IMPROVING NEIGHBORING VEHICLE METHOD TO DETECT SYBILE ATTACK IN VEHICULAR AD HOC NETWORK

HODA SOLTANIAN BOJNORD

A thesis submitted in partial fulfillment of

the requirements for the award of the degree of

Master of Computer Science (Information Security)

Advanced Informatics School

Universiti Teknologi Malaysia

JUNE 2013

ABSTRACT

Recent technology known as Vehicular Ad Hoc Network (VANET) is invited to serve new vehicle driving experience. It is very useful to mitigate collision and utilizes traffic. Even though, VANET seems to be a promising technology, its drawbacks are inadequate with the security for a public accessible technology. VANET security is essential because a badly designed VANET is vulnerable to network attacks, and this may danger the safety of drivers, and As long as VANETs are the wireless network, there are different kinds of attacks and threats can happen in VANETs. Sybil attack is one of the most important attacks in VANETs. This thesis deals with the problem of the security in VANET especially in Sybil attack. In Sybil attack, a vehicle makes the identities of several vehicles; these IDs can be used for playing any kind of attack in the network. These false identities also create the illusion that there are additional vehicles on the road. In this research, a robust detection mechanism against Sybil attack in VANET is addressed based on fuzzy detection mechanism. Our contribution behind the implementation of proposed approach is that each vehicle has different set of neighbors providing sufficiently high density in VANET. In the simulation section, we study the proposed method in different ways and present the efficiency of the fuzzy method based on true and false detection rate and overall overhead.

ABSTRAK

Teknologi terkini yang dikenali sebagai kenderaan Ad Hoc Network (VANET) adalah dijemput untuk berkhidmat baru pengalaman memandu kenderaan. Ia amat berguna untuk mengurangkan perlanggaran dan menggunakan lalu lintas. Walaupun, VANET seolah-olah menjadi satu teknologi yang cerah, kelemahannya adalah tidak mencukupi dengan keselamatan untuk teknologi diakses awam. VANET keselamatan adalah penting kerana VANET yang direka buruk adalah terdedah kepada serangan rangkaian, dan ini boleh menjejaskan keselamatan pemandu, dan Selagi VANETs adalah rangkaian tanpa wayar, terdapat pelbagai jenis ancaman dan serangan yang mungkin berlaku pada VANETs. Sybil serangan adalah salah satu serangan yang penting pada VANETs. Tesis ini berkaitan dengan masalah keselamatan di VANET terutama dalam Sybil serangan. Dalam serangan ini, memalsukan identiti kenderaan pelbagai kenderaan; identiti ini boleh digunakan untuk bermain apa-apa jenis serangan dalam sistem. Ini identiti palsu juga mewujudkan ilusi bahawa terdapat kenderaan tambahan di jalan raya. Dalam kajian ini, satu mekanisme pengesanan yang teguh terhadap Sybil serangan di VANET ditujukan berdasarkan mekanisme pengesanan fuzzy. Sumbangan kami di sebalik pelaksanaan pendekatan yang dicadangkan ialah setiap kenderaan mempunyai set jiran menyediakan kepadatan yang cukup tinggi dalam VANET. Dalam seksyen simulasi, kita mengkaji kaedah yang dicadangkan dalam cara yang berbeza dan menyampaikan kecekapan kaedah fuzzy berdasarkan benar dan palsu kadar pengesanan dan overhed keseluruhan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATION

DMV	-	Department of Motor Vehicle
EDR	-	Event Data Recorder
ELP	-	Electronic License Plate
GPS	-	Geographical Positioning System
MAC	-	Medium Access Control
MANET	-	Mobile Ad hoc Network
OBU	-	On-Board Units
PKI	-	Public Key Infrastructure
RSU	-	Road-Side Units
VANET	-	Vehicular Ad hoc Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

Every year many accidents take place which causing injuries and fatalities. For example, from 2000 through 2004, there were 44,192 accidental deaths in Canada; 32% of them (14,082) were the result of motor vehicle accidents (Ramage-Morin, 2008). The statistics are worse in the U.S.; the health care expenses associated with these accidents form a burden on the economy of any country. These statistics raise the query to achieve better road safety. As a result for the advances in wireless communications technologies, Vehicular Ad hoc Network (VANET) emerged as an excellent candidate to change the life style of the traveling passengers along the roads and highways in terms of improving the safety levels and providing a wide range of comfort applications.

