ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Footprint: Detecting Sybil Attacks in Urban Vehicular Networks

Shaik Imran
Assistant Professor
Princeton College of Engineering and Technology,
Hyderabad.

Abstract:

In urban vehicular networks, where privacy, especially the location privacy of anonymous vehicles is highly concerned, anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining a disproportionately large influence. In this paper, we propose 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 likable) 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.

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 intervehicle 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 [1], [2], 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 [3], overwhelmingly influencing the result. The consequence of Sybil attack happening in vehicular networks 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. 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. For example, it can be inferred that the driver of a vehicle may be sick from knowing the vehicle is parking at a hospital. It is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

inhibitive to enforce a one-to-one correspondence between claimed identities to real vehicles by verifying the physical presence of a vehicle at a particular place and time. Third, conversations between vehicles are very short. Due to high mobility of vehicles, a moving vehicle can have only several seconds [4] 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.To eliminate the threat of Sybil attacks, it is straightforward to explicitly bind a distinct authorized identity (e.g., PKI-based signatures) [5], [6], [8] to each vehicle so that each participating vehicle can represent itself only once during all communications. Using explicit identities of vehicles has the potential to completely avoid Sybil attacks but violates the anonymity concern in urban vehicular networks. As an alternative scheme, resource testing [9],[10], [11] can be conducted to differentiate between malicious and normal vehicles, where the judgment is made whether a number of identities possess fewer resources (e.g., computational and storage ability) than would be expected if they were distinct. This scheme fails in heterogeneous environments where malicious vehicles can easily have more resources than normal ones. Considering the fact that a vehicle can present itself at only one location at a time, localization techniques or other schemes like the Global Positioning System (GPS) aiming to provide location information of vehicles can be exploited to detect hostile identities. However, these schemes often fail in complicated urban settings (e.g., bad GPS signals due to urban canyons, inaccurate localizations due to highly dynamic wireless signal quality). Recently, two group-signature-based schemes [16], [17] have been proposed, where a message received from multiple distinct vehicles is considered to be trustworthy. Using group signatures can provide anonymity of vehicles and suppress Sybil attacks by restraining duplicated signatures signed by the same vehicles. One practical issue of these schemes is that different messages with similar semantics may be ignored from making the decision, which leads to a biased or no final decision. As a result, there is no existing successful solution, to the best of our knowledge, to tackling the online Sybil attack detection problem in urban vehicular networks. In this paper, we propose a novel Sybil attack detection scheme Footprint, using the trajectories of vehicles for identification while still preserving the anonymity and location privacy of vehicles. Specifically, in Footprint, when a vehicle encounters an RSU, upon request, the RSU issues an authorized message for this vehicle as the proof of its presence at this RSU and time. Intuitively, authorized messages can be utilized to identify vehicles since vehicles located at different areas can get different authorized messages. However, directly using authorized messages will leak location privacy of vehicles because knowing an authorized message of a vehicle signed by a particular RSU is equivalent to knowing the fact that the vehicle has showed up near that RSU at that time. In Footprint, we design a location-hidden authorized message generation scheme for two purposes. First, RSU signatures on messages are signer-ambiguous which means an RSU is anonymous when signing a message. In this way, the RSU location information is concealed from the final authorized message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same RSU are recognizable if and only if they are issued within the same period of time. Thus, authorized messages can be used for identification of vehicles even without knowing the specific RSUs who signed these messages. With the temporal limitation on the linkability of two authorized messages, authorized messages used for longterm identification are prohibited. Therefore, using authorized messages for identification of vehicles will not harm anonymity of vehicles. To be uniquely identified, a vehicle collects a consecutive series of authorized messages as it keeps traveling. Such a sequence of authorized messages constitutes a trajectory of this vehicle. In Footprint, a vehicle is free to start a new trajectory by using a new temporary public key.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Furthermore, a malicious vehicle can abuse this freedom to elaborately generate multiple trajectories, trying to launch a Sybil attack. Based on the observation that Sybil trajectories generated by a malicious vehicle are very alike, Footprint establishes the relationship between a pair of trajectories according to our definition of similarity. With this relationship, Sybil trajectories generated by the same malicious vehicle form a "community." By finding and eliminating "communities" of Sybil trajectories, Footprint can detect and defend against Sybil attacks. The advantages of Footprint are fourfold. First, Footprint does not need the identities of vehicles, which ensures the anonymity of vehicles. Second, no geographical information is leaked in Footprint, which guarantees the location privacy of vehicles. Third, Footprint only needs each vehicle to be equipped with a cheap commercial GPS receiver and DSRC wireless communication module. Last, Sybil attack detection can be online independently conducted by a conversation holder (e.g., an individual vehicle or an RSU) which initializes a conversation among vehicles. Besides the advantages, the main limitation of Footprint is that Footprint requires an infrastructure of RSUs and a trust authority (TA) existing in the system in order to generate trajectories and establish trust among entities, respectively. We verify that Footprint can achieve all design objectives through security, privacy, and performance analysis and extensive trace-driven simulations which involve 2,100 taxies in Shanghai city. Footprint can largely restrict Sybil attacks and enormously reduces the impact of Sybil attacks in urban settings (above 98 percent detection rate).

