PRIVACY FRIENDLY DETECTION TECHNIQUE OF SYBIL ATTACK IN VEHICULAR AD HOC NETWORK (VANET)

SEYED MOHAMMAD CHERAGHI

A project report submitted in partial fulfillment of the
Requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System (FSKSM)
Universiti Teknologi Malaysia

JANUARY 2013

Dedicated to my beloved father, mother and brothers

ACKNOWLEDGEMENT

I wish to express my deepest appreciation to all those who helped me, in one way or another, to complete this project. First and foremost I thank God almighty who provided me with strength, direction and purpose throughout the project. Special thanks to my project supervisor Associate Professor Dr. Mohammad Abdur Razzaque for all her patience, guidance and support during the execution of this project. Through her expert guidance, I was able to overcome all the obstacles that I encountered in these enduring ten months of my project. In fact, she always gave me immense hope every time I consulted with her over problems relating to my project.

ABSTRACT

Vehicular communications play a substantial role in providing safety in transportation by means of safety message exchange. Researchers have proposed several solutions for securing safety messages. Protocols based on a fixed key infrastructure are more efficient in implementation and maintain stronger security in comparison with dynamic structures. Security is an important concern in VANETs because a malicious user may deliberately mislead other vehicles and vehicular agencies. Sybil attacks have been regarded as a serious security threat to ad hoc networks and sensor networks. They may also impair the potential applications of VANETs (Vehicular Ad hoc Networks) by creating an illusion of traffic congestion. Sybil attack is a malicious vehicle pretends to be multiple vehicles. Reported data from a Sybil attacker will appear to arrive from a large number of distinct vehicles, and hence will be credible. Privacy is another issue that must be preserved. In order to maintain security, privacy ca be compromised, hence this research study proposes a privacy friendly framework to detect Sybil attack. Finally, we use MATLAB as a simulator and compare the simulation results with other method.

ABSTRAK

Komunikasi kenderaan memainkan peranan yang besar dalam menyediakan keselamatan dalam pengangkutan melalui pertukaran mesej keselamatan. Penyelidik telah mencadangkan beberapa penyelesaian untuk mendapatkan mesej keselamatan. Protokol berdasarkan infrastruktur utama tetap adalah lebih berkesan dalam pelaksanaan dan mengekalkan keselamatan yang lebih kukuh dalam perbandingan dengan struktur yang dinamik. Keselamatan adalah satu kebimbangan yang penting dalam VANETs kerana pengguna yang berniat jahat boleh sengaja mengelirukan kenderaan dan agensi-agensi lain kenderaan. Sybil serangan telah dianggap sebagai ancaman keselamatan yang serius kepada rangkaian ad hoc dan rangkaian sensor. Mereka juga boleh menjejaskan potensi aplikasi VANETs (kenderaan Ad hoc Networks) dengan mewujudkan ilusi kesesakan lalu lintas. Sybil serangan adalah kenderaan yang berniat jahat berpura-pura untuk menjadi pelbagai kenderaan lain. Melaporkan data dari penyerang Sybil akan muncul tiba dari bilangan besar kenderaan yang berbeza, dan dengan itu akan menjadi kredibel. Privasi adalah satu lagi isu yang mesti dipelihara. Dalam usaha untuk mengekalkan keselamatan, privasi ca boleh dikompromi, maka kajian ini mencadangkan satu rangka kerja privasi mesra untuk mengesan serangan Sybil. Akhirnya, kita menggunakan MATLAB sebagai simulator dan bandingkan keputusan simulasi dengan kaedah lain.

TABLE OF CONTENTS

LIST OF TABALES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Vehicular ad hoc network (VANET) is a form of MANET. It is used for communication between vehicles in order to provide safer environment for them. It is infrastructure-less network that is constructed on self-organizing. Furthermore it is based on short range wireless communication among vehicles. Some challenges in VANET are similar to MANET such as: wireless links communications, limited band-width, multi-hop broadcast and lack of established infrastructure.

However, VANET has some differences as compared to MANET. For example in VANET, vehicles are the components which building the network and the network restricted vehicle movements. Sufficient computational and power resources are the advantages of VANETs over MANETs that eliminate the need for energy-aware algorithms [1].

Vehicles' movements in VANET make it dynamic in time and space; therefore it offers flexibility which is associated to the vulnerability of wireless communications. Hence, it brings new challenges to achieve safe and secure communication. The defenseless of VANET due to its specificities and characteristics make it target to all types of attacks (passive and active) from malicious and malfunctioning nodes.