VANET is a special type of Mobile Ad hoc Network (MANET) that provides communication between (1) close vehicles and (2) vehicles and close roadside facilities (Fussler et al., 2007).VANETs are one way to apply Intelligent Transportation System, a method for transmitting information and communication technology (Manvi et al., 2008) of transport infrastructure and vehicles. VANET is based on IEEE 802.11p standard (Jiang et al., 2008) for Wireless Access for Vehicular Environment. These systems have no fixed structure, and they depend on themselves for the implementation of the network features (Sichitiu et al., 2008). A VANET is a decentralized network as each node performs the functions of both host and router. The main advantage of VANET communications strengthening of passenger security through exchange of warning messages between the vehicles. VANETs differ from MANETs in high mobility of the nodes, large scale networking, and geography limited topologies, and common system fragmented. Most of the research on VANET focuses on Medium Access Control (MAC) layer and the network layer (Boukerche, 2008).VANETS objectives to create applications such as collision avoidance, path changes, and so on.

VANET, being a wireless network, inherits all the security threats that a wireless system has to deal with (Qian et al., 2008).VANET security is essential because a badly designed VANET is vulnerable to network attacks, and this may endanger the safety of drivers. A security system must ensure that transfer is from a trusted source and is not a modified en route from other sources. It must also strike the right balance with privacy because implementation of security and privacy together in a system is conflicting so the security of VANETs is remains largely an exploration field.

VANET security is different from that of wireless and wired networking because it is unique features of mobility limitations, infrastructure-less framework and short term links between the nodes. In the wired network, the infrastructure components of specific features, for example, the router determine the route to destination while a network host sending and receiving messages. Security application is relatively simple as networks have to physically alter for listening.

Wireless networks use infrared or radio frequency signals to communicate between devices. These networks may be either (a) infrastructure based or (b) infrastructure-less. Infrastructure-based wireless networks are based on Public Switched Telephone Network switches, MSCs, base stations, and mobile hosts. In ad hoc networks, a kind of infrastructure-less wireless networks, nodes perform all operations such as routing, packet forwarding, and network administration, and so on. The current security solutions use conventional digital signature (El Zarki et al., 2002) and by using Public Key Infrastructure (PKI).

In VANETs, main focus of security is in safety-relevant applications. Non safety applications are less rigorous security requirements. There is no prior trust relationship between the nodes of VANETs because of its infrastructure-less character. Any node can join and leave the network at any time without informing other nodes in vicinity. Cooperative security systems are more effective in VANETs as node misbehavior can be found via collaboration among the numbers of nodes by assuming that majority of nodes are honest.

As long as VANETs are a wireless network, there are different kinds of attacks and threats can occur in VANETs. It is essential that VANET security must be able to handle all types of attacks. Sybil attack is one of the major attacks in VANETs. Sybil attack may occur in each situation where there is no centralized device control of all entities in the network. As wireless communication is more susceptible to security threats, Sybil attack leaves its effect on all the wireless networks. This research deals with the problem of the security in VANET particularly in the Sybil attack.

1.2 Background of problem

VANETs have the following characteristics which distinguish themselves from other wireless networks (Chen et al., 2011):

a) The unique mobility model which is limited by roads, speed, and neighboring nodes.
b) The rich functionalities of network nodes (e.g., high computing ability, unlimited power supply).
c) The fast changing network topology and the short-lived communication link.
d) In some intersections and hot spots, there are scattered authorized infrastructures to provide extra services.

Sybil attack detection on VANETs is the challenging problem because of the aforementioned properties of them. The Sybil attack would also become a serious threat to VANETs because:

1) It may bring extremely negative influence to the security of VANETs and the safety of drivers by emerging the wrong traffic information in network or by not forwarding the warning messages (Chen et al., 2011).
2) If number of Sybil attackers increase significantly in a network, they can take over the control of the whole network (Grover et al., 2010).
3) It violates the fundamental assumption of the VANET research (Park et al., 2009).

Due to highly dynamic property of the VANETs fast and completely detecting of the Sybil attacks can reduce the adverse safety effect of Sybil attacks and the performance reduction of VANETs due to Sybil attacks.

