Privacy Compliant Secure Routing in VANET

Hamed Sayyadi

UNIVERSITI TEKNOLOGI MALAYSIA

PRIVACY COMPLIANT SECURE ROUTING IN VANET

HAMED SAYYADI

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 Systems
Universiti Teknologi Malaysia

FEBRUARY 2013

This dissertation is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

All praises are due to Allah for giving me the ability to write this work. All praises are due to Allah for giving me the honor of helping the humanity by contributing to enrich its knowledge.

I would like to express my appreciation and sincere thanks to my project advisor Dr**. Mohammad Abur Razzaque**, also special thanks to **Dr. Anazida Zainal** and **Dr. Majid Bakhtiari,** Department of Computer Systems and Communication, FSKSM, encouragement and patience throughoutthe duration of this project. I am extremely grateful to them for their valuable timeand vast experience which has been most critical in making this projectmeaningful and successful.

ABSTRACT

A Vehicular Ad-Hoc Network (VANET) facilitates communication between vehicles and between vehicles and infrastructure. The study of VANETs has recently become an increasingly popular research topic in the area of wireless networking as well as the automotive industries. The goal of VANET research is to develop a vehicular communication system to enable quick and cost-efficient distribution of data for the benefit of passengers' safety or comfort.

Usually, security in routing has conflict with privacy. Although, all prior works improved security on VANET routing, there is no strong advancement on privacy. This study designed a new routing protocol based on both identity and position to improve privacy compliant secure routing in VANET. The new routing protocol called as PIDP contains five kinds of packets: Route Request, Route Reply, Source Route Reply, Data, and Acknowledgement. The first three packets are based on position and the rest packets are based on identity. As a result, PIDP can hide both position and real identity of terminal nodes from intermediate nodes.

ABSTRAK

Sebuah kenderaan Ad-Hoc Network (VANET) memudahkan komunikasi antara kenderaan dan antara kenderaan dan infrastruktur. Kajian VANETs telah baru-baru ini menjadi topik penyelidikan yang semakin popular di kawasan rangkaian wayarles serta industri automotif. Matlamat VANET penyelidikan adalah untuk membangunkan satu sistem komunikasi kenderaan untuk membolehkan pengedaran cepat dan menjimatkan kos data untuk faedah keselamatan atau keselesaan penumpang.

Biasanya, keselamatan di laluan mempunyai konflik dengan privasi. Walaupun, semua lepas berfungsi meningkatkan keselamatan pada VANET routing, tidak ada kemajuan yang kuat ke atas privasi. Kajian ini direka routing protokol baru berdasarkan identiti dan kedudukan kedua-dua untuk meningkatkan privasi routing patuh selamat di VANET. Protokol routing baru yang dipanggil sebagai PIDP mengandungi lima jenis paket: Minta Laluan, Balas Route Source Reply Route, Data, dan Penghargaan. Yang pertama tiga paket berdasarkan kedudukan dan paket yang lain adalah berdasarkan kepada identiti. Hasilnya, PIDP boleh menyembunyikan kedua-dua kedudukan dan identiti sebenar nod terminal dari nod pengantara. Juga, PIDP boleh mengurangkan kelemahan Sybil serangan dan serangan Sinkhole.

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURE

LIST OF ABBREVIATION

ACK-REP	Acknowledgement Reply message
AODV	Ad hoc On-Demand Distance Vector Routing
BID	Bogus information dissemination
DSR	Dynamic Source Routing
DSRC	Dedicated Short Range Communication
FCC	Federal Communication Commission
GSIG	Group Signature
IEEE	Institute of Electrical and Electronics Engineers
IGW	Internet GateWay
MANET	Mobile Ad hoc Network
NS2	Network Simulator 2
OBU	On Board Unit
PIDP	Position-IDentity based Protocol
PKI	Public Key Infrastructure
PKTMP	Public Key Temporary
PRISM	Privacy-friendly Routing in SuspiciousMANET
RREP	Route Reply message
RREP2	source Route Reply

RREQ	Route Request message
RSU	Road Side Unit
SPECS	Secure and Privacy Enhancing Communications Schemes
VANET	Vehicular Ad hoc Network

CHAPTER 1

INTRODUCTION

1.1 Introduction

In order to increase the vehicle traffic safety, modern vehicle will be equipped with intelligent on board systems that supply drivers with valuable information. Apart from safety applications, the commuters will also be able to enjoy the non-safety application e.g. on board internet surfing, multimedia applications and so on. Currently, several ideas around the world are considering vehicular safety applications by means of short range wireless communications. (Maqsood, 2012)

The Federal Communication Commission (FCC) allocated 75 MHz spectrum at 5.9 GHz for vehicular communication in 1999 in the US to help the interchange of information between local vehicles without appropriate infrastructure. Dedicated Short Range Communication (DSRC) is an instruction for utilizing this allocated spectrum. Nowadays, Vehicular Ad hoc Network (VANET) uses this range of spectrum under DSRC to connect and transfer information between vehicles.