For example if message integrity is not protected, the messages' contents which are sent by one node can be modified by an attacker in order to change the behavior of other nodes. Hence, an attacker can keep its identity unknown and use this situation in order to obtain many benefits. Consequently, the vehicle that was attacked by the attacker would be made responsible for the damage caused.

Base on the types of communications (Vehicle to vehicle (V2V) and Vehicle to infrastructure (V2I)) and in order to provide security and privacy of the vehicles, following issues need to be provided in VANET:

Authentication: It means that receiver must be able to check the legitimacy of an event or message and its sender; otherwise an attacker can impersonate an emergency vehicle to surpass speed limits without being sanctioned.

Non repudiation: It ensures that the sender and the receiver of one message cannot deny that they have ever sent or received specific messages that exist. If it is not supported, an attacker can report false information in order to misuse a situation. In other word both the transmitter and receiver of any messages should be identifiable at any given time.

In order to provide safety in VANETs applications, we need to deal with the security issues. Although there are various security attacks in VANET, this research study try to concentrate on Sybil attack. It is one of the most important attacks in VANET that may cause negative effects to both VANETs security and driving safety.

Sybil attack was first introduced and formalized by Douceur in peer to peer networks. Based on this attack, a malicious node fabricates fake identities in the form of multiple nodes. These fake nodes (identities) behave like normal nodes in order to deceive other vehicles by distributing false traffic information. On the other hand cooperative driving plays a critical role in VANET because it increases cars' safety. According to the cooperative driving any sensed event should be reported by multiple distinct vehicles. Therefore Sybil attack can target this assumption by creating fake identities and report fake events in order to deceive other vehicles to follow its desire.

For example, in a typical attack, a malicious node creates several fake identities. These identities are considered as vehicles. If each of these fake vehicles declares false information about an accident and cars with genuine identities consider them as an honest report, they may either choose other ways and free the road for the purpose of the attacker or decrease their speed which can cause traffic jam.

Privacy is another critical issue in VANETs which related to protection of drivers sensitive information against unauthorized observers. Location-based services has several privacy problem, For example, a malicious node eavesdrop and collect information sent by vehicles and track their location. It also can guess critical data of users such as their residence and their real identities. Nevertheless, privacy in VANETs refer to sensitive data related to driver such as license plate, current speed, current position, identification number, and the like which must be kept private from other vehicles in the system.

This research study attempts to evaluate the performance of the security mechanisms which are proposed to detect Sybil attack in vehicular networks. It also tries to propose a technique for detecting the Sybil nodes in VANETs.

1.2 Problem Background

The Sybil attack is a well-known harmful attack in networking which forges identities, claims as multiple users and send multiple messages from one vehicle with multiple identities. Several methods are suggested for detecting Sybil attacks but some of them such as radio resource testing [8] are not applicable in VANETs since the attacker can access to further computational resources than an honest node.

Using of public key cryptography [15] is another method which uses a PKI for VANET (VPKI) to solve the security issues that are caused by Sybil attack. This method is not suitable because it is difficult to deploy PKI for VANET and also testing this method in a real world for assessing it, is impossible.

Some researches assume a predefined propagation model in wireless networks in order to deal with detection of Sybil attack [4][5]. They tried to estimate received signal power in order to find some inconsistencies between the signal's power and the claimed position. However, most of these techniques which are based on propagation model suffer from imprecision of devices. It is mainly because an attacker can defeat these models by changing the transmitted power. Almost all the solutions that have been proposed are inefficient for a complete VANET security solution.

1.3 Problem Statement

A malicious vehicle have interested in spreading false traffic messages and compelling other vehicles to make wrong decisions. Incorrect message reported by a malicious node is not sufficient. For accepting it as truth, applications need several vehicles to confirm a particular message. By considering this assumption, if a malicious vehicle tried to pretends to be multiple vehicles (Sybil attack), it could distribute some false messages in order to make other vehicles to follow its desires. If other vehicles cannot recognize the Sybil attack, they accept the information and decide base on it. Therefore, recognizing this problem is critical for vehicular network systems. Previous work are based upon different assumptions, which are often not realistic in a VANET context. It is important to provide a theoretical insight of which assumptions reduce the potential for Sybil attacks.

Privacy of vehicles is another big issue which must be preserved. It is a critical attributes of a VANET which is related to sensitive information of driver, and must be protected from compromising at any time. Simply by overhearing periodic beacon messages sent from vehicles, an adversary can identify locations visited by a certain car and then breach the privacy of the driver. This study will investigate the role of the assumptions on the success rate of Sybil attacks and try to propose a privacy friendly detection technique to detect Sybil attacks in VANETs.