As will be discussed later in literature review chapter, there are many methods presented to detecting the Sybil attack, some of them neglect the privacy of the vehicles (Zhou et al., 2007), some of them will not applicable on crowded or empty highways or streets, some methods adapted from other networks and does not work on high speed vehicles on highways and some of them needs cryptographic methods which needs expensive devices to implement in real vehicles (Kaur et al., 2012).

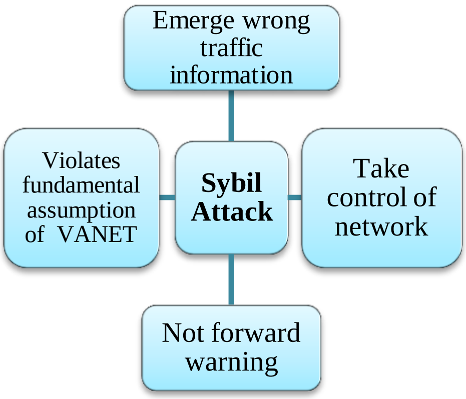
Emerge wrong traffic information
Violates fundamental assumption of VANET
Sybil Attack
Take control of network
Not forward warning

Figure 1-1 Sybil attack threats

1.3 Problem Statement

Due to the problem above one general and applicable method is needed to defend against Sybil attack which both preserve the privacy of the vehicles and work in every situation even crowd or empty roads, in highways or streets. The Neighboring Vehicles method cover the above requirements (Kaur et al., 2012). In Detection using Neighboring Vehicles approach every node participates to detect the suspect node in the network. Every vehicle has a different group of neighbors at different time interval. If every vehicle has same neighbors at different interval then that vehicle is a suspect (Grover et al., 2011).

In this method computation are required to calculate the neighboring information of the vehicles as nodes in the neighborhood of the vehicles change their position rapidly, high computation property of this method make this method a slow detection scheme and this method is being unable to detect the Sybil attack at the early time of incident (Kaur et al., 2012).

1.4 Research Questions

The main questions this research motivates to answer are as follows:

1) What are the various Sybil attack detection schemes function, requirements and practicality on VANETs?
2) What are the possible approaches to improve performance weakness (e.g. computation time) of Neighboring Vehicles method to detect Sybil attacks on VANETs?
3) How to evaluate the performance improvement of Neighboring Vehicles method to detect Sybil attack on VANETs?

1.5 Project Aim

The aim of this study is to investigate various approaches for detecting Sybil attacks function, requirements and practicality on VANETs, improve the Neighboring Vehicles detection method computational time consumption on detecting Sybil attacks on VANETs, in this way the VANETs against Sybil attacks are more defiance and totally the VANETs become more reliable. The following aims are represented in below:

1- Investigate on various detection scheme functionality and practicality.
2- Introducing the improved Neighboring Vehicles method to detect Sybil attack.
3- Performance assessment of the improved Neighboring Vehicles detection method for detecting Sybil attacks on VANETs.

1.6 Project Objective

The objectives of this study can be arranged as follows:

I. To investigate the current methods to detect Sybil attacks on VANETs.
II. To improve detection using the Neighboring Vehicles method to detect Sybil attacks on VANETs.
III. To evaluate detection using the Neighboring Vehicles method to detect Sybil attacks on VANETs.

1.7 Scope of the Study

This research focuses on improving a neighboring method against Sybil attack on the VANETs in a way that some of the problems mentioned in the problem statement will rectify. The proposed methods will be in the area where all nodes are equipped with same wireless communication equipment necessary for establishing a VANET. There are a certain number of vehicles traveling independently and most of them are trusted. Only a few of the drivers may perform the Sybil attack. It is assumed that clocks of all the nodes are synchronized and their transmission range is same meters in this case. Some RSUs (Road-Side Units) are uniformly deployed in the network either in the form of a traffic light or any service provider (providing information about petrol pumps, hospitals, and restaurants) take into assumption. For physical and MAC (Medium Access Control) layers is assumed in 802.11p, and routing protocol AODV. To evaluate the proposed method the simulation software would be NS2, which is combined with MOVE and SUMO.

