# A Secure Business Framework for File Purchasing Application in Vehicular Ad Hoc networks

by

Shuang Yuan

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Master of Applied Science

in

Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2008

©Shuang Yuan 2008

## AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

# Abstract

Vehicular ad hoc networks (VANETs) are gaining growing interest from both industry and academia. Driven by road safety requirements, the car manufacturers, transportation authorities and communications standards organizations are working together to make a quantum step in terms of vehicular information technology (IT) by equipping the vehicles with sensors, on-board processing and wireless communication modules. VANETs are composed of OBUs (On Board Units) and RSUs (Road Side Units). The communication standard used in VANETs is called DSRC (Dedicated Short Range Communication). With many essential vehicle components (radios, spectrum, standards, etc) coming into place, a lot of new applications are emerging beside road safety, which support not only safety related services, but also entertainment and mobile Internet access services.

In this study, we propose a promising commercial application for file purchasing in VANETs, where a legitimate vehicle can purchase digital files/data through a roadside unit (RSU). Due to the high mobility of the vehicles, the contact period between an RSU and a vehicle could be insufficient to download the complete file. To purchase a digital file, a vehicle purchases a permission key from a fixed RSU and then begins to download the file from the RSU via vehicle-to-RSU communications (V2R) when it is in the transmission range of the RSU. Once the vehicle in the process of downloading a file leaves the transmission range of the RSU, its neighboring vehicles with a piece of the file cooperatively help to complete the file transfer via vehicle-to-vehicle (V2V) communications. Such a commercial file purchasing system can obviously initiate a new application scenario. However, it cannot be put into practice unless the security issues, such as the user privacy, incentives for inter-vehicle cooperation, and the copyright protection for the file content are well addressed. In order to deal with these security issues, we develop a secure business framework for the file purchasing system in this study. In this framework, we preserve the user privacy by using the pseudo

identity for each vehicle. We stimulate the cooperation between vehicles through micro-payment incentive mechanism and guarantee the secure payment at the same time. To protect the digital file content from unauthorized distribution, we encrypt the file content before delivery to an end user and use digital fingerprint technology to generate a unique copy for each vehicle after delivery. In a word, we propose a file purchasing application in VANETs and also develop a secure framework for this application.

# Acknowledgements

First of all, I would like to thank my supervisor Prof. Pin-Han Ho, for his numerous support and encouragement throughout the pursuit of my master degree. He helped me to set up the master's research topic and gave me tremendous assistance on how to do the research. I could not explain in pale words how much I have learned from him as a great mentor and respectable scholar.

I am also thankful to Prof. Sherman Shen for his advices and help during my study. He gave us his valuable suggestions and encouragement every time at the group meeting. I would especially like to acknowledge Prof. Naik for being my thesis reader.

I also thank Prof. Agnew for his assistance for my five-month internship. I have learned a lot from the internship and gained the working experience from it.

I would also like to thank to Chenxi Zhang, a Ph.D. student in the same group as me, who helped me during the cooperation of the projects. He is such a diligent and friendly person who gave me generous help. I would also like to thank to all the other members in BBCR group who helped me in my master's program and make my life memorial.

My very special thanks also go to the faculty and staff in the Department of Electrical and Computer Engineering for their financial, technical and logistic support. Their kindness and care have made my stay here a very rewarding and enjoyable experience.

# Table of Contents

AUTHOR'S DECLARATION ..... ii

Abstract ..... iii

Acknowledgements ..... v

Table of Contents ..... vi

List of Figures ..... viii

List of Tables ..... ix

Chapter 1 Introduction ..... 1

1.1 Vehicular ad-hoc networks (VANETs) ..... 1

1.2 Wireless communication technology in VANETs ..... 1

1.3 Characteristics of VANETs ..... 5

1.4 Applications on VANETs ..... 6

1.5 Security requirements and objectives ..... 9

1.6 Contributions of the thesis ..... 11

1.7 Outline of the thesis ..... 12

Chapter 2 Background and Related work ..... 13

2.1 Security in safety-related applications ..... 13

2.1.1 Classification of the attacks ..... 14

2.1.2 Attack models ..... 15

2.1.3 Security requirement ..... 16

2.1.4 Related work ..... 18

2.2 Security in commercial applications ..... 24

2.2.1 Related work ..... 24

2.3 Preliminaries ..... 26

2.3.1 Micropayments ..... 26
2.3.2 One-way hash chain ..... 27
2.3.3 Digital fingerprints ..... 29
Chapter 3 A Secure Business Framework for File Purchasing in VANETs ..... 30
3.1 Overview of the file purchasing application ..... 30
3.1.1 Network model ..... 31
3.1.2 User-broker-seller relationship model ..... 34
3.1.3 Payment certificate model ..... 35
3.1.4 Tamper-proof secure module ..... 36
3.2 The proposed secure transaction protocol ..... 36
3.2.1 Permission purchasing ..... 37
3.2.2 File collecting ..... 38
3.2.3 File reading ..... 42
3.3 Security analysis ..... 44
3.4 Performance analysis ..... 47
3.4.1 Communication cost ..... 47
3.4.2 Computation overhead ..... 49
3.4.3 Delay analysis ..... 50
Chapter 4 Conclusion and Future Work ..... 54
Bibliography ..... 55

# List of Figures

Figure 2-1: Hash Chain ..... 28

Figure 3-1: Network Model ..... 33

Figure 3-2: Tamper-proof device ..... 43

Figure 3-3.Transmission Overhead vs Piece Size ..... 49

Figure 3-4: The map used in simulation ..... 51

Figure 3-5: Delay vs Transmission Interval ..... 52

Figure 3-6: Delay vs Probability ..... 53

# List of Tables

Table 1-1: Comparison of 915M Hz and 9.5G Hz DSRC technologies ..... 4

Table 1-2: A Comparison of Wireless Technologies ..... 4

Table 3-1: Notations ..... 34

# Chapter 1 Introduction

## 1.1 Vehicular ad-hoc networks (VANETs)

With the rapid development of micro-electronic and wireless communication technologies, vehicles are becoming “computers on wheels” by equipped with intelligent electronic devices called as wireless On Board Units (OBUs). The OBUs integrate computing processers, Global Positioning System (GPS), sensing and storage devices together, providing Ad-Hoc Network connectivity for vehicles. With the OBUs, vehicles can communicate with each other when moving on roads and with fixed roadside infrastructure as well when passing by them. These fixed roadside infrastructures are described as Roadside Units (RSUs), which are usually connected to backbone Internet though wired or wireless connection. Thus, the vehicle-to-vehicle (V2V) communications and vehicle-to-roadside infrastructure (V2I or V2R) communications basically form the Vehicular Ad Hoc networks (VANET) which are attracting considerable attention from both automotive industry and research community.

## 1.2 Wireless communication technology in VANETs

Dedicated Short-Range Communication (DSRC) is a set of standards specially designed for vehicular networks which aim to provide wireless communication services over vehicle-to-vehicle (V2V) and vehicle-to-roadside infrastructure (V2I) channels. The first generation of DSRC system worked at 915MHz with the transmission rate of 0.5Mb/s. Currently, all the standards organization are developing the second generation DSRC which overcomes many of the weakness associated with 915MHz DSRC and provides higher data rate and longer transmission range. The current DSRC protocol is working at the 5.9 GHz band (U.S.) or 5.8 GHz band (Japan, Europe).

There are many international or national organizations working on DSRC standards programs all over the world, such as ISO, European CEN, Japan, etc. As an international standardization, ISO TC (Technical Committee) 204 is working for ITS (Intelligent Transport Systems). Within TC204, WG (Working Group) 15 and WG (Working Group) 16 are working on DSRC or DSRC-like communication standards. The European CEN organization has developed its DSRC standards for the Physical Layer (L1), Data Link Layer (L2), and Application Layer (L7). The Japanese have published ARIB T55 as their DSRC standards. A new Japanese generation of standards, ARIB T75, is finished at December 2007.

The current North America DSRC standards are being coordinately developed by many standards organizations such as ASTM (American Society for Testing and Materials), ITS America, IEEE and ISO. They are focusing on the new spectrum available at 5.9 GHz. In October 1999, US FCC (Federal Communication Commission) allocates 75MHz of bandwidth in the 5.850 to 5.925 GHz band for DSRC. The North American DSRC standards program aims at creating an interoperable standard to allow the US, Canadian, and Mexican ITS programs to enable a whole new class of communications and a new class of applications to support future transportation systems and needs. The primary goal is to enable the drivers to send and receive the up-to-date information to increase the driving safety, but many other applications which provide the comfort driving experience for passengers are also considered and allowed. The safety-related applications will have the highest priority in terms of access to the spectrum, but commercial applications will also use this bandwidth as long as they comply with the prioritization scheme.

The 5.9G Hz DSRC have much more advantages over the 915M Hz DSRC. A comparison of them is listed in Table 1-1. First, the transmission range is largely increased. The 5.9G Hz DSRC has transmission range up to 1000 meters, while the 915M Hz DSRC has transmission range less than 30 meters. Next, the 5.9G Hz DSRC supports high speed data rate ranging from 6Mb/s to 27Mb/s while

the 915M Hz DSRC supports only 0.5Mb/s data rate. Third, the interference for 5.9G Hz is much lower than 915M Hz DSRC because the only interference at 5.9G Hz is from sparsely located military radars and satellite uplinks but there are many other uses on 915M Hz such as 900M Hz PHONES, rail car AEI readers and wind profile radars. In addition, the 915M Hz DSRC only has single unlicensed channel. Whereas, the 5.9G Hz DSRC provides seven channels with each of 10M Hz. One channel is reserved for the control channel and the other six channels are used for service channels. The control channel supports both safety messages and very short service channel announcements or messages only, and any extensive data exchange is conducted on service channels. In DSRC, Vehicles must periodically switch to the control channel to receive the safety message. The period time is chosen from 100ms to 300ms to guarantee the safety messages are exchanged in real-time. When a vehicle discovers an interesting service, it will switch to a service channel as long as it does not affect the safe message application. For example, an RSU provides map update service. A vehicle demands this service from the RSU and switch to a service channel to begin the transfer of the map. If the transfer of the map takes too long time, the vehicle must switch to the control channel to receive safety messages and then switches back to the service channel to continue the map transfer.