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

Existing system

- In existing system, 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.

Disadvantages

- 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.

PROPOSED SYSTEM

In this proposed system, hackers can not act as source, because one centralized server is maintaining to check authentication of source. This centralized server is sybilguard. It blacks unauthorized users or hackers. Sybilguard 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

destination. Destination has not been receiving any attacker information.

ADVANTAGES

- Sybilguard 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.
- Sybilguard act as the centralized server to all users. It handles the message transmission between those users. Each user has to register individually. Those user informations are stored in centralized server and find the attackers using that information.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2.Select methods for presenting information.
3.Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

MODULES

1. Topology Construction
2. Node entry
3. Message transmission
4. Sybilguard

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

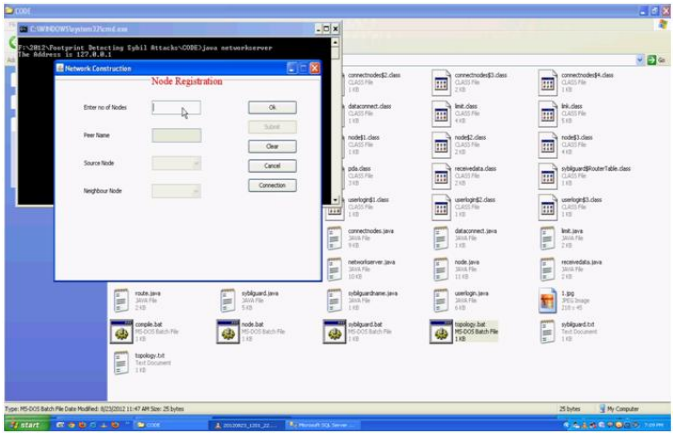
Each node (source node) can send the data to some other node(destination) which one connected with that source node. While sending message, the source node should mention the header information. Source node can send the data to destination. Destination will receive that message.