1.8 Significance of the study

Until recently, road vehicles were the realm of mechanical engineers. But with the plummeting costs of electronic components and the permanent willingness of the manufacturers to increase road safety and to differentiate themselves from their competitors, vehicles are becoming “computers on wheels”, or rather “computer networks on wheels” (Hubaux et al., 2005). VANET technology provides a fast, easy to deploy and an inexpensive solution for intelligent traffic control and traffic disaster preventive measure. In VANET, moving vehicles communicate using wireless technology. This communication can be used to divert traffic from congested or dysfunctional routes, to seek help in an emergency and to prevent accident escalation in addition to providing intelligent traffic control. However, an attacker can use the same system to spread false warning messages resulting in congestion on certain routes thereby leading to accidents or causing delay in providing help etc. (Grover et al., 2010). One of these threats is Sybil attacks, in which a malicious vehicle creates an illusion of traffic congestion by claiming multiple identities. Not only does this create an illusion, it has the potential to inject false information into the networks via a number of fabricated non-existing vehicles; it can even launch further DoS attacks by impairing the normal operations of data dissemination protocols (Xiao et al., 2006). There are many possible methods to defend against Sybil attack, but the effective defense against Sybil attack should firstly identifies an attack and attacker in the very first of its launch to reduce the degree of its damage. In this project by reducing the computation time, detection will settle the Sybil attack in the early stage of its occurrence.

1.9 Summary

This chapter introduced of the importance of VANET and security on VANETs and described about its problem. Afterwards, we present research objective, research scope and significance about the project. The next chapter presents the review of the VANET and Sybil attack and related work.

REFERENCES

Akyildiz, I. F., & Wang, X. (2005). A survey on wireless mesh networks. *Communications Magazine, IEEE, 43*(9), S23-S30.

Armknecht, F., Festag, A., Westhoff, D., & Zeng, K. (2007). *Cross-layer privacy enhancement and non-repudiation in vehicular communication.* Paper presented at the Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference.

Boukerche, A. (2008). Algorithms and protocols for wireless, mobile ad hoc networks (Vol. 77): Wiley-IEEE Press.

Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. (2012). Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. *Parallel and Distributed Systems, IEEE Transactions on, 23*(6), 1103-1114.

Chen, C., Han, W., & Wang, X. (2011). Sybil attack detection based on signature vectors in VANETs. *International Journal of Critical Computer-Based Systems, 2*(1), 25-37.

Chen, C., Wang, X., Han, W., & Zang, B. (2009). *A robust detection of the sybil attack in urban vanets.* Paper presented at the Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on.

Choi, J. Y., Golle, P., & Jakobsson, M. (2006). *Tamper-evident digital signature protecting certification authorities against malware.* Paper presented at the Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on.

Creswell, J. W. (2008). Research design: Qualitative, quantitative, and mixed methods approaches: Sage Publications, Incorporated.

Douceur, J. (2002). The sybil attack. *Peer-to-peer Systems*, 251-260.

El Zarki, M., Mehrotra, S., Tsudik, G., & Venkatasubramanian, N. (2002). *Security issues in a future vehicular network.* Paper presented at the European Wireless.

El Zoghby, N., Cherfaoui, V., Ducourthial, B., & Denœux, T. (2012). Distributed Data Fusion for Detecting Sybil Attacks in VANETs. *Belief Functions: Theory and Applications*, 351-358.

Fussler, H., Schnaufer, S., Transier, M., & Effelsberg, W. (2007). *Vehicular ad-hoc networks: from vision to reality and back.* Paper presented at the Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference on.

Golle, P., Greene, D., & Staddon, J. (2004). *Detecting and correcting malicious data in VANETs.* Paper presented at the VANET '04 Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks.

Grover, J., Gaur, M. S., Laxmi, V., & Prajapati, N. K. (2011). *A sybil attack detection approach using neighboring vehicles in VANET.* Paper presented at the SIN '11 Proceedings of the 4th international conference on Security of information and networks.

Grover, J., Kumar, D., Sargurunathan, M., Gaur, M., & Laxmi, V. (2010). Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks. *Recent Trends in Network Security and Applications*, 473-482.

Guette, G., & Ducourthial, B. (2007). *On the Sybil attack detection in VANET.* Paper presented at the Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on.

Hao, Y., Tang, J., & Cheng, Y. (2011). *Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE.

Heron, M. P., Hoyert, D. L., Xu, J., Scott, C., & Tejada-Vera, B. (2008). Deaths: Preliminary data for 2006. *National vital statistics reports, 56*(16), 1-52.

Hubaux, J. P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *Security & Privacy, IEEE, 2*(3), 49-55.