1.4 Objectives

The objectives of the study include

- To study the characteristics of Sybil attack in VANETs perspective.
- To enhance privacy friendly technique to detect Sybil attacks.
- To evaluate the technique and compare with Privacy Preserving Detection of Abuses of Pseudonyms (P2DAP)

1.5 Project Scope

Security and privacy are two important aspects of safety communications in VANET. There are a great number of attacks in VANET. These attackers have been classified according to the layers used by them. The scope of this research is to study all types of attacks in VANET but the main concentration is on Sybil attack. It is mainly because Sybil attack can import false information into the network which can put the drivers and passengers life endanger. It means that it can target the basic principles of VANET which are Road safety and Traffic control. This research study also tries to propose a method to detect Sybil attack in a vehicular ad hoc network (VANET) based on roadside unit (RSU). Matlab will be used to develop and test the proposed framework. Currently, this method cannot detect the colluding vehicles if each malicious vehicle only reports a faked event with one pseudonym. However, such an attack is not a Sybil attack and is beyond the scope of this paper.

1.6 Thesis outline

This thesis is organized as follows.

Chapter 2 reviews all attacks an security requirement in VANET and then gives an insight to the existing Sybil attack detection method which have been developed by various researcher.

Chapter 3 prepares the methodology of the proposed detection, and provides a short explanation for each of the main steps in the developed detection system.

Chapter 4 explains the design of proposed scheme and the design of simulation model of the proposed scheme.

In Chapter 5, the findings of the simulation modeling are assessed.

Finally, the last chapter concludes the dissertation and offers some directions for future works.

REFERENCES

1. Papadimitratos, P., Fortelle, A. L., Evenssen, K., Brignolo, R. and Cosenza, S. 2009. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Communications Magazine, 47(11): 84–95.
2. Kargl, F., Papadimitratos, P., Buttyan, L.,M¨uter, M.,Wiedersheim B., Schoch, E., Thong, T.-V., Calandriello, G., Held, A., Kung, A. and Hubaux, J.-P. 2008. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. IEEE Communcations Magazine, 46(11): 110–118.
3. Ardelean, P. . and Papadimitratos, P. 2008. Secure and Privacy-Enhancing Vehicular Communication: Demonstration of Implementation and Operation. IEEE Vehicular Technology Conference VTC. Sophia Antipolis, France. 1–2.
4. Raya, M. and Hubaux, J.-P. 2007. Securing vehicular ad hoc networks. J. Comput. Secur., 15(1): 39–68. ISSN 0926-227X. URL http://dl.acm.org/citation.cfm?id=1370616.1370618.
5. Douceur, J. R. 2002. The Sybil Attack. Revised Papers from the First International Workshop on Peer-to-Peer Systems. London, UK, UK: Springer-Verlag. IPTPS ’01. ISBN 3-540-44179-4. 251–260. URL http://dl.acm.org/citation.cfm?id=646334.687813.
6. Bouassida, M., Guette, G., Shawky, M. and Ducourthial, B. 2007. Sybil nodes detection based on received signal strength variation within VANETs. INTERNATIONAL JOURNAL OF NETWORK SECURITY, 2009. 9(1): 22– 33. URL http://hal.archives-ouvertes.fr/hal-00333140/ en/. 7. Guette, G. and Ducourthial, B. On the Sybil attack detection in VANET. MASS. IEEE. ISBN 978-1-4244-1454-3. 1–6. URL http://dblp. uni-trier.de/db/conf/mass/mass2007.html#GuetteD07.
8. Sichitiu, M. L. and Kihl, M. 2008. Inter-vehicle communication systems: A survey. IEEE Communications Surveys and Tutorials, 10(1-4): 88–105. URL http://dblp.uni-trier.de/db/journals/comsur/ comsur10.html#SichitiuK08.

9. Jiang, D. and Delgrossi, L. 2008. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. Proceedings of the IEEE Vehicular Technology Conference - Spring. 2036–2040. doi:http: //dx.doi.org/10.1109/VETECS.2008.458.

10. Aijaz, A., Bochow, B., Dtzer, F., Festag, A., Gerlach, M., Kroh, R. And Leinmller, T. 2006. Attacks on Inter Vehicle Communication Systems - an Analysis. In Proc. WIT. 189–194.

11. Papadimitratos, P., Gligor, V. and Hubaux, J.-P. 2006. Securing Vehicular Communications - Assumptions, Requirements, and Principles. WORKSHOP ON EMBEDDED SECURITY IN CARS. 5–14.

12. Yang, Q., Lim, A., Ruan, X. and Qin, X. 2010. Location Privacy Protection in Contention Based Forwarding for VANETs. Proceedings of the Global Communications Conference, 2010. GLOBECOM 2010, 6-10 December 2010, Miami, Florida, USA. IEEE. ISBN 978-1-4244-5638-3. 1–5. doi: http://dx.doi.org/10.1109/GLOCOM.2010.5684166.

