Detection Of Sybil Attack For Urban Vehicle Networks With Topological Schemes

MS. Fathima Syed M.Tech.,
Computer Science & Engineering Department
DR.K.V.Subbareddy College Of Engineering
For Women, DUPADU, Kurnool-518218
Affiliated to J.N.T.University, Anantapur
Andhra Pradesh, India,

R.Samaiah M.Tech, MISTE., Asst Professor
Computer Science & Engineering Department
DR.K.V.Subbareddy College Of Engineering
For Women, DUPADU, Kurnool-518218
Affiliated to J.N.T.University, Anantapur
Andhra Pradesh, India,

Abstract

A novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the appearance time at this RSU. We design a location-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification. With the temporal limitation on the likability of two authorized messages, authorized messages used for long-term identification are prohibited. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages. Utilizing social relationship among trajectories according to the similarity definition of two trajectories, Footprint can recognize and therefore dismiss “communities” of Sybil trajectories. Rigorous security analysis and extensive trace-driven simulations demonstrate the efficacy of Footprint.

Index Terms: Sybil Attack, Networks, Location hidden Trajectory

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 a malicious vehicle masquerades as multiple identities The consequence of Sybil attack happening in vehicular networks can be vital.

II. IMPLEMENTATION

Hackers easily can act as source node and sends message to destination. Destination receives wrong message from hackers. Destination believes that its correct message from source. Destination receives the wrong information from hackers. Messages are passed from sender to destination (receiver) without any security. Message header holds source node information which sends the message to receiver. Hackers can easily change that header information and sends to destination. Destination gets the wrong information from hackers or malicious user. There is no any server to detect hackers. Header information may be hiding by malicious user. Source node does not get any response from destination while hackers get that source information hackers cannot act as source, because one centralized server is maintaining to check authentication of source. This centralized server is Sybil guard. It blacks unauthorized users or hackers. Sybil guard is maintaining source node information and header information of message. It checks the users using that details whether they are attackers or normal user. Hacker's information has not been transferred to destination. Destination has not been receiving any attacker information. Sybil guard is maintained to detect the attackers who are all act as source node. It deletes that wrong information from hackers and indicates that they are attackers. Hackers' information has not transferred to receiver. Sybil guard act as the centralized server to all users. It handles the message transmission between those users. Each user has to register individually. Those user information are stored in centralized server and find the attackers using that information.

III Design Goals

TOPOLOGY CONSTRUCTION:

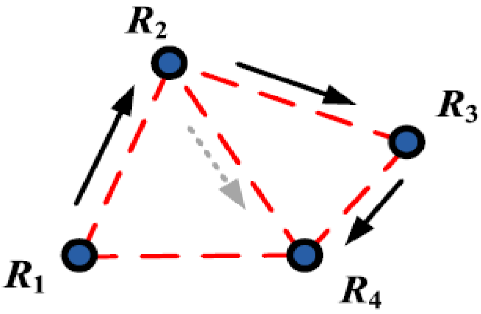
Topology construction is designed to construct one topology with available nodes. Register all nodes which are involved to transfer the data to some other nodes. Depends upon total nodes, topology will be constructed. Topology construction module allows you to construct node path. If already exits, it will not allow to construct that same path. All nodes are mentioned in topology construction. User can't modify node information after construction.

NODE ENTRY

Node entry module describes node authentication. To activate node who are all involved in topology, node should be login into that topology. It does not allow unauthorized node entry. Many nodes can enter into that mentioned topology. Each node can send the messages to their destination after login.

MESSAGE TRANSMISSION

Each node (source node) can send the data to some other node(destination) which one connected with that source node. While sending message, the source node should mention the header information. Source node can send the data to destination. Destination will receive that message.



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.

SYBLGUARD

Sybil guard is maintained in this project to detect the attacker. Sybil guard is called as centralized server. Sybil guard does not allow hackers to send the wrong data. It compares node information and header information. If matches, normal user sending the message to destination. Otherwise sybilguard will not allow the hackers to send message. It blocks that data and it provides the attacker information to attacker. Sybil guard gets node information from its registration. While data transmission, Sybil guard will get their header information. This centralized server maintains to find out the attacker details.

IV CONCLUSIONS AND FUTIRE WORK

We have developed a Sybil attack detection scheme Footprint for urban vehicular networks. 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. It is also demonstrated by both analysis and extensive trace driven simulations that Footprint can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings (above 98 percent detection rate).With the proposed detection mechanism having much space to extend, we will continue to work on several directions. First, in Footprint, we assume that all RSUs are trustworthy. However, if an RSU is compromised, it can help a malicious vehicle generate fake legal trajectories (e.g. by inserting link tags of other RSUs into a forged trajectory).In that case, Footprint cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by itself nor forge link tags generated by other RSUs, which can be utilized to detect a compromised RSU in the system. In future work, we will consider the scenario where a small fraction of RSUs are compromised. We will develop cost-efficient techniques to fast detect the corruption of an RSU. Second, we will delve into designing better linkable signer-ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced.

REFERENCES

[1] 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.

[2] 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.

[3] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), pp. 251-260, Mar. 2002.CHANG ET AL.: FOOTPRINT: DETECTING SYBIL ATTACKS IN URBAN VEHICULAR NETWORKS 1113

[4] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: Vehicular Content Delivery Using WiFi," Proc. MOBICOM '08, pp. 199-210,Sept. 2008.

[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] 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.

[7] 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.

[8] S. Capkun, L. Buttya_n, and J. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

About the Authors

Ms.Fathima Syed, recieved her B.tech degree from Jawaharlal Nehru Technological University, India in the year 2011. She is currently pursuing M.Tech in Computer Science and Engineering from Dr. K.V.S.R.C.E.W, Kurnool, India.

Mr.R.Samaiah(MTECH,MISTE) received his B.Tech degree in Computer Science and Engineering from Sri Venkateswara University, Tirupati, India in the year 2005 and M.Tech in Computer Science from Vishwaswaraiah Technological University, India, in the year 2008. He is currently working as a Assistant Professor at Dr.K.V.S.R.C.E.W, Kurnool, India. His research interests includes Computer Networks .