In VANET, in order to communicate between multi hop, the data is sent to the destination via using location-based or identity-based Ad hoc routing instead of IP addresses. There are a number of multi hop routing protocols developed over the years in which AODV, DSR, OLR are among them. The VANET plays an important role in the development of Vehicular centered applications where cars collect the local information about the road conditions and distribute this information

.

Apart from the safety information the non-safety information are also provided to the commuters, for this purpose the Internet Gateways (IGWs) are installed along the roadside to provide a temporary internet access. Though, mobility management is required to handle the mobility of a vehicle in IGW to ensure that the requested data is from the internet always deliver to the appropriate vehicle through IGW. The vehicle must also be able to discover the IGW within VANET even its multi-hop away. To address these problems the IEEE 802.11p task group made some enhancement to the MAC layer for better support of safety and non-safety applications and PHY layer to support communication distance up to 1000m. Also to enhance larger distance, multi-hop communication is to be supported in an efficient way. By enforcing such a technology in transportation, congestion problems could be solved out which could save billions of dollars of fuel, also millions of hours of waste of time on the road. (Kaur, 2012)

VANET uses cars as nodes could provide new areas for ad hoc networks. In this kind of wireless network, each participating car turn as a wireless router or node. When a car leaves the network, other cars can come and repair the route. Fixed equipment can belong to the government or private network operators or service providers.

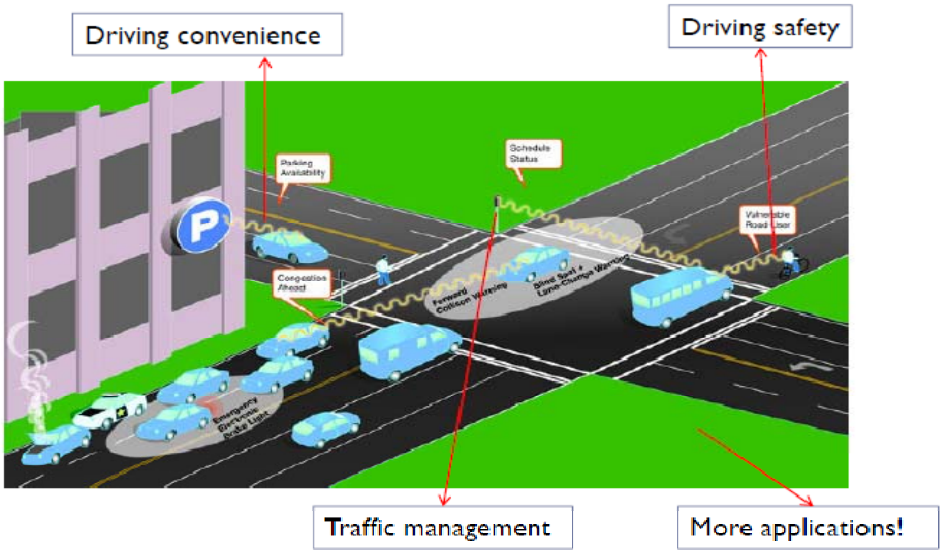

Figure 1.1: VANET structure and benefits

1.2 Problem Background

Nowadays, VANET is in the implementation phase. Message transmission in VANET is the popular area of research in which vehicles as personal nodes are supposed to be protected for the security and privacy of transferring data.Position based and identity based are two general classes of routing protocols for MANET and VANET which. Position based routing protocols (or Geographic protocols) send data to a group of nodes based on their location. PRISM is the most famous routing protocol in this area. Identity based routing protocols (or ID protocols) are designed to send data to an individual node. AODV and DSR are amongst two important identity-based protocols for MANET and VANET (Fubler, 2002).

One of the problems is that an adversary can infiltrate from the outside of the VANET or it can be a node inside VANET. The virulent effect of the presence of an adversary might be decreased if a routing protocol implies both security and privacy measures well. Security in VANET is similar to other Ad hoc networks and it could be enhanced satisfactorily by attaching cryptographic algorithms. However, approaching to a reliable privacy state is to some extent more complicated. This is due to the cumbersome procedure of hiding both location and identity of nodes in each routing protocol during data transfer.