Hubaux, J. P., Luo, J., & Raya, M. (2005). *The security of vehicular networks.* Paper presented at the Proc. of WiSe.

Isaac, J., Zeadally, S., & Camara, J. (2010). Security attacks and solutions for vehicular ad hoc networks. *Communications, IET, 4*(7), 894-903.

Jiang, D., & Delgrossi, L. (2008). *IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments.* Paper presented at the Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE.

Kaur, K., Batish, S., & Kakaria, A. (2012). Survey of Various Approaches To Countermeasure Sybil Attack. *computer science and information, 1*(4), 96-100.

Kuhn, M. (2005). *An asymmetric security mechanism for navigation signals.* Paper presented at the Information Hiding.

Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P. H., & Shen, X. (2008). Security in vehicular ad hoc networks. *Communications Magazine, IEEE, 46*(4), 88-95.

Mackey, A., & Gass, S. M. (2005). *Second language research: Methodology and design*: Lawrence Erlbaum.

Manvi, S., & Kakkasageri, M. (2008). Issues in mobile ad hoc networks for vehicular communication. *IETE Technical Review, 25*(2), 59.

Muñoz, D. (2009). Position location techniques and applications: Academic Press.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). *The sybil attack in sensor networks: analysis & defenses.* Paper presented at the IPSN '04 Proceedings of the 3rd international symposium on Information processing in sensor networks.

Park, S., Aslam, B., Turgut, D., & Zou, C. C. (2009). *Defense against sybil attack in vehicular ad hoc network based on roadside unit support.* Paper presented at the Military Communications Conference, 2009. MILCOM 2009. IEEE.

Parno, B., & Perrig, A. (2005). *Challenges in securing vehicular networks.* Paper presented at the Workshop on Hot Topics in Networks (HotNets-IV).

Pathan, A. S. K. (2010). Security of self-organizing networks: MANET, WSN, WMN, VANET: Auerbach Pub.

Piro, C., Shields, C., & Levine, B. N. (2006). *Detecting the sybil attack in mobile ad hoc networks.* Paper presented at the Securecomm and Workshops, 2006.

Pishro-Nik, H., Valaee, S., & Nekovee, M. (2010). Vehicular ad hoc networks. *EURASIP Journal on Advances in Signal Processing, 2010*(1), 864032.

Plossl, K., Nowey, T., & Mletzko, C. (2006). *Towards a security architecture for vehicular ad hoc networks.* Paper presented at the Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on.

Qian, Y., & Moayeri, N. (2008). *Design of secure and application-oriented VANETs.* Paper presented at the Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE.

Ramage-Morin, P. L. (2008). Motor vehicle accident deaths, 1979 to 2004. *Health Rep, 19*, 45-51.

Raniwala, A., & Chiueh, T. (2005). *Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network.* Paper presented at the INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE.

Raya, M., Aziz, A., & Hubaux, J. P. (2006). *Efficient secure aggregation in VANETs.* Paper presented at the Proceedings of the 3rd international workshop on Vehicular ad hoc networks.

Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39-68.

Romer, K., & Mattern, F. (2004). The design space of wireless sensor networks. *Wireless Communications, IEEE, 11*(6), 54-61.

Sichitiu, M. L., & Kihl, M. (2008). Inter-vehicle communication systems: a survey. *Communications Surveys & Tutorials, IEEE, 10*(2), 88-105.

Stampoulis, A., & Chai, Z. (2007). Survey of Security in Vehicular Networks. *Project CPSC, 534*.

Wang, Y., & Li, F. (2009). Vehicular ad hoc networks. *Guide to Wireless Ad Hoc Networks*, 503-525.

Xiao, B., Yu, B., & Gao, C. (2006). *Detection and localization of sybil nodes in VANETs.* Paper presented at the DIWANS'06.

Yan, G., Olariu, S., & Weigle, M. C. (2008). Providing VANET security through active position detection. *Computer Communications, 31*(12), 2883-2897.

Zhang, C., Lin, X., Lu, R., Ho, P. H., & Shen, X. (2008). An efficient message authentication scheme for vehicular communications. *Vehicular Technology, IEEE Transactions on, 57*(6), 3357-3368.

Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. (2007). *Privacy-preserving detection of sybil attacks in vehicular ad hoc networks.* Paper presented at the

Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on.

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