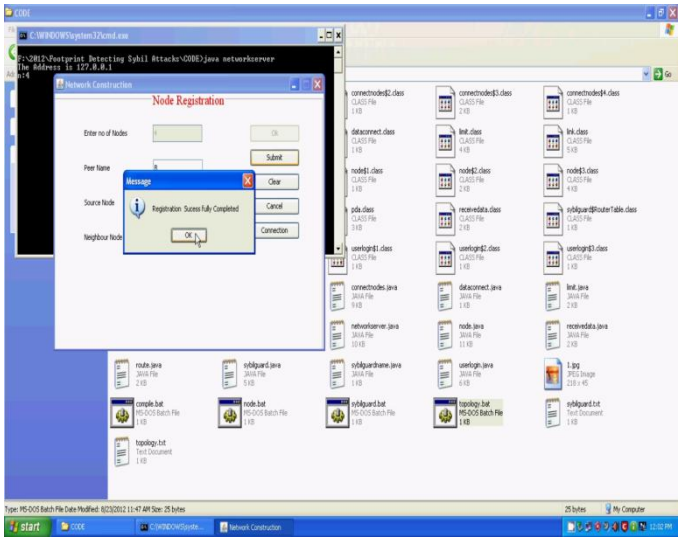
SYBLGUARD

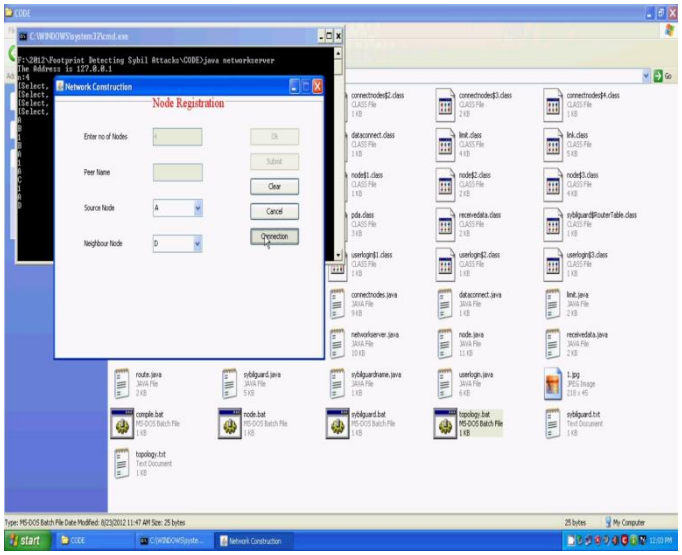
Sybilguard is maintained in this project to detect the attacker. Sybilguard is called as centralized server. Sybilguard does not allow hackers to send the wrong data. It compares node information and header information. If matches, normal user sending the message to destination. Otherwise sybilguard will not allow the hackers to send message. It blocks that data and it provides the attacker information to attacker.

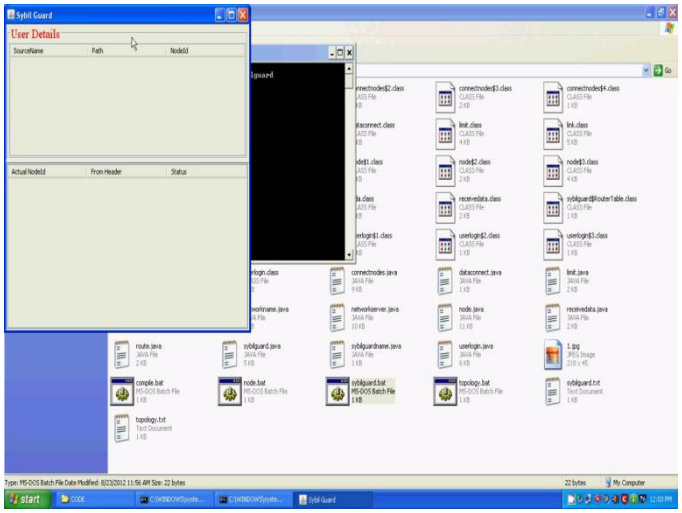
Sybilguard gets node information from its registration. While data transmission, sybilguard will get their header information. This centralized server maintains to find out the attacker details.