| | 915M Hz Band | 5.9G Hz Band |
|---|---|---|
| Spectrum | 12M Hz | 75M Hz |
| Data Rate | 0.5Mbps | 6Mbps – 27 Mbps |
| Communication Range | 30m | 100-1000m |
| Channel Capacity | Single unlicensed channel | seven licensed channels |
| Communication Ways | Vehicle to Roadside | Vehicle to Roadside & Vehicle to Vehicle |

| | | |
|---|---|---|
| Interference Potential | High | Low |

**Table 1-1: Comparison of 915M Hz and 9.5G Hz DSRC technologies**

IEEE 802.11p is a draft amendment to the IEEE 802.11 standard used as groundwork for the PHY and MAC layers of the 5.9G Hz DSRC in the environments where the physical layer properties are rapidly changing and where very short-duration communications exchanges are required. It aims to ensure interoperability between wireless devices attempting to communicate in potentially rapidly changing communications environments. Compared with other radio communications technologies, 802.11p provides very high data transfer and low latency which are important requirements in a mobile environment. Fox example, both the cellular and satellite systems offer a significant amount of bandwidth but have too long latency which is not suitable for up-to-date information transmission in the high speed mobile networks. Furthermore, the cost of the 5.9G Hz DSRC must be low and should require no usage fee from the users to access the network. Both the cellular and satellite systems are expensive. The comparison between DSRC and other wireless technologies is listed in Table 1-2 [DSRC_Home].

| | DSRC | Cellular | Satellite |
|---|---|---|---|
| Range | 100m -1000m | Kilometers | Thousands of kilometers |
| Latency | 200us | 1.5 - 3.5s | 10 - 60s |
| Data Rates | 6-27Mbps | Future 2-3Mbps | |
| Cost | None | Expensive | Very expensive |

**Table 1-2: A Comparison of Wireless Technologies**

## 1.3 Characteristics of VANETs

Vehicular Ad-hoc networks are one type of ad hoc networks, but have significantly different characteristics from other wireless ad hoc network such as sensor network, mobile ad hoc network, etc.

*Infrastructure-based:* VANETs are infrastructure-based networks which have RSUs usually located at some high traffic density places by transportation government to provide services for every vehicle passing by them. With these RSUs connected with the Internet, VANETs can provide reliable broadband communication services, access online resources, communicate with other people, and access local services (e.g., traffic information, tourist information) which are not residing on vehicles.

*Short connection time:* The connection time for a communication link is very short and inconstant due to the high mobility of vehicles. Vehicles can travel at a speed up to 180 km/h, which makes it difficult to maintain a long V2R or V2V communication connection especially when vehicles travel in opposite directions.

*Predictable mobility:* The movement of the vehicles can be predicted and limited along the road. The vehicles must stay on the road and cannot move randomly.

*No significant power constraint:* The power problem is not a big issue in vehicular networks. Unlike other mobile PDAs or laptops, power for OBUs inside vehicles can be drawn from on-board batteries and recharged from gasoline during the travelling.

*High computation ability and data rates:* Vehicle computers are equipped inside vehicles which can support heavier and larger computing devices; therefore they can provide more powerful computing ability and larger storage size (up to Terabytes of data). Together with wireless communication technology, VANETs can provide much higher data rates than other ad hoc networks.

Because of these characteristics, the requirements for protocols used in VANETs are different from other networks.

## 1.4 Applications on VANETs

VANETs are envisioned to play an important role in the enhancement of road safety and driving experiences by providing numerous promising services. Many automobile manufacturers started planning to build communication devices into their vehicles for the purposes of safety, convenience, and entertainment. The applications on the VANETs can be classified into two classes: safety related applications and non-safety related applications.

Every year almost thousands of deaths and millions of injuries are caused by more than six million crashes in the U.S. Vehicle-to-vehicle and vehicle-to-infrastructure communications can prevent some of these collisions by warning drivers via on-board computers in vehicles about dangerous situations such as traffic signal/stop sign violation warning, road condition warning, and accident report warning. They provide a better awareness of the surrounding environment for drivers such that the drivers can make an earlier decision when meeting unsafe situation, therefore improve driving safety. A large number of safety-related applications have been proposed on VANETs. Complete applications can be found in Vehicle Safety Communications project final reports [DOT_AppendixB].

One example is the brake message warning. Many of us experienced this situation: when we were driving on the highway, suddenly, the vehicle in front of you made a brake. At that moment, we had to make a quick brake to avoid heading into the car in front of us. Even so sometimes our vehicle was just one meter away from the front one after the vehicles stopped. If we made the brake one second late, an accident could have happened. This one second is critical for people's lives. For example, it's not rare we heard that tens or even hundreds of vehicles rear-ended each other when the drivers were

not able to make an immediate decision in time. With the help of V2V communications, this kind of chained collide could be largely reduced. When a vehicle wants to brake for emergency stop, it can send a warning message including its position and current velocity to all the vehicles behind and notify them to slow down. The recipients will forward the message to the vehicles further behind. Any vehicle behind the message sender will alert its driver to slow down. In this way, the vehicles behind will get the warning information much faster than they get the information from seeing the brake lights from the vehicle in front of it. After the drivers in other vehicles receive this warning message, they will make an much earlier decision to avoid the hazardous conditions.

Another example is the called SOS service. It is used after an accident happens. It sends emergency (SOS) messages after airbags are deployed, and a rollover or other life-threatening emergency is sensed when involved in an accident. In the case that there is a roadside unit nearby, we make use of the vehicle-to-infrastructure communications to transmit the SOS messages. The emergency is sent from the vehicle to a roadside unit and then forwarded to the nearest local authority for immediate assistance. In the case that no roadside unit is nearby, emergency messages can be sent via vehicle-to-vehicle communications. The vehicle sends out emergency messages to a passing vehicle, which stores and then relays the messages when in range of a roadside unit. The message is then forwarded to the nearest local authority through Internet for immediate assistance.

In addition to reduce the number of accidents, the traffic management can be better provided by VANETs as well. For example, the traffic lights are usually changed in a fixed time interval but the traffic density is actually quite different during the different time periods in a day. Therefore, we can put an RSU on an intersection and let the RSU periodically broadcast messages requesting the traffic information from nearby vehicles. The vehicles will send the messages back reporting their position, heading direction and velocity to the RSU. The RSU then processes all the corrected information from the vehicles at the intersection and determines the optimal signal phasing of the traffic light

based on the dynamic traffic flow. For example, when you arrive at an intersection at night, the traffic light is red and you have to stop there to wait for the green light. However, because there are no cars passing by at this time, it is not reasonable to stop there for several minutes to wait for the red lights turning into green lights. In this situation, if we have an RSU at the intersection, the RSU will only receive one car's message and therefore it knows no other cars passing by. Thus, the RSU can inform the traffic lights do not change into red lights and just let the car pass by directly. In this way, the communications between RSUs and vehicles increase the efficiency of the transportation system.

Beyond these traditional safety and traffic-related applications, the availability of powerful car radios and abundant spectrum allocated by DSRC protocols make unlimited opportunities to provide a class of new interesting services in VANETs. The significant market demand for more entertainment value and better quality of life also stimulate the development of new services. These new emerging applications span many fields, such as web browsing, voice and video streaming, music downloading, local restaurant/hotel information discovering and video uploading. They create numerous commercial chances developed in vehicular networks. In this thesis, we focus on the commercial applications on VANETs. Among them, one of the most promising applications is the file (map, music, and video) purchasing application for in-car entertainment.

In VANETs, RSUs are connected to the Internet, and act as product agents of merchants. Lots of infotainment applications can be got via RSUs, such as map, music and video downloading. V2I communications enable a vehicle to purchase files and download them from RSUs. However, RSUs are only placed at some important traffic points such as busy intersections and the distance between two RSUs can be tens of kilometers, thus the transmission range of RSUs cannot fully cover everywhere along the road due to the limited transmission range of an RSU which is up to 1000m according to DSRC. When passing by an RSU, a vehicle may ask to purchase files such as a map via V2I communications and then tries to download it from the RSU. However, due to the vehicular high

mobility, the contact period between a vehicle and an RSU may be insufficient to download the whole file. Once out of the transmission range of the RSU, the file transmission between the RSU and the vehicle will be terminated. On the other hand, although the vehicle is not in the communication range of the RSU, it is still in the communication range of its neighboring vehicles. If its nearby vehicles have bought this file before, they can transmit the file to it via V2V connections. Thus, what the buyer needs to do is paying the RSU to get allowed to use the file, but does not have to download the file from the RSU. Instead, it can get this file from other vehicles. We divide the file into several small pieces. A buyer can buy the permission to use the file from an RSU firstly and then collect different pieces of the file from the RSU and other different vehicles.

In such an application scenario, the file is typically shared among vehicles. The V2V file sharing among the vehicles brings a great advantage to a buyer. The buyer does not need to depend on an RSU to get the file. Otherwise, it may have to stop to wait for the file transmission completed.

## 1.5 Security requirements and objectives

To implement such a system in reality, we have to take security issues into consideration.

The V2V file sharing transmission depends on the cooperation of the vehicles. In reality, some users may not want to transmit the files for free. To make such an application work, our scheme has to provide incentives to motivate the vehicles to transmit the files. The buyer pays vehicles which send the pieces of the file to him/her. However, because these two parties (the buyer and the sender) are both individual and they cannot trust each other, the security problem appears. The buyer can deny getting the pieces and the sender can deny receiving the payments. Thus, the proper incentives and security mechanisms have to be considered to deploy this application in reality. In this thesis, we use micropayment to solve this problem.

The second security issue in such an application is confidential problem. Because the application has commercial purpose, the file should be encrypted and only the user who pays for it can get the permission key to decrypt it. The permission key should only be obtained from RSUs. To get a permission key, the user has to pay an RSU. The permission key for individual buyer to open the file should be different; otherwise one vehicle who bought this file can simply give its permission key to the others. It implies that we have to find a way to bind the user identity and the permission certification together to authenticate the buyer before it can decrypt the map.

Another problem is copyright issue. A digital file can be copied and instantaneously distributed everywhere, thus potentially depriving the copyright holder of revenue from licensed sales. As a result, we have to prevent the users from generating unauthorized copy after it decrypts the file. For example, we assume that one vehicle V1 wants to buy a digital map from an RSU. The other vehicle V2 who bought this map before is V1's friend. V1 can simply get the copy from V2 without paying an RSU. Therefore, the service provider, the RSU (an agent of the service application server), gets nothing. We cannot prevent V2 from giving the unauthorized reproduction of the copyrighted file (which belongs to RSU) to V1, but we can provide a way to trace V2 who is the distributor for unauthorized copy. Traitor tracing is an efficient copy and leak detection system. When each copy is given out, in our example, i.e., when V2 decrypts the map using its own permission certification, the unique information for V2 can be inserted into the file at the same time. This inserted information does not affect V2 to use the file, but it can imply that this copy is generated for V2. One technology that can be adopted for this problem is digital fingerprinting.

All security problems mentioned above are specifically related to our file purchasing application. In addition to these, other general security requirements for exchanging messages in VANETs are as follows:

*Message Integrity and Authentication*: The message content should not be changed during transmission and the receiver can verify that it comes from the source that it claims. Without this security requirement, messages are not safe because any adversary can change the content of messages and send fake messages.

*User authentication*: the user should be authenticated as a legitimate user before building up a communication connection.

*Preventing impersonation attack*: The adversary may pretend to be another vehicle or even an RSU to send false messages to fool others. We should prevent this kind of users.

*Non-Repudiation*: An authorized party cannot deny the message that he generated before.

*Privacy*: The protection of the drivers' privacy is another important issue as well. The drivers do not want to explore their real identities to others during transaction, which means the users should keep anonymous no matter they are buyers or sellers. We have to find proper mechanisms to prevent the tracing of a driver's identity.

## 1.6 Contributions of the thesis

The contribution of this file is two-fold. First, we introduce a new commercial application scenario in VANETs: by way of V2I and V2V communications to implement the file purchasing application in VANETs. In this application, the drivers can buy an interested file from the Internet when driving. It enhances the experience of the driving comfort. Second, the study mainly addresses the security issues happening in this application. Instead of focusing on one specific security problem, in this study, we propose a secure business framework for file purchasing in VANETs.

## 1.7 Outline of the thesis

The rest of the thesis is organized as follows: Related work and some background knowledge such as micropayment and copyright are introduced in the chapter 2. The proposed secure framework is presented in chapter 3. Finally, in chapter 4, we give the conclusions and future work.

# Chapter 2 Background and Related work

Many projects on VANETs have been made by car manufactures, government agencies and academia all over the world, which include the Vehicle Safety Communication Consortium (VSCC) developing the DSRC technology and the Vehicle Infrastructure Integration (VII) Program in USA, the car-2-car Communication Consortium in Europe, the Networks-on-Wheels Project in Germany, and the Advanced Safety Vehicle Program in Japan [VSCC, DSRC, VII C2C, NOW, ASV]. They aim to improve road safety in vehicular environments, but also provide non-safe related applications such as transport efficiency, comfort and commercial applications by the use of wireless communications. Many aspects of vehicle communications such as the medium access control (MAC) layer design [MLS2005]. [XMKS2004] and routing algorithms [TC2003, LH2004, NAG2004, K2005, and YASM2005] have been investigated. In [MLS2005], Mak *et al.* proposes a MAC protocol to support the multi-channel operation in DSRC, especially to provide potentially high bandwidth for non-safety applications provided by roadside unit in service channels without compromising safety communication occurring in a separate control channel.

## 2.1 Security in safety-related applications

To put VANETs into practice, the security problems on VANETs are important. For different applications, security demands are different but some common requirements are the same. In literatures, many related study focus on addressing security issues for safety-related applications. The safety-related applications broadcast the messages every 100-300ms according to DSRC. To transmit these messages reliable, the security issues in VANETs usually include: privacy and anonymity, authentication, non-repudiation, fast verification, etc. They can be found in [PNM2006, PGH200, ABD2006, RH2005, RH2007, RPH2006, and SURH2007]. The studies in [PNM2006, PGH2006,

and ABD2006] discussed general security issues such as attack models, security requirements, properties of inter-vehicle communications systems and system design principle but they do not provide any detailed solution. In [RH2005, RH2007, RPH2006 and SURH2007], they provide not only a detailed threat analysis in VANETs but also a set of security protocols using Public Key Infrastructure (PKI) based security schemes.

### 2.1.1 Classification of the attacks

The behavior of attacks on vehicular networks can vary widely according to their capabilities and the implemented protocols. In this section, we generally classify them into the following models from different points of view:

*Insider and Outsider*. The insider is a legitimate user who shares the common secret and obeys the same rules to communicate with other members in the network. Usually, the insider possesses a public key certificate obtained from the Certificate Authority (CA). The outside does not own such keys as other members belonging to the network and is considered by the network members as an intruder. For example, any wireless-enabled device that runs over a rogue version of the vehicular communication protocol can make a threat to the networks, such as cell phones providing the Wi-Fi connections. It is important to distinguish such devices (outsiders) from the legitimate vehicles (insiders) in the networks.

*Active and Passive.* A passive attacker usually eavesdrops on the wireless channel to extract information from those messages. It learns information about system and causes information release. Another type of passive attack is called traffic analysis by which the intruder can observe the message flow but he/she may not understand the information. More general, a passive attacker observes the network nodes but cannot affect or change the network nodes' behavior. Howerver, an active attacker can control and affect the operation of the netwoks by inserting or modifying the information in the

data flow. It causes not only information release but also information change. Comapred with a passive attacker, an active attacker has stronger capability to attack the network and brings more serious problems to networks. A passive attacker must be an outsider because an insider can definitely affect the operation of the networks. In contrast, an active attacker can be an insider or an outsider as well. An outside attacker cannot generate and inject messages as a legitimate node, but it can still pretend to be so such that it looks like a part of the communication environment. Therefore, an outside attacker could be an active attacker.

*Malicious and selfish.* A malicious node does not try to obtain any benefit from the network but just aims to make the bad affection on the functionality of the network. For example, it can just send a lot of junk messages to consume the bandwidth of the network. However, a selfish user tries to seek personal profit. It will not waste its resource to make any action without any benefit for itself. Therefore, the affection that a selfish node makes to the network is much less than a malicious node. Both he malicious and selfish nodes can be either outsiders or insiders, but they must be the active attackers.

### 2.1.2 Attack models

There are several attacks in VANETs we define here:

*Bogus messages:* An attacker may send the fake messages into the network to affect the other vehicles' behavior. For example, the attacker may tell others that there is traffic jam ahead, which causes other vehicles to change their route and free the way for itself. In this case, the attacker can be an insider or outsider. When it is an insider of the network, the content of the message it generates is fake. When it is an outsider of the network, the message itself is not authorized.

*Masquerading attack:* An attacker may pretend to be others to send bogus messages into the network. In this case, the attacker does not want others to know the sender of the message, and he/she uses false identity to fool others.

*Replay attack:* An attacker may replay messages he/she received from others to disturb the traffic. In this case, the message is not changed and message identity is correct but the message is invalid already.

*Location tracking attack:* A global attacker may observe and collect the messages in a certain region which include vehicles' identity, location and speed information. Based on these identifiable and locatable broadcasts, an attacker can link them together and track the movement of a vehicle through information analysis. This presents potential threats to the location privacy of the users in VANETs.

*Denial of Service (DOS) attack:* An attacker may send a lot of irrelevant messages and try to consume all the bandwidth of the channel and bring down the VANET. It can cause significant destroy to the network, all the normal traffic information is blocked and the vehicles cannot communicate with each other.

### 2.1.3 Security requirement

Because of the above attacks existing in the VANETs, a secure system should meet the following requirements:

*Message integrity:* The messages sent to the network should be protected from any alteration. The most popular method for achieving data integrity is to use hash function, which generates a digest value of the input data. Once the input data is changed, the digest value will be changed. The sender sends the message together with the hash value. When a receiver receives the message, it will

calculate the hash value using the same hash function algorithm with the message as input data and then compares this calculated hash value with the received hash value. If they are identical, it indicates that the message is unchanged. Otherwise, the message is changed.

*User authentication:* The messages should be generated by a legitimate sender. We need to authenticate the senders of the messages. Without authentication, an attacker could masquerade as a legitimate party and disturb the network. The public key certificate is usually used to authenticate the identity of the user.

*Availability:* A network should have the ability to consistently and continually provide the service even in the presence of malicious users. Some mechanism should be considered to protect the network from attackers who aim to bring down the network.

*Non-repudiation:* The message sender cannot deny the generation of a message. For example, in the case that the message sender causes a traffic accident because of the false information that he/she sends, he/she should be reliably identified by the police.

*Privacy and anonymity:* Drivers do not want to expose their private information such as their identities and locations to other users. Personal or sensitive data needs special protection or limited disclosure. This is a very general statement and a requirement against the location tracing attack. Anonymity is required for the actions of the vehicles. The level of the anonymity may be different. At least, any of the observers should not be able to tell if a vehicle performed a specific action, assuming that the vehicle performs the action. However, if the probabilities that vehicles perform the action are not equal, such a system cannot guarantee that the observer cannot analysis the actions and deduce the identity of the vehicle that performs the action. Therefore, stronger probabilistic anonymity [PGH2006] requirements would be necessary in some situations: vehicles should have performed an action with the same probability as other vehicles as far as an observer is concerned. Otherwise, the

observer can still tell the identity of the vehicle that has more probability to do the action. The highest anonymity level is full anonymity, that is, any action has been performed by a vehicle could have been performed by any other vehicle in the system as far as the observer is concerned.

### 2.1.4 Related work

To solve the privacy and anonymity problems, Raya and Hubaux suggested a security and privacy scheme based on digital signatures under the PKI in [RH2005, RH2007]. Each message is sent out with the digital signature and the corresponding certificate. Vehicles are preloaded with a large number of public and private key pairs together with the corresponding anonymous certificates. When a vehicle communications with others, it randomly selects one pair of them at a time to sign each message in order to meet the driver's privacy requirement. To avoid being tracked, a vehicle should change its anonymous key after having used it for several minutes. The Vehicle Safety Communications (VSC) project group, organized by the Department of Transportation in the United States, evaluated the feasibility by using the DSRC standard [DoT2006] including the security aspect. In [DoT_AppendixH], the DSRC standard also proposes to use a list of short-lived anonymous certificates to preserve the privacy of drivers and the certificates are discarded after a short lifetime. All these public and private key pairs are stored in the certification authority (CA). In case that the real identity need to be found such as someone sends a fake message and causes an accident, the CA is able to find the real identity of the message generator. A vehicle's privacy is clearly protected from exposing to others except for the CA in this system. However, one disadvantage of using short lifetime certification is that they need a big storage size in each vehicle because of the large number of certifications. In [RH2007], there are 43,800 certificates required per year assuming that an average driver uses his car 2 hours per day, which amounts to around 4.2Mbytes (assuming a storage space of 100 bytes per key, including its certificate). Furthermore, the CA needs to keep the records

of all pseudo IDs and their corresponding certificates for every vehicle in order that it can find the real identity of a message's generator in necessary situations. The large number of certificate at CA is not only inconvenient for the CA to find a real identity of a vehicle but also difficult to manage. Another disadvantage is that it is possible for a vehicle to make a Sybil attack [D2002] with a lot of legitimate identities in hand. For example, in the congestion avoidance scheme, one vehicle could claim to be hundreds using these preloaded identities in order to create the illusion of a congested road. In addition to the above weakness, the movement tracking attack could be generated in these schemes.

To overcome the Sybil attack, a dynamic key distribution scheme is introduced in [PP2005], in which vehicles could create a new anonymous certificate any time when it needs to change its pseudo identity. The vehicle does not preload a list of the key pairs. Instead, it has a permanent public and private key pair and a certificate issued by its manufacturer. To create an anonymous identity, the vehicle generates a new public and private key pair and then sends a request signed by his/her permanent key pair asking for a new anonymous certificate for the new public key to a Certificate Authority (CA). The CA knows all the manufactures and can verify the signature on the message and issues a limited-lifetime certificate for the temporary public key. Thus, each vehicle only has one valid public key pair every time to avoid Sybil attack. The disadvantage of this method includes the need for the communication with the online CA. It has to maintain the Internet connection with the CA. The communication overhead in this method is increased as well.

Movement tracking attack can be performed in above schemes. A malicious global observer can track the movement path of a vehicle even if the vehicle changes its identity information frequently. This is because that each public key has a life time of several minutes [RH2007] and different vehicles update their public keys asynchronously. At a specific time *t*, if only one vehicle changes its public key, then it is easy to find that the vehicle using the new identity after time t is still the same

vehicle that uses an old identity before time *t*. Thus, the link between the new public key and old public key is built up and the observer can correlate the locations before and after each identifier updates. Upon a long time period, the observer can trace the whole movement path of a vehicle even if it does not know the real identity of the vehicle. The location privacy is violated. To cope with this location privacy problem, Freudiger et al. in [FRF2007] propose a concept called Mix-Zone. The Mix-Zone is the area in the transmission range of an RSU. Within the Mix-Zone area, all the vehicles share a common secret key initiated by the RSU and all traffic messages are encrypted by this shared secret key. Only the insiders who have the secret key can read the messages. Public keys are used when vehicles go out of the mixed zone. Thus, the Mix-Zone area is invisible to the malicious observer. Once the vehicles enter the Mix-Zone area, the malicious observer loses the trace of the vehicle. The location information is therefore protected. Li et al. in [LSHP2006] also proposes two schemes called “Swing and Swap” to protect the location privacy. They aim to address the location privacy challenges due to the predictability of the movements of the vehicles. Swing enables the vehicles to loosely synchronize their identifiers updates when changing their direction and speed. Swap is an extension of Swing, which enables the vehicles to exchange their identifiers to potentially maximize the location privacy provided by each update.

Another approach to provide the anonymity is to use group signature. Guo et al. in [GBW2007] developed a group signature based scheme. In a group signature scheme, all the members in a group share the same group identity and public key but have different private keys. When a member in the group wants to send a message, it uses his/her own private key to sign the message but gives out the same public key certificate. When a signed message is received by the other member in the same group, the receiver verifies the message using the group public key. If the message is valid, the receiver knows that it must be generated by a legitimate member in the group but cannot identify who is the exactly person sending this message. In case that the real identity needs to be found, the group

manager is able to reveal the unique identity of the signature's originator. By using group signature, the amount of the public and private key pairs is large reduced. The disadvantage of group signature is that the verification time is longer than the conventional PKI based scheme. Therefore, it is not suitable to be used in a high traffic density area. Sha et al. in [SXSSZ2006] proposed another adaptive group-based signature scheme in which the privacy is a user-specific. It allows users to select the degrees of privacy that they wish to have in order to achieve better tradeoff between the privacy degree and computation and communication overheads. In this scheme, each group has a set of public keys. With this set of public keys, the whole group are organized and stored as an ordered list. Inside each group, different subgroups are divided and organized into a complete binary tree over the ordered list. Each member can choose its privacy degree by set the depth of the ID-tree. For example, if the vehicle wants the maximum privacy, it can set the value of ID-tree as the root of the group key tree. If the user does not care about its privacy, he can set the value of ID-tree as his own ID. This adaptive privacy satisfies the different user's privacy requirements and achieves a balance between privacy protection and resource usage.

In vehicular networks, many vehicles in the same area may generate the messages with the same content. For example, all the vehicles involved in a traffic jam will broadcast the same event to others. If the vehicle forwards this entire message to the next hop, the network resource is wasted to provide the same information. To achieve better communication efficiency but not sacrificing security, in [RAH2006], the authors present a set of mechanisms using secure aggregation techniques. Three major classes of aggregation techniques are introduced in this paper: combined signatures, overlapping groups and dynamic group key creation. By grouping the same messages together with different users' signatures, it provides the receiver with more evidence concerning a same event. The false message will be discarded because most of the vehicles are honest and send out the same correct message related to one same event. For the same event, if there is one person reporting the different

situation while others in the same region reporting the same information, then this message must be detected as fake message. The message reliability is greatly increased. They also achieve better efficiency in term of the message overhead because only one message is sent out instead of sending out multiple messages with the same content. One problem in these methods is how they define the groups. In their design, the cells are geographically defined. When vehicles are located in a predefined cell, they are considered as one group. The vehicle closest to the centre of the cell is automatically chosen as the group leader of the vehicles in the cell, which aggregates messages for the whole group and relays them to the next leader of the neighbor groups. However, the vehicle is moving in high speed, which leads to the frequent update of the group leader of a cell. It means the methods need to be improved to be used in practical applications.

Authentication is another critical problem in VANETs. Digital signature is usually used to authorize the user. However, the verification of digital signature takes time. In case of high density traffic area, one vehicle will receive a lot of messages per second. According to DSRC, each vehicle broadcasts its own message every 100ms-300ms. If there is 200 neighbors in the communication range of a user, it will need to verify 667-2000 messages per second. It is impossible for a vehicle to verify so many messages in a second. Thus, fast verification is needed to solve the scalability issue. In [ZLLH2008], Zhang et al. developed a fast verification approach with the help of roadside unit. When a vehicle enters into an RSU's transmission range, the RSU assigns a unique shared symmetric key and a pseudo identity to this vehicle. The vehicle generates a symmetric MAC code using this symmetric key, and then broadcasts each message by signing the message with the symmetric MAC code instead of a PKI-based private key. The other vehicles receiving the messages signed with the MAC code will calculate the hash values of the messages and then buffer these messages together with their hash value for a short time interval *T*. During this time interval *T*, the RSU is able to verify the messages signed by the MAC code because it shares the symmetric key with the vehicle. The

symmetric MAC code verification is much faster compared to the PKI based signature. After RSU verifies all the messages received in the time interval, it will generate a hash value for each message and then sends them together to other vehicles with its own signature signed by its private key. Each vehicle receiving this aggregated message will only need to verify the signature of the RSU, and then compare each hash value with that it buffered before. If there is a match with the buffered one, it means this message is valid. Otherwise, it will drop the mismatched one. Both the hash computation and comparison are very fast. In short, this scheme let an RSU to verify the authenticity of a group messages using the HMAC which is much fast than the PKI based signature. After the RSU verify the grouped messages, it will notify other vehicles the authentication results. In this way, a receiver does not need to verify each message using the PKI based signature, it can verify a group of messages at one time by only verifying one digital signature signed by the RSU. Other than the less computation overhead, the communication overhead is also reduced because the message senders do not need to send out the public key certificates. Because of its less computation and communication overhead, this scheme is very efficient and can be used in the high traffic density area. The disadvantage is that it has to depend on the help of RSUs. In reality, RSUs are not located everywhere and the roads are not fully covered by the communication range of RSUs. Thus, this scheme cannot work in the area without RSUs.

There is another paper called “an efficient identity-based batch verification scheme for VANETs” introduced in [ZLLHS2008]. The scheme in this paper also implements the fast verification and solves the scalability problem but without the help of RSUs. It makes use of the bilinear pairing operations on bilinear groups [BF2001, MNT2001] to verify the signature. Basically, three pairing operations are required to verify a single signature; however, verifying $n$ signatures also takes $3$ pairing operations instead of $3n$ pairing operation with the designed verification scheme [CHP2007]. Therefore, instead of verifying one signature one by one, the receiver will verify a bunch of

signatures together. It reduces the verification delay, particularly when verifying a large number of signatures in the high traffic dense area.

## 2.2 Security in commercial applications

The safety related applications usually broadcast the messages every 100-300ms in the control channel. DSRC provides the service channels for commercial applications as well. For these commercial applications, more specific security issues should be considered expect for the general security problems appearing in the safety-related applications.

### 2.2.1 Related work

Similar to the file purchasing application, some researchers have developed application scenarios such as advertisement dissemination [LPPG2007], FleaNet [LPAG2007], and Digital Billboards [NDZPG2005]. In [LPAG2007], they propose another commercial application on vehicles: a virtual market place on vehicular networks. The customers express their demands (i.e. buy or sell an item) in the form of radio queries. The neighbors record the queries in their database. When driving along the road, they will meet new vehicles which send out their queries. Once they find a matching resource, they will forward the query's information to the vehicle with the matching resource. Thus, two parties in a transaction, a buyer and a seller are found and a virtual market can be formed in vehicular networks. However, in this paper, they do not talk about the security issues in this application. In [NDZPG2005] and [LPPG2007], the authors make use of VANETs to disseminate the advertisement. The former investigate the feasibility of targeted dissemination of ad content in a vehicular network. The studies in the latter give a research on the secure dissemination of commercial advertisements.

We may notice that the above applications have to depend on the cooperation of the vehicles. In safety related applications, vehicles send out and forward the messages in order to maintain public

safety without incentives because everybody benefits from the public safety environment. However, in commercial applications, the vehicles may get nothing for cooperation on forwarding information. Therefore, a well developed incentive mechanism to stimulate the nodes has to be guaranteed for these applications.

A secure incentive framework is developed in [LPPG2007]. In this application, an ad provider sends out their commercial ads via V2R communication and the receiving vehicles forward these ads to their neighbors via V2V communication while moving. Since the vehicles are always moving from place to place, the ads dissemination system is very efficient. This system makes use of the fast mobility characteristic of VANETs to achieve a new application. In this new application, the vehicles cooperate to disseminate those ads. A secure incentive framework called Signature-seeking Drive (SSD) by utilizing a PKI is proposed to provide secure incentives for cooperative nodes. SSD employs the notion of *virtual cash* to reward the provision of advertising services. A vehicle who forwards the ads tries to obtain receipts from its neighbors who receive those ads. With these receipts, both the vehicle and its neighbors can exchange those collected receipts with *virtual cash* from virtual cashier (e.g. gas stations). Later, the ad–providing company will pay the cost back to virtual cashier for *virtual cash* induced by the ad. With the virtual cash as an incentive for users in the networks, the cooperation among users is well stimulated.

Micropayment system is another common approach to provide incentive. Zhang et al. proposed UPASS as a secure authentication and billing architecture for wireless mesh networks in [ZF2007]. A lightweight real-time micropayment protocol is used in this paper to stimulate the cooperation between the intermediate nodes. In this system, a mobile user may access the network either by a one-hop wireless link to a nearby mesh router or multi-hop access through intermediate users to a distant mesh router. The mobile user should not only pay the network operator for providing network access but also pay intermediate users for cooperation in forwarding its traffic to and from the mesh router.

There are brokers, users and operators relationship existing in this system. Each user has a universal pass authorized by a broker to make payments to the intermediate users who help to forward the packets and the operator who provides the network service. Each user will make a micropayment which is worth m-units once it transmits n bytes in the networks. The receiver who receives the payments can redeem them from the brokers. Such a scheme ensures incontestable billing in the networks.

In our file purchasing application, we will use micropayment scheme to stimulate the neighbors to transmit the files to the user.

## 2.3 Preliminaries

Before the proposed security framework for the file purchasing is presented, several important preliminaries: micropayments, one-way hash chain and digital fingerprints are introduced in the following subsections.

### 2.3.1 Micropayments

Micropayments are electronic payments of a small amount. There are two important requirements for micropayments: (1) utmost security is not required, and (2) the payment mechanism must be lightweight. Otherwise, the cost of using the scheme will outweigh the value of the payment. It is similar to using the vending machines in real-world. Because the goods sold in the vending machine are usually low-cost, it is not worth to hire people to sell the goods. Therefore, the goods inside the vending machine may be stolen, or clients may receive low-quality goods. Both the profit of the seller and buyer are not guaranteed. And from other point of view, it does not worth people to open the vending machine to steal the low-cost goods because the effort took to open the machine may cost more than the cost of goods. The owner of the vending machine usually does not make low-quality

goods to cheat customs in case they want to do a long term business. Similarly, micropayment schemes do not guarantee fair exchange of goods and payment.

In micropayment system, offline payments are preferred from a practical standpoint because they have lower latency, communication costs and computation costs. Therefore, the coin fraud may not be found immediately. On the other hand, large-scale fraud needs to be detected and punished. Therefore, effective micropayments systems simply need "good enough" security where fraud is detectable, traceable and unprofitable, and at the same time maintaining high efficiency.

### 2.3.2 One-way hash chain

One-way hash chain is a widely-used cryptographic primitive. It is a method to produce many one-time keys from a single key or password, also called seed. One of the first uses of one-way chains was for one-time passwords used in an insecure environment by Lamport [L1981]. Haller later used the same approach for the S/KEY one-time password system [H1994]. One-way hash chains are also used in many other applications such as secure data forwarding in wireless ad hoc networks [HAKL2005], stream data authentication [GM2001], etc.

Because One-way hash chains are very fast algorithms that produce very low overhead, they have been adopted previously to make micropayment [ZL1998, TO2003, and RS1996].

Figure 2.1 shows how to generate the one-way hash chain. Firstly, we randomly pick one number called seed *S* and make it as the last element of the hash chain. Then we generate the chain by repeatedly applying a one-way hash function *H (.)*. Thus, we get a hash chain donoted as $h_0, h_1, ..., h_n$, where $h_0 = H(h_1)$, $h_{i-1} = H(h_i)$, $h_n = S$. The first element $h_0$ is called a *commitment* to the entire one-way hash chain, and we can verify any element $h_i$ of the chain through $h_0$ by checking that $H^i(h_i) = h_0$.

More generally, if we know that $h_i$ is the ith element of the chain, to verify that $h_j$ is an element of the chain, we check that $H^{(j-i)}(h_j) = h_i$ , where $i < j$ .

The hash function *H(.)* is described as one-way because it has an important property that given a number *x*, it is easy to compute the hash value *H(x)* but given the hash value *H(x)* , it is computational hard to compute the number *x*, therefore, when given $h_j$ , it is easy to compute $H^{(j-i)}(h_j)$ in order to verify if $h_j$ is part of the chain but it is difficult to get $h_j$ when given $h_i$ *(assuming* $H^{(j-i)}(h_j) = h_i$*)*. Thus, the sender reveals the chain elements in the opposite order of the generation: first $h_0$, then $h_1$,..., then $h_n$ when using the hash chain. The first element $h_0$ is usually signed using a standard signature scheme such as a private key. The receiver verifies the first element $h_0$ using the sender's public key. However, the following revealed element $h_i$ can be verified easily by the previous revealed elements such that the verification is much faster than the verification using private key. If the following revealed element $h_i$ is verified as a part of the chain, that means $h_i$ comes from the same sender as the first element $h_0$ because no one else can generate $h_i$ even with the knowledge of $h_0$ due to the one-way property.

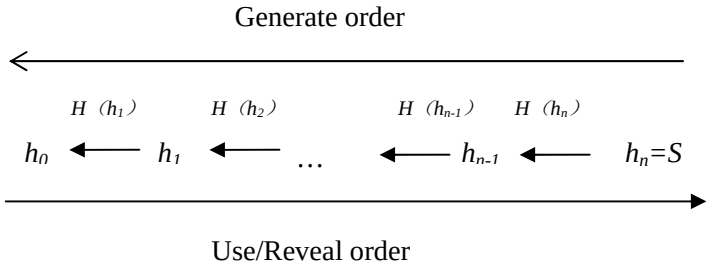


**Figure 2-1: Hash Chain**

### 2.3.3 Digital fingerprints

To protect digital rights in commercial operations, it is extremely important to ensure that digital content is used for its intended purpose. For example, the digital content should be only used by the legitimate users who have paid for the service. Cryptographic encryption can be used to disseminate the data to users and implement access control and confidentiality protection, but the protection usually terminates once the content is delivered to the user and decrypted by the user. Usually, it is not possible to prevent the user from redistributing the copy after delivery, thus some solutions must be developed for tracking and identifying those involved in unauthorized redistribution of digital content. The urgent need to address post-delivery protections should be noticed.

Digital Fingerprinting is an emerging technology to protect digital content from unauthorized redistribution after delivery. It embeds a unique identity called digital fingerprints into each user's copy before distribution, which can be extracted to help identify culprits who unauthorized disseminates the information and causes an unauthorized leak. In order to protect digital content, it is essential that the fingerprints are difficult to be removed. Some digital fingerprinting techonologies can be found in the [WTWL2004, and WWZTL2005].

# Chapter 3

# A Secure Business Framework for File Purchasing in VANETs

## 3.1 Overview of the file purchasing application

The file purchasing application is in the paradigm of e-commerce applications, where the buyer is a vehicle[1], while the seller is an RSU with large storage size and strong computation ability. The RSU works as an access point that provides Internet connection. Many resources can be obtained at a vehicle from an RSU locally or from the public Internet by way of an RSU. For example, when a vehicle arrives at a new city, it is very convenient for this vehicle to buy the latest version of the local map from the RSUs located at the main entrances of the city.

Since RSUs are only located at some important locations such as the intersection of streets, the main entrance of a city, and some high traffic density area, it is not likely that the RSUs can fully cover the whole city. When a vehicle requests to purchase a file from an RSU, it electronically pays the RSU and then starts to download the file from the RSU. However, due to the high mobility of vehicles in VANETs, the contact period between the RSU and the vehicle could be too short to download the complete file. One of the novel devices in the proposed application is that the vehicle does not need to stop and wait for the completion of file downloading. The file acquisition process can be performed through V2V communications with the vehicles that contain one or multiple pieces of the file. To effectively and securely achieve such V2V cooperation, the vehicle (i.e., the file buyer) first acquires a permission to use this file from the RSU, and then takes advantage of V2V communications to transmit the file. In particular, the vehicle out of the RSU communication range can still acquire some pieces of the file from its neighbors that are necessary to compose the whole

file. After getting the permission from the RSU and collecting all the pieces of the file, the vehicle can open to use the file.

To put this application into practice, a number of security issues have to be considered. Firstly, the file content must be protected from unauthorized uses because a digital file can be easily copied and instantaneously distributed everywhere. Secondly, some selfish neighbors may not like to transmit the file to the vehicle without any incentive. Forthrightly, even for the naive users, they may not help transmitting the file for the benefit of the business companies. Thus, we have to find a proper incentive mechanism to stimulate the cooperation among the neighbors. Finally, the authentication and the protection of the drivers' privacy in VANETs are critical factors for putting the applications into practice.

With these security concerns and selfish nature among vehicles in mind, to implement such an application in reality, we develop a secure framework that can support the novel application scenario of commercial file purchasing through V2R and V2V communications in VANETs. Public Key Infrastructure (PKI) is taken in this study for ensuring authentication and privacy in V2V communications, which is considered as a suitable approach to meet the corresponding security requirements [RH2005]. In the aspect of the incentive mechanisms for V2V cooperation, a micropayment is devised to stimulate the neighbors of a buyer to transmit files. For the copyright protection of the digital file, we make use of the tamper-proof device to prevent the user from getting the authorized copies. The digital fingerprint technology is adopted in this study to perform the tractor tracing for identifying any unauthorized distributor.

### 3.1.1 Network model

[1] In the following paper, we use the terms "buyer", "user" and "vehicle" interchangeably.

Our vehicular network is in a two-layer architecture shown in Figure 3-1. This network model is capable of supporting different applications such as safety message dissemination, traffic control, infotainment, and payment services.

In the layered network architecture, the upper layer is composed of RSUs, application servers (ASs) and brokers, which are connected to the Internet through either wired or wireless connection. RSUs, ASs, and brokers can communicate through secure channels, such as using Transport Layer Security (TLS) protocol. Brokers are responsible to issue a payment certificate to each user (vehicle), with which vehicles can make payments and enjoy shopping on VANETs. Application servers provide data to RSUs, and RSUs deliver the demanded data to the lower layer.

The lower layer of the network model is composed of RSUs and Vehicles. RSUs work as gateways between two layers. RSUs are located at several important points and their transmission range cannot fully cover the whole road. Each vehicle can communicate with other nearby vehicles or with an RSU using the Dedicated Short Range Communications (DSRC) protocol. Each vehicle has its own public/private key pairs issued by the Certificate Authority (CA). Each message is sent out with the sender's signature and its certificate (public key). The receivers verify each message using the sender's public key.

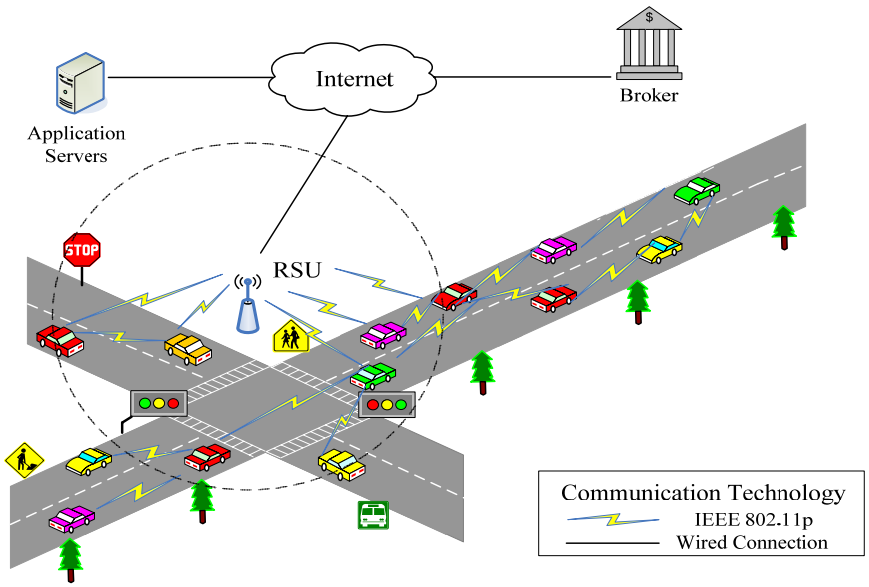


**Figure 3-1: Network Model**

In this thesis, we focus on the secure issues in the V2V and V2R communications along with the file purchasing process between vehicles and RSUs. The notations taken throughout this thesis are listed in Table 3-1.

| Notations | Descriptions |
|---|---|
| OBU | On Board Unit |
| RSU | Road Side Unit |
| $U$ | Vehicle (Buyer) |
| $B$ | Broker |
| $R$ | RSU |

| | |
|---|---|
| $C_i$ | *i's* Certificate |
| $PK_i$ | *i's* Public Key |
| $SK_i$ | *i's* Secret Key |
| $PID_i$ | *i's* pseudo ID |
| $\{M\}_{SKi}$ | *i's* digital signature on M |
| $P_U$ | The permission that U buys from RSU |
| $C_U$ | *i's* Payment certificate |
| $H(.)$ | Hash function |
| $D$ | The amount of money |
| $E$ | Expiration time |
| $I_U$ | Extra information |
| $FID$ | File identity |
| $T$ | Current time stamp |

**Table 3-1: Notations**

### 3.1.2 User-broker-seller relationship model

From the commercial point of view, there are three parties involved in the file purchasing application: broker, user and seller. The broker issues universal payment certifications to the user, which authorizes it to make payments to the seller. The broker can also redeem the collected payments for the seller.

The relationship among the user, the seller and the broker is just like what happens in real life. A user first applies for a credit card with a bank. Upon receiving the credit card, it can purchase goods

from any supermarket which accepts credit cards. The supermarkets do not need to have any relationship with each other, but need to build a trust relationship with the bank which redeems the users' payments. The bank is also trusted by users. But the user and the supermarkets do not fully trust each other. In our VANET application, if we treat the payment certificate as a credit card, the payment certificate holder (user) is the credit card holder. This analogy motivates us to adopt the sophisticated credit card-based business model as our payment design. In the file purchasing application, the vehicle *U* is acted as the user, the seller is the RSU *R*. The relationship between a user *U*, an RSU *R* and a broker *B* is analogous to that between a credit card user, a supermarket and the bank.

### 3.1.3 Payment certificate model

To make a payment, firstly, the vehicle $U$ needs to establish an account with a broker, in which the vehicle has to provide his/her personal confidential such as his/her driver license and Vehicle Identification Number (VIN). It also chooses some pseudo identities $PID_U$ to use in the future payment. The broker builds a record for each vehicle to save its real identity and the corresponding pseudo identities. Since the broker is fully trusted, it is responsible for keeping all the users' data secret. Depending on the registration policies and the vehicle's credit status, the broker may ask for a security deposit from the vehicle, which is just like a security credit card in real life. After the registration, the broker issues the vehicle *U* a digitally-signed *payment certificate* which has the following form:

$$PC_U = ID_B, PID_U, E, I_U, \{B, PID_U, E, I_U\}_{SK_B}. \quad (1)$$

The payment certificate contains the broker's identity $ID_B$, the vehicle's pseudo identity $PID_U$, the expiration date $E$ and some other extra information $I_U$ such as the maximum amount the user can

spend one day. Note that the pseudo identity $PID_U$ in this payment certificate should be the same with the one in its certificate $C_U$ issued by CA. Also, this payment certificate has to be renewed by the broker $B$ (e.g. monthly) before the expiry data. The broker will perform the renewal if the corresponding vehicle keeps its account in a good record. Otherwise, the vehicle will not get its new certificate from the broker. It is just like the credit card and you have to pay your bills of your credit card every month.

### 3.1.4 Tamper-proof secure module

We assume that each vehicle is equipped with a tamper-proof secure module including the built-in hardware and firmware. Each tamper-proof device has a unique identifier that can be used to uniquely identify and address each vehicle. There are two types of functionality for a tamper-proof module: cryptographic operations and storage. Some secret material such as keys is stored in the tamper-proof module. The cryptographic operations such as the encryption or decryption are implemented by it. The stored information and operation functionalities of the tamper-proof secure module can only be modified by the trusted authorization. For a user, the tamper-proof works just like a black box which only provide the input and output interface to a user. A user may be able to modify both the input and the output data of the tamper-proof module, but never to access and modify any information stored inside it and any functionality it has. With this tamper-proof module, the vehicle's cryptographic material is protected inside the storage and the operations of the data are guaranteed. In real world, this secure module can be part of the medium access control (MAC) or an independent smart card such as the SIM cards in GSM cell phones [ZLLF2007].

## 3.2 The proposed secure transaction protocol

We divide the whole file purchase implementation into three procedures: *permission purchasing*, *file*

*collecting* and *file reading*. The first communication procedure is between a vehicle *U* (buyer) and an RSU. The vehicle *U* sends out a requirement to buy permission from an RSU and then makes a payment to the RSU. After the RSU verifies the payment, it sends out the permission back to the vehicle *U*. The second procedure is done between the vehicle *U* and its neighbors. The vehicle collects all the pieces of the file from its neighbors during the second procedure. Finally, in the third procedure, the vehicle *U* uses the permission it obtained in the first procedure to open the file that was got from the second procedure. We focus on addressing security issues in each procedure due to their different requirements. These three procedures are discussed in details in the following subsections.

### 3.2.1 Permission purchasing

In this procedure, we focus on the communications that are between an RSU and a vehicle. When a vehicle *U* enters the transmission range of an RSU, it will send a message to the RSU to ask for the file *F* that the vehicle *U* is interested in. In order to protect privacy, the vehicle *U* uses its pseudo identity $PID_U$. After the RSU receives this requirement, it will send a message back containing the price of this file. The vehicle *U* will reply with the payment commitment which includes the amount of the money *D*, its payment certificate $PC_U$, time stamp *T* and the expiration date *E*. Next, the RSU verifies the *U's* signature on the message and the broker's signature on *U's* payment certificate. If the verification passes, the RSU sends a message back which is the *permission* to use the file. The whole procedure is as follows:

$$U \rightarrow R : FID, \{FID\}_{SK_U}, C_U \tag{2}$$

$$R \rightarrow U : D, \{D\}_{SK_R}, C_R \tag{3}$$

$$U \rightarrow R : ID_R, PC_U, D, T, E, \{R, PC_U, D, T, E\}_{SK_U} \tag{4}$$

$$R \rightarrow U : PID_U, H(F), \{PID_U, H(F)\}_{SK_R} \tag{5}$$

The last message which the RSU sends to the buyer actually includes the permission for using the

file. We denote the permission:

$$P_U = PID_U, H(F), \{PID_U, H(F)\}_{SK_R}. \quad (6)$$

If a user wants to use the file, he/she has to pay the RSU to get the permission. Without the permission, the buyer cannot use the file even if it obtains the file from others. This is because the file is encrypted. Only when the user has the permission, the file can be decrypted and used. We will describe how this works in the following subsections. In this procedure, four messages are exchanged. According to DSRC, the transmission range of an RSU is up to 1km. The range can provide enough time for a vehicle and an RSU to exchange the above four messages. In addition to these four messages, the RSU can transfer a part of the file to the user *U*. Once the user *U* is out of the range of the RSU, the left part of the file is transmitted by other vehicles.

### 3.2.2 File collecting

Suppose that a vehicle is on the road at the speed of 60 km/hr (17m/s). The RSU transmission range is 1km. In this case, the vehicle can stay in the transmission range of the RSU at most 2 minutes, which is not long enough to download a large file such as some videos. However, each vehicle in VANETs has a lot of neighbors. If some neighbors have already purchased the file, they can share the file content with the file buyer using cooperation communication such as P2P technology. Since the file is a commercial product, it is encrypted by the service provider (application server) and then delivered to a buyer over wireless channels. The buyer will decrypt it with the permission after collecting the complete encrypted file. The buyer that owns the decrypted file should not send it to others.

**Key agreement***:* The communications between a buyer (denoted by *U*) and its neighbors (denoted by *V*) should be encrypted. Otherwise, other users in the middle can also receive the file content. Therefore, the buyer *U* and its neighbor *V* need to build a shared secret key. The shared secret key can be achieved using Diffie-Hellman key agreement protocol, which is shown as follows:

$$U \rightarrow V : g^a, C_U \tag{7}$$

$$V \rightarrow U : g^b, \{PID_U \parallel g^a \| g^b\}_{SK_V}, C_V \tag{8}$$

$$U \rightarrow V : g^b, \{PID_V \parallel g^b\}_{SK_U}. \tag{9}$$

The shared key between the vehicle $U$ and its neighbor $V$ is $K_{UV} = g^{ab}$. When $V$ receives the first message, it verifies *U's* public key $PK_U$ using *U's* certificate and then verifies *U's* signature on $g^a$ using the public key $PK_U$. For the message which *V* sends to *U*, *U* also verify the signature on it. In this way, both *U* and *V* authenticate each other and build up the shared session key between them. They will use this secret shared key to transmit the pieces of the file during the communications.

**Incentive protocol:** The file is divided into many pieces. Each vehicle sends some pieces of the encrypted file to the buyer through V2V communications. Because nobody likes to send the file for free, we have to provide an incentive protocol to stimulate each file sender. We adopt micropayment technology based on payword [RS1996] as a solution to this problem.

The micropayment approach is a combination of PKI and one-way hash chain techniques. We define an important data structure called a payword chain used in the billing process. The payword chain is actually a hash chain generated by hash function such as SHA-1 [24]. Each payword is a hash value included in the hash chain. The hash chain is generated as follows. The vehicle first picks a random number $w_n$, and then recursively computing

$$w_i = H(w_{i+1}) \tag{10}$$

for $i = n-1, n-2, ..., 0$. Due to the one-way feature of the hash function, given $w_{i-1}$ it is computationally infeasible to find $w_i$, while given $w_i$, it is very efficient to compute $w_{i-1}$. Here the

first value $w_0$ is not used to make a payment but used as the root of the chain to verify the payment chain. The following hash value $w_1, w_2, \ldots, w_n$ are used as paywords to make payments.

Together with the payment certificate, the vehicle *U* uses the payword chain to pay the file provider *V* . Thus, *V* believes that the payment from *U* is redeemable by the broker. The vehicle *U* pays one payword to *V* when the vehicle *U* receives one piece of the file from *V*. We can assume that each payword is worth one cent and the size of one piece of the file is 1KB.

Before the vehicle *U* buys pieces of a file from *V*, the vehicle *U* sends his/her first message called *commitment* (denoted by M) for the payword chain to *V*, which has the following form:

$$M = PID_V, PC_U, w_0, E, T, \{PID_V, PC_U, w_0, E, T\}_{SK_U}, \quad (11)$$

where $PID_V$ is the pseudo identity of *V*, $PC_U$ is the payment certificate of the buyer *U*, $w_0$ is the root of the payword, *E* is the expiration date(such as the current day) . $T$ represents the current time stamp. This commitment authorizes the broker $B$ to redeem *V* the paywords that *V* gets from the buyer *U* before the date $E$ .

After receiving this commitment, the vehicle *V* begins to send the pieces of the file to *U*. A payment is made from *U* to *V* when *U* receives a piece of the file from *U*. The payment is consisted of a payword and its index: $P = \{w_i, i\}$ . *U* spends its paywords in order: $w_1$ first, $w_2$ second, and so on. When *V* receives $w_1$ , it can verify $w_1$ using $w_0$ by checking if $w_0 = H(w_1)$ . If the verification fails, the file provider *V* can stop transmitting more pieces of the file to the buyer *U*. The following paywords are verified in the similar way. Once receiving a new payword $w_i$ , *V* will verify it using the previous payword $w_{i-1}$ by checking if $w_{i-1} = H(w_i)$ . Therefore, the file provider *V* needs to save only the last payment which has the highest index. The broker can decide the value to be paid by determining how

many times to apply the hash function $H(.)$ to map the hash value with the highest index into the payword root $w_0$.

We can conclude the above procedure as follows:

$$U \rightarrow V : E_{K_{UV}}\{M\} \tag{12}$$

$$V \rightarrow U : E_{K_{UV}}\{ist\ piece \| format, \{ist\ piece \| pattern\}_{SK_V}\} \tag{13}$$

$$U \rightarrow V : \{w_i, i\} \qquad (i = 1, 2, .....) \qquad . \tag{14}$$

In equation (12), *M* is the commitment which the buyer *U* sends to *V*. *V* could know that if *M* comes from the buyer *U* by reading the time stamp *T* included in *M* because *M* is encrypted by the secret symmetric key $K_{UV}$ which is only shared between *U* and *V*. If *M* does not come from *U*, the time stamp should be wrong. Thus, $V$ does not need to verify *U's* signature on *M*. The *U's* signature included in *M* is saved and used when it redeems the paywords from the broker. What $V$ needs to do is to verify the broker's signature on the payment certificate of *U* which is contained in *M* and check the expiration date. If they successfully pass the verification, *V* will send out the first piece of the file content. Each piece of the file includes the actual file content plus one "pattern" byte which has special pattern such as 11010101. This byte is used for the user authentication. If the neighbor who does not have the secret symmetric key $K_{UV}$ generates the message, then when V decrypts this message, it will not get the piece of the file content ending with this special extra byte. After receiving the first piece of the file content, *U* sends out his/her first payment including the payword and its index. After receiving the first payment, *V* verifies it using the root of the payword $w_0$. If it is correct, the procedure continues until they are out of each other's transmission range or have no more content to transmit.

The buyer *U* keeps collecting all the pieces of the file from its neighbors until it gets the complete file. In the following subsection, we discuss how the buyer will use this file after it gets the permission and the complete file.

### 3.2.3 File reading

Each vehicle is equipped with a tamper-proof device, which is securely against any compromise attempt in any environment. After a buyer obtains the whole file and the corresponding permission, the buyer can use the permission to open the file. The buyer needs to input the permission and the file into his/her tamper-proof device. The tamper-proof device is responsible to verify whether the file can be used for the buyer. If the verification passes, the tamper-proof device will generate a copy for this user. The tamper-proof device is composed of three secure modules: an authentication module, a decryption module, and a digital fingerprint generation module, which is shown in Figure 3-2.

**Authentication module***:* The authentication module is responsible for access control. Only the authorized user can precede further access to the file. The pseudo identity $PID_U$ is preloaded into the device by the authority organization. The permission $P_U$ the vehicle buys from an RSU and the certificate of the RSU are input into this module. The authentication module verifies the signature of the RSU and then compares the pseudo identity it gets from the message with the pseudo identity it saved. If they successfully pass the verification of this module, the hash value $H(F)$ included in the permission $P_U$ is saved, and then the whole collected file is inputted into the second module of the tamper-proof device. Otherwise, if the verification fails, the device will reject to continue the service for the user. Although the verification of the permission $P_U$ indicates that the user with pseudo identity $PID_U$ has bought the permission from the RSU, the verification does not verify whether this permission is dedicated for using the file with the file identity $FID$. Therefore, we have to guarantee

that this permission can be used only for this file. Otherwise, one user can only buy the permission once but use it for any file. That is the reason why we save the file hash value $H(F)$ here. We will further discuss the use of $H(F)$ in the next module.

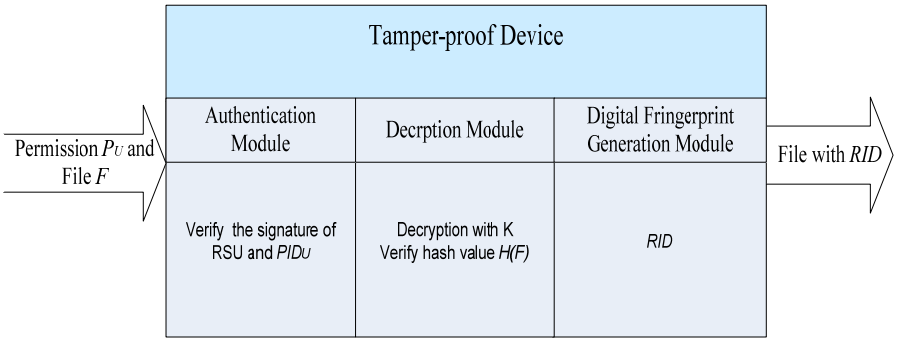


**Figure 3-2: Tamper-proof device**

**Decryption Module:** The decryption module is preloaded with the secret key, which is used to decrypt the collected file based on based on a symmetric encryption algorithm such as Data Encryption Standard (DES) algorithm. The application server encrypts the file using the same symmetric key and the same algorithm as well. After decrypting the file, the second module will calculate the hash value of the file and compare it with the saved hash value in the first module. If the two hash values are equal, that means it is the authorized user with the pseudo identity $PID_B$ who has bought the permission for the file with the identity *FID*. Then the decryption module begins to decrypt the file, and sends the decrypted file to the next digital fingerprint generation module. If the two hash values are not equal, the tamper-proof device will reject the further service.

**Digital fingerprint generation module:** After obtaining the decrypted file from the decryption module, the digital fingerprint generation module embeds a digital fingerprint into the decrypted file.

The fingerprint includes the user's real identity, which is able to uniquely identify each copy of the file for each buyer. The digital fingerprint generation module finally outputs the unique copy for the buyer. A trust authority can trace the vehicle that distributes this file to others because the unique digital fingerprint information is associated with the user. Here, designing a digital fingerprint is beyond the scope of this thesis, we can adopt the existing fingerprint technologies [BS1995, CM2000, and WTWL2004].

## 3.3 Security analysis

The security issues are discussed in terms of privacy preservation, protection of file content, and secure payment.

**Privacy:** It is an important issue in VANETs to preserve drivers' privacy. In our applications, each vehicle is giving its pseudo identity when making transactions. The vehicle can apply for multiple pseudo identities (i.e. public/private key pairs) from the broker and the pseudo identities can be changed every time when the vehicle renews its payment certificate from the broker. A vehicle uses a different pseudo identity each time it makes a purchase. Furthermore, the vehicle is not always making purchase all the time and it may do this only one or two times one day or even one time several days. A vehicle uses the same pseudo identity only for a short time and changes it when the vehicle makes the next purchase, which prevents some malicious observers from tracking its real identity of the vehicle.

**Protection of the file content:** One of the most important issue in developing the file purchasing system is the protection of the file copyright. To guarantee the profit of the content provider, we should protect the digital content from unauthorized dissemination. In this paper, RSUs take the role of file providers and vehicles can use the file only if they pay the RSUs for the file. Cryptographic encryption is a powerful tool for access control and confidentiality protection. RSUs only send out the

encrypted file to the buyers. The key for decrypting the file is preloaded by the authority organization in the tamper-proof device equipped on each vehicle. Nobody can access and change the data stored in the tamper-proof device expect for the authority organization, which prevents the key from being leaked out, such that only the user who gets the permission from the RSU can active the tamper-proof device to decrypt the file. In order to get the permission, the user has to pay the RSU. The permission includes the user's pseudo identity with the signature of the RSU. The signature is unique to each user. Thus, the permission for a specific user can only be used for the user himself/herself and is not useful for anyone else. In this way, we guarantee the permission for using the file can be only obtained from RSUs.

During the file collecting procedure, the file content is sent to the vehicle from its neighbors. Before the transmission, they build up the session key for the communication. This also helps to prevent the file content from being distributed to others who do not pay the file sender.

Once the user gets the permission and collects the complete file, it sends them into the tamper-proof device. The tamper-proof device decrypts the file content after the verification. The tamper-proof device decrypts the file content after the verification. The protection of the content usually terminates once the device output the original file because the user can still send this original file to his/her friends in the future. That means all the protection efforts before the delivery are useless. Therefore, the protection after the delivery and decryption is also important. We use the digital fingerprint technology to tackle this issue. The tamper-proof device generates the digital fingerprint for each copy of the file. It embeds the user's real identity into each user's copy such that the user can be traced if he/she distributes his/her copy to others. Therefore, the digital fingerprint stops users from disseminating their files for commercial purpose.

**Secure payment:** When the user pays an RSU, the RSU first verifies the signature of the broker included in the user's payment certificate, which indicates whether the user is a legal one or not. With the user's payment certificate and the user's signed commitment, the RSU can get paid by the broker. The signed commitment includes the RSU's name and the amount of the money. The user's bank payment certificate is credit-based and the user pays his/her broker periodically. Anyone who does not pay the bills cannot get the new payment certificate and can be sued by the law. Furthermore, we can set a limit value $m$. If the amount of the payment is larger than $m$, the RSU communicates with the broker in real time. Only when the user has enough credit on the user's account, the broker authorizes this payment. Otherwise, the payment is rejected. This enhances the protection of the payment from cheating by the user. On the other hand, regarding the payment process from the RSU, we argue that the RSU has the right motivation to give the permission out honestly. The reason is that if the RSU does not give the permission out, it will lose its reputation. Since the RSU aims a long term business, its reputation is worth much more than what it can earn from the short time cheating.

In the procedure of collecting the digital file from neighbors, the micropayment approach ensures incontestable billing although the business for the neighbors is short term compared to the business for RSUs, which may lead to cheating from both the seller and buyer. The user signs a commitment before using the paywords to make payments. After receiving the commitment, the neighbor $V$ sends one piece of the file each time, and the user $U$ releases one payword each time after receiving each piece of the file. $U$ cannot get more services than $U$ actually pays. The neighbor $V$ cannot get more paid than what $V$ should earn. The cheating might only happen at the end of the service. For example, either the user $U$ does not pay the last payword to the neighbor $V$, or $V$ does not send the last piece of the file to the user $U$. We believe that the loss of either one payword or one piece of the file is quite small and should be tolerable. This is also the feature of the micropayment.

Since each payment commitment in the micropayment includes the seller's identity and a time stamp with the user's signature, it is both user-specific and seller-specific, which prevents from double-spending and double-redemption problems. In other words, the user cannot use the same payment to pay different neighbors and the neighbors cannot redeem the same payment more than once. For example, we assume the expiration time for the payments is the midnight on the current day when the payment is made. The broker keeps all the records for the payments until the midnight. Every time the broker receives a new payment for redemption, the broker checks the records and redeems only once for the same payment.

## 3.4 Performance analysis

### 3.4.1 Communication cost

The entire communication does not require the real-time involvement of the third party such as a broker. Only in some cases when the user pays an RSU, if the amount of the money is larger than *m*, the RSU may execute a real-time check with the broker. Thus, the communication is off-line from the broker's point of view. Imaging that one broker may have thousands of users, if all the users need to have the real-time communication with the broker, the broker will become a bottleneck. With offline system, the broker can verify and redeem payments at any low traffic load time such as at night. Therefore, the system is much more efficient than some online systems.

The release of paywords uses the hash function to implement. For a typical hash function such as SHA-1, the length of the hash value is 20 bytes. Plus the index of the payword, each payment is 21 bytes. This overhead is less significant compared to the traffic volume. For example, if we define one piece of the file is 10K Bytes, then a 21-byte payment is released every 10K Bytes data, which is about 0.2 percent overhead and considered very low lightweight.

The file is divided into numerous pieces with the same size. Given a file, the total overhead to transmit a complete file mainly depends on the piece size of the file. To successfully transmit one piece of the file, the sender adds one extra format byte and a signature on it, and the receiver replies one payment back. The length of the signature is 42 bytes assuming we choose ECDSA [ANSI X9.62-2005] (21 bytes) as the signature scheme. One payment is 21 bytes in length. Thus, the overhead for each piece of the file is 64 bytes. The total overhead is inversely proportional to the size of a piece. The smaller the size is, the more pieces the file is divided into and the more overhead we will get. And the other factor to affect the overhead is the size of the given file. Obviously, the overhead increases with the increase of the file size. The relationship among them is shown in Figure 6. Three curves represent three different file sizes: 5MB, 10MB, and 15MB. Each curve indicates the relationship between the total overhead and the size of a piece. We can see that 6MB is the proper piece size because the trends of the curves become flat from this point. In other words, increasing the piece size has little effect on the transmission overhead. The relationship between transmission overhead and the piece size is shown in Figure 3-3.

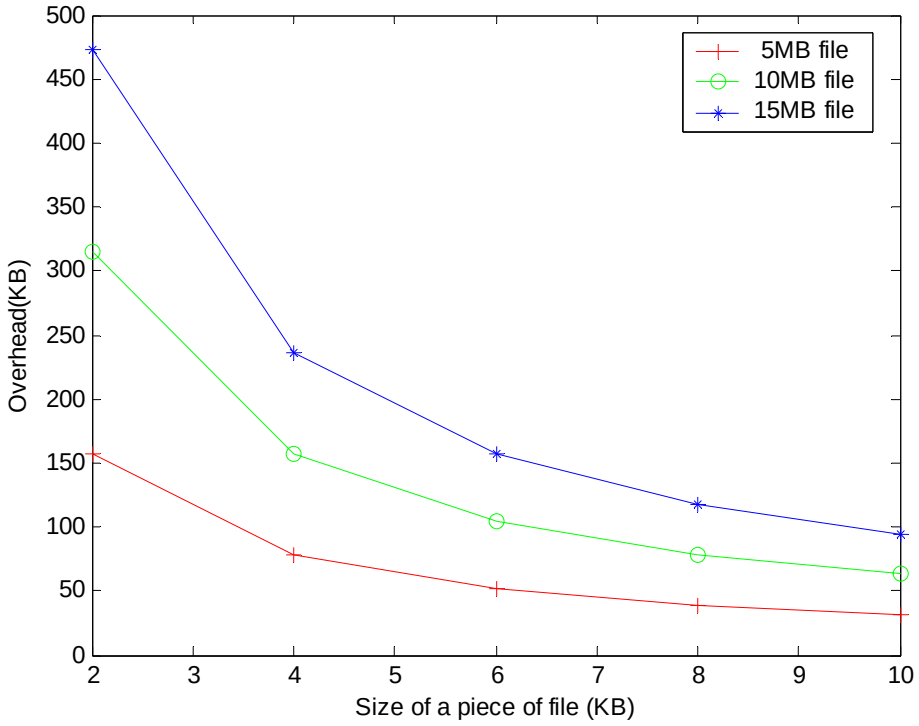


**Figure 3-3.Transmission Overhead vs Piece Size**

### 3.4.2 Computation overhead

During the first procedure, a user and an RSU need to perform a few public-key related operations, including signing and verification. We choose the Elliptic Curve Digital Signature Algorithm (ECDSA), which has fast signing and verification speed, the signing and verification time are 3.255 ms and 7.617 ms [RH2005], respectively. Moreover, the communication between an RSU and a user is transient and the messages they exchange are only 4 times. The communication is successful once the user receives the permission. Thus, the computation time between a user and an RSU is about 63.08 ms ((7.617×2+3.255) ×2 + (7.617×2+3.255) + 7.617)). Most of the time, the duration which

the vehicle stays in the transmission range of an RSU should be much longer than this computation time. This computation delay is affordable.

During the file collecting procedure, we use the symmetric key encryption to keep the data traffic confidential. The speed with a symmetric encryption is much faster than that of public-key based encryption. We may notice that neighbors also need to sign on each piece of the file, but the user does not verify it. The user could tell the message comes from the correct neighbor because they share the same shared key. The signature is only used to trace back in case that the user finds the neighbor provides wrong content. The payments that the user gives to the neighbor include only fast hash operations, except for the signature operations for the first payment commitment generation and verification.

After the user gets the permission and collects the complete file, all the computation depends on a tamper-proof device. It is rather affordable for a tamper-proof device to do a few public key operations and generate a digital fingerprint.

### 3.4.3 Delay analysis

We conducted simulations using the ns-2 simulator [NS2] to further evaluate the performance and feasibility of our file purchasing application model.

We use 802.1a to approximate the 802.11p Medium Access Control (MAC) protocol. We simulate a city environment by using the mobility model generation tool which is developed by [SJ2004] .This tool is specialized to generate realistic traffic scenario files for the ns-2 platform. We extract a street map of 1×1 $km^2$, from the US Census Bureau's TIGER (Topologically Integrated Geographic Encoding and Referencing) database which gives detailed street maps of the entire United States. The map we are using is shown below in Figure 3-4 which corresponding to the west university place area in Houston. A vehicle is first scatted randomly on some intersection of the roads