Identity based routing protocols send their packets on the basis of the identity of the terminal notes hence, the identity privacy of these nodes can not be preserved. On the other hand, location-based routing protocols hide identity from an adversary, however, the location cannot be hidden on the grounds that the sequence of movements in a given VANET node disclose the location supposed to be hidden and secure.

1.3 Problem Statement

According to the background, the major problem in VANET is to hide both location and identity of terminal nodes from those of intermediates at the same time that is remained as a crucial challenge in sensitive cases such as military uses and law enforcement cirtcumstances(Defrawy, 2011).The vast majority of previously annotated protocols only take security into account and there is a lack of experience on important case of privacy that does not encompass solely confidentiality of communications.

1.4 Research Question

In this study, the following research questions are addressed:

i. What are the current issues which threaten privacy of nodes in VANET?

ii. What are the previous protocols privacy capabilities?

iii. How did previous protocols improve privacy of nodes in VANET?

iv. How to hide identity and location of terminal nodes from intermediate nodes?

1.5 Objectives of the Study

Based on the stated problem the objectives of this study are as follows:

i. To investigate the privacy capabilities of the existing routing protocols such as PRISM, AODV.

ii. To improve privacy compliant secure routing by designing a routing protocol to hide the identity of terminal nodes from intermediate nodes.

iii. To improve privacy compliant secure routing by designing a routing protocol to hide the location of terminal nodes from intermediate nodes.

1.6 Scope of the Study

To achieve the objectives of the study, the following scopes of the study have been identified:

i. This study reviews the available literature on PRISM and AODV privacy capabilities to hide the location and identity of terminal nodes from the intermediate nodes.

ii. Focuses on hiding identity and location of terminal nodes from intermediate nodes by using unreal identities.

iii. Designing a routing protocol based on the identity and location of terminal nodes.

iv. This study changes the AODV based on proposed routing protocol in NS2 to analyze the privacy improvements.

1.7 Organization of the Thesis

The thesis is divided into six chapters. The chapter 1 presents introduction, background of the problem, problem statement, research objectives, and scopes. Chapter 2 provides a literature review on specific characteristics of VANET, demonstration of routing protocol, and an overview of related works in security and privacy in VANET routings. Chapter 3 is dedicated to methodology of study including five segments comprising planning, analysis, design, and evaluation. In chapter 4, design and analysis of the position-identity-based routing protocol (PIDP) and its details accomplished in order to satisfy the objectives. Chapter 5 encompasses the evaluation of the achievements of the present study. Final chapter, chapter 6 is describing the conclusion and the potential future works.

REFRENCES

Abdoos, M. Faez, K. and Sabaei, M. (2009). *Position Based Routing Protocol with More Reliability in Mobile Ad Hoc Network*. World Academy of Science, Engineering and Technology 49.248-252.

AntolinoRivas, D. J. Barcelo´, M. M. Zapata, G. Morillo, J. D. (2011). *Security on VANETs: Privacy, Misbehaving Nodes, False Information and Secure Data aggregation*. Journal of Network and Computer Applications 34. PP 1942–1955.

Blazevic, L. Boudec, J. L. and Giordano, S. (2005). *A Location-Based Routing Method for Mobile Ad Hoc Networks*.IEEE Transaction on Mobile Computing, VOL. 4, NO. 2. PP 97-110.

Brestford, A. R, Stajano, F. (2005*). Location Privacy Computing*. IEEE Pervasive Computing 2, PP 46-55.

Camp, T. Boleng, J. Williams, B. Wilcox, L. Navidi, W. (2001). *Performance Comparison of Two Location Based Routing Protocols for Ad Hoc Networks*. International Conference on Mobile Computing and Networking (Mobicom), PP 243–254.

Chen, S. Wu, M. (2010).*Anonymous Multipath Routing Protocol Based on Secret Sharing in Mobile Ad Hoc Networks*. International Conference on Measuring Technology and Mechatronics Automation.IEEE.PP 582- 585.

Chim, T. W. Yiu, S. M. L. Hui, C. K. V. Li, O. K. (2011*). SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs*. Ad Hoc Networks. PP 189–203.

Defrawy, K. E. and Tsudik, G. (2011).*Privacy-Preserving Location-Based On-Demand Routing in MANETs*.IEEE Journal on Selected Areas in Communication, VOL. 29, NO. 10. PP 65-74.