13. Alsharif, N., Wasef, A. and Shen, X. 2011. Mitigating the Effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks. ICC. IEEE. ISBN 978-1-61284-232-5. 1–5.

14. Leinm¨uller, T., Schoch, E. and Maih¨ofer, C. 2007. Security Issues and Solution Concepts in Vehicular Ad Hoc Networks. Proceedings of the Fourth Annual Conference on Wireless On demand Network Systems and Services (WONS 2007). Obergurgl, Austria.

15. Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A. And Raya, M. 2007. Architecture for Secure and Private Vehicular Communications. INTERNATIONAL CONFERENCE ON ITS TELECOMMUNICATIONS. IEEE Computer Society. 1–6.

16. Golle, P., Greene, D. and Staddon, J. 2004. Detecting and correcting malicious data in VANETs. Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. New York, NY, USA: ACM. VANET ’04. ISBN 1-58113-922-5. 29–37. doi:10.1145/1023875.1023881. URL http://doi.acm.org/10.1145/1023875.1023881.

17. Newsome, J., Shi, E., Song, D. and Perrig, A. 2004. The sybil attack in sensor networks: analysis & defenses. Proceedings of the 3rd international symposium on Information processing in sensor networks. New York, NY,

USA: ACM. IPSN ’04. ISBN 1-58113-846-6. 259–268. doi:10.1145/984622.984660. URL http://doi.acm.org/10.1145/984622.984660.

18. Breuer, J., Held, A., Leinmller, T. and Delgrossi, L. 2008. Trust issues for vehicular ad hoc networks. in 67th IEEE Vehicular Technology Conference VTC2008- Spring.

19. Raya, M. and Hubaux, J.-P. 2007. Securing vehicular ad hoc networks. J. Comput. Secur., 15(1): 39–68. ISSN 0926-227X.

20. Khalili, A., Katz, J. and Arbaugh, W. A. 2003. Toward Secure Key Distribution in Truly Ad-Hoc Networks. Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT’03 Workshops). Washington, DC, USA: IEEE Computer Society. SAINT-W ’03. ISBN 0-7695-1873-7. 342–.

21. Hubaux, J.-P., Capkun, S. and Luo, J. 2004. The Security and Privacy of Smart Vehicles,

22. Sun, X., Lin, X. and Ho, P.-H. 2007. Secure Vehicular Communications Based on Group Signature and ID-Based Signature Scheme. Proceedings of IEEE International Conference on Communications, ICC 2007, Glasgow, Scotland, 24-28 June 2007. IEEE. 1539–1545. doi:http://dx.doi.org/10.1109/ICC.2007.258.

23. Piro, C., Shields, C. and Levine, B. N. 2006. Detecting the Sybil attack in mobile ad hoc networks. in Proc. SecureComm. IEEE Press. 1–11.

24. Park, S., Aslam, B., Turgut, D. and Zou, C. C. 2009. Defense against Sybil attack in vehicular ad hoc network based on roadside unit support. Proceedings of the 28th IEEE conference on Military communications. Piscataway, NJ, USA: IEEE Press. MILCOM’09. ISBN 978-1-4244-5238-5. 37–43. URL http://dl.acm.org/citation.cfm?id=1856821.1856828.

25. Yan, G., Olariu, S. and Weigle, M. C. Providing VANET Security Through Active Position Detection.

26. Raya, M., Aziz, A. and Hubaux, J.-P. 2006. Efficient secure aggregation in VANETs. Holfelder, W., Johnson, D. B., Hartenstein, H. and Bahl, V., eds. Vehicular Ad Hoc Networks. ACM. ISBN 1-59593-540-1. 67–75.

27. Raya, M., Papadimitratos, P., Aad, I., Jungels, D. and Hubaux, J.- P. 2007. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. IEEE Journal on Selected Areas in Communications, 25(8): 1557– 1568.

28. Leinmller, T., Schoch, E. and Kargl, F. 2006. Position Verification Approaches for Vehicular Ad-Hoc Networks. IEEE Wireless Communications, Special Issue on ”Inter-Vehicular Communications, 16–21.

29. Zhou, T., Choudhury, R. R., Ning, P. and Chakrabarty, K. 2011. P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, 29(3): 582–594.

30. Raya, M. and Hubaux, J.-P. 2005. The security of vehicular ad hoc networks. Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM. SASN ’05. ISBN 1-59593-227-5. 11–21. doi:10.1145/1102219.1102223.