many different approaches have been introduced in the literature. Deploying trusted certificates is the only approach which has the potential to eliminate Sybil attacks completely. Moreover, for an attacker it is possible to violate the assumption, and gets more than one identities. This method has the problem of key revocation which is difficult in wireless mobile networks. Resource testing is another category of Sybil attack detection schemes. If a number of identities possess fewer resources than would be expected if they were independent is determined by the resource testing.

## 4. CONCLUSION:

The multiplication of false nodes in a wireless network in order to launch various kinds of attack is known as the Sybil attack. The vehicular network has been in use as a promising technology in a ubiquitous environment with the significant development of network technologies and facilities. Sybil attack is one of the most serious attacks to vehicular networks and detects the attack by using footprint scheme in which the route of vehicle is produced and vehicle's place is found from successive messages send by vehicle toward road side unit. The widely accepted privacy preserving communication scheme in vehicular network is by using pseudonyms which has left the doors open for security problems such as Sybil attack. A message sent from a neighboring vehicle is said to be trustworthy if the content of the message is identical with at least a certain number of messages sent from other neighboring vehicles. By means of the trajectories of

vehicles in support of recognition while still protecting the anonymity as well as location privacy of vehicles, we put forward a new Sybil attack detection method Footprint. The approved messages are utilized to make out vehicles which are positioned at different areas can get dissimilar authorized messages. By analysis and extensive trace driven simulations that Footprint can mainly confine Sybil attacks and can extremely decrease effect of Sybil attacks in urban situation is demonstrated by footprint design which can be incrementally implemented in large city.

## REFERENCES:

[1] T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy- Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," Proc. Fourth Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '07), pp. 1-8, Aug. 2007.

[2] J.K. Liu, V.K. Wei, and D.S. Wong, "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract)," Proc. Ninth Australasian Conf. Information Security and Privacy (ACISP '04), pp. 325-335, 2004.

[3] Footprint: Detecting Sybil Attacksin Urban Vehicular Networks,2012

[4] 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.

[5] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous Identification in Ad Hoc Groups," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '04), pp. 609-626, 2004.

[6] P. Maniatis, D.S.H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi, "Preserving Peer Replicas by Rate-Limited Sampled Voting," Proc. 19th ACM Symp. Operating Systems Principles (SOSP '03), pp . 44-59, Oct. 2003.

[7] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010

[8] Q. Wu, J. Domingo-Ferrer, and U. Gon_zalez-Nicola´ s, "Balanced Trustworthiness, Safety and Privacy in Vehicle-to-vehicle Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 2, pp. 559-573, Feb. 2010.

[9] S. Park, B. Aslam, D. Turgut, and C.C. Zou, "Defense against Sybil Attack in Vehicular Ad Hoc Network Based on Roadside Unit Support," Proc. 28th IEEE Conf. Military Comm. (MILCOM '09), pp. 1-7, Oct. 2009.

[10] 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.

[11] 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.

[12] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[13] C. Chen, X. Wang, W. Han, and B. Zang, "A Robust Detection of the Sybil Attack in Urban Vanets," Proc. IEEE Int'l Conf. Distributed Computing Systems Workshops (ICDCSW '09), pp. 270-276, June 2009.

[14] P.P. Tsang, V.K. Wei, T.K. Chan, M.H. Au, J.K. Liu, and D.S. Wong, "Separable Linkable Threshold Ring Signatures,"

Proc. Int'l Conf. Cryptology in India (INDOCRYPT '04), pp. 384-398, 2004

[15] 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.

[16] B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust," Technical Report SRI-SDL-04-02, SRI Int'l, Apr. 2002.