Defrawy, K. E. Tsudik, G. (2008). *PRISM: Privacy-friendly Routing in Suspicious MANETs (and VANETs).* Irvine. PP 248-258.

Eichler, S. D¨otzer, F. Schwingenschl¨ogl, Ch. Caro, F. J. F. and Ebersp¨acher, J. (2004). *Secure Routing in a Vehicular Ad Hoc Network*.

Emmelman, M. Bochow, B. Kellum, C. (2010).*Vehicular Networking*. Wiley, USA.

F¨ußler, H. Mauve, M. (2002).*A Comparison of Routing Strategies for Vehicular Ad-Hoc Networks*. REIHE INFORMATIK. PP 100-114.

Festag, A. Hessler, A. Baldessari, R. Le, L. Zhang, W. and Westhoff, D. (2009). *Vehicle-to-Vehicle and Road-Side Sensor Communication for Enhanced Road Safety*.Network Research Division.

Festag, A. Noecker, G. Strassberger, M. Lübke, A. Bochow, B. Torrent-Moreno, M. Schnaufer S., Eigner, R. Catrinescu, C. and Kunisch, J. (2008). *NOW – Network on Wheels: Project Objectives, Technology and Achievements*. Proceedings of 5rd International Workshop on Intelligent Transportation (WIT). PP 211-216.

Frikha, M. (2011).*Ad Hoc Network*.Wiley, USA.

Gerlach, M. Festag, A. Leinm¨uller, T. Goldacker, G. and Harsch, Ch. (2007). *Security Architecture for Vehicular Communication*. Open Communication Systems. PP 152-158.

Harsch, Ch. Festag, A. and Papadimitratos, P. (2008).*Secure Position-Based Routing for VANETs*. Proceedings of IEEE 66th Vehicular Technology Conference (VTC Fall). PP 103-112.

Hartenstein, H. K. Laberteaux, P. (2010). *VANET*.Wiley, USA.

Hui, F. (2005).*A survey on the characterization of Vehicular Ad Hoc Networks and routing solutions*. ECS 257 Winter.

Johnson, D. B. Maltz, D. A. (1996). *Dynamic Source Routing in Ad Hoc wireless Networks, in: Mobile Computing*. Kluwer Academic Publisher.

Kaur, M. Kaur, S. and Singh, G. (2012). *VEHICULAR AD HOC NETWORKS*.Journal of Global Research in Computer Science.Volume 3, No. 3. PP 61-64.

Kent, S. T., Millet, L. I. (2002). *IDs-not That Easy: Questions about Nationwide Identity Systems*. Natl. Academy Pr. PP 42-49.

Li, F. Wang, Y. (2007). *Routing in Vehicular Ad Hoc Networks: A Survey*.IEEE VEHICULAR TECHNOLOGY MAGAZINE. PP 12-22.

Maqsood , A. Khan, R. (2012). *Vehicular Ad-hoc Networks*.IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3. PP 401-408.

Namboodin, V. Agarwal, M. and Gao, L. (2004). A Study on the Feasibility of Mobile Gateway for Vehicular Ad Hoc Networks.Proceeding of the First ACM Workshop on Vehicular Ad Hoc Networks. PP 66-75.

Perkins, C. E. Royer, E. (1999). *Ad Hoc on Demand Distance Vector Routing*.Proceeding of IEEE WMCSA. PP 344-352.

Perkins, C. E. Royer, E. (2003). *Ad Hoc on Demand Distance Vector (AODV) routing, Internet Draft, Draft-IETF-MANET-AODV.*

Qian, Y. Moayeri, N. (2008). *Design Secure and Application-Oriented VANET*. National Institute of Standards and Technology. PP 264-272.

Raya, M. and Hubaux, J. P. (2007).*Security Vehicular Ad Hoc Networks*.Journal of Computer Security, 15 (1). PP 39-68.

Sarma, A. H. K. D. Kar, B. A. and Mall, C. R. (2011*). Secure Routing Protocol for Mobile Wireless Sensor Network*. IEEE.

Xiong, H. Chen, Zh. Li, F. (2011). *Efficient and Multi-Level Privacy-Preserving Communication Protocol for VANET*.Computers and Electrical Engineering.

Zakhary, S. R. Radenkovic, M. (2009).*Reputation-Based Security Protocol for MANETs in Highly Mobile Disconnection-Prone Environments*.Computer Science & IT. PP 214-221.