Screen Shots

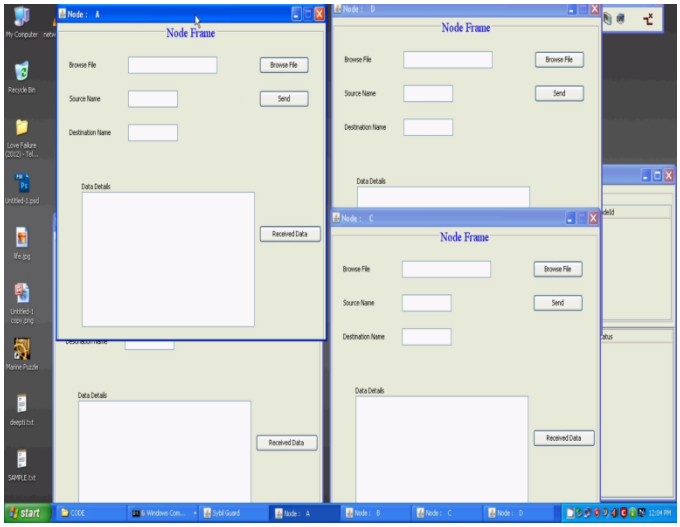


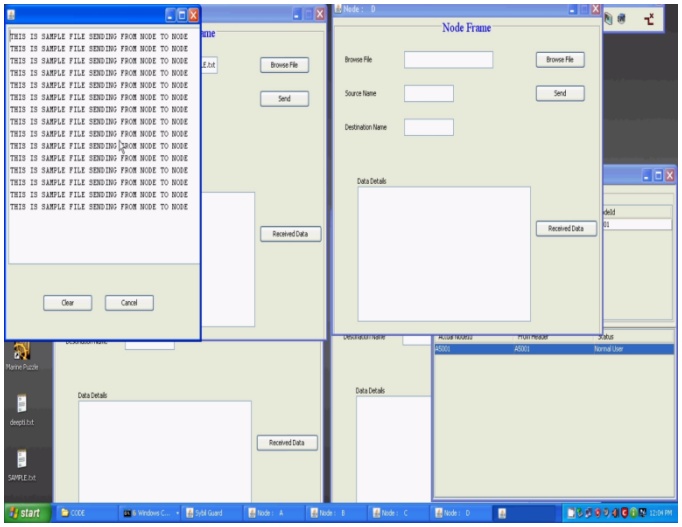


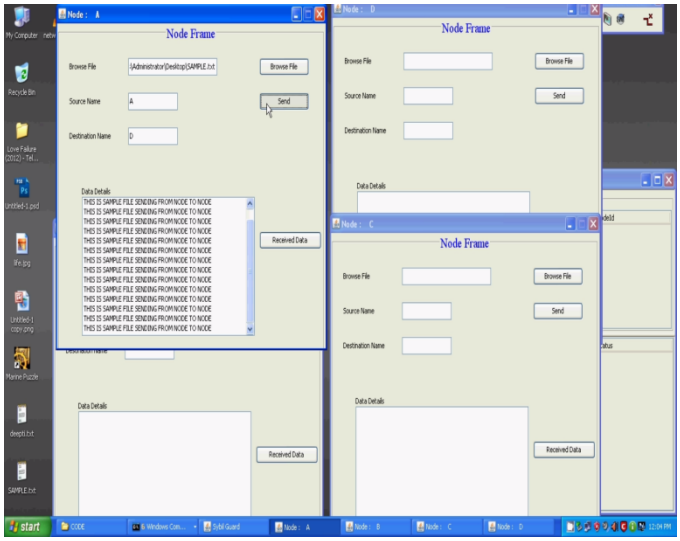


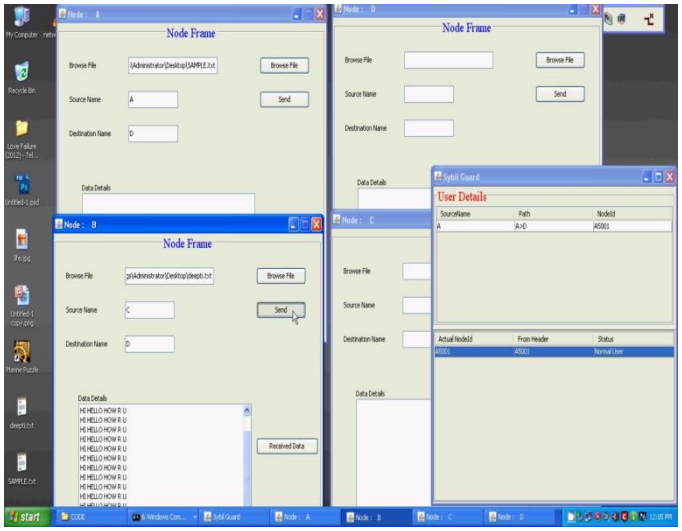


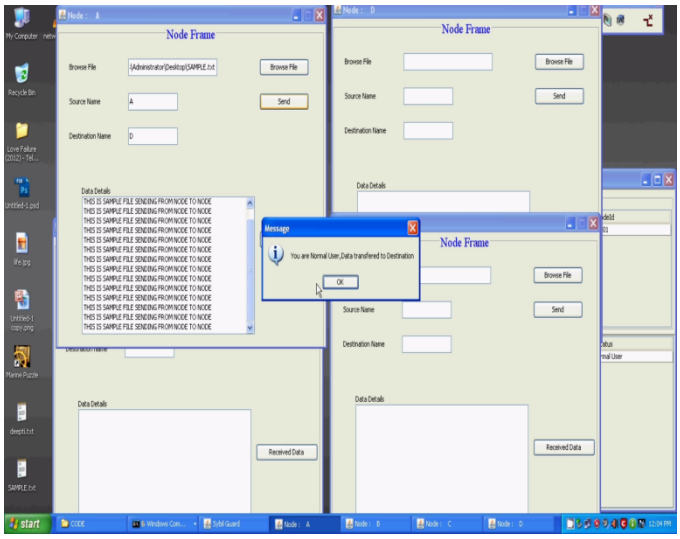
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

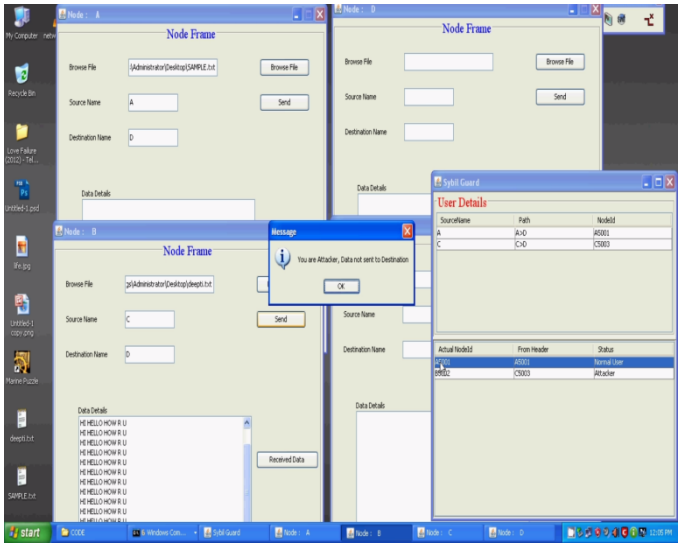












ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSIONS AND FUTIRE WORK

In this paper, 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 tracedriven 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. Last, we will validate our design and study its performance under real complex environments based on our ongoing realistic prototype testbed built at Xi'an Jiao Tong University.

Improvements will be made based on the realistic studies before it comes to be deployed in large-scale systems.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[9] C. Piro, C. Shields, and B.N. Levine, "Detecting the Sybil Attack in Mobile Ad Hoc Networks," Proc. Securecomm and Workshop, pp. 1-11, Aug. 2006.

[10] N. Borisov, "Computational Puzzles as Sybil Defenses," Proc. Sixth IEEE Int'l Conf. Peer-to-Peer Computing (P2P '06), pp. 171-176, Oct.2006.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] L. Chen, S.-L. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs," IEEE J. Selected Areas in Comm., vol. 29, no. 3, pp. 1-11, Mar. 2011.

[18] 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.

[19] 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.

[20] IEEE Vehicular Technology Soc.: 5.9 GHz Dedicated Short Range Comm. (DSRC) - Overview. http://grouper.ieee.org.groups/scc32/dsrc/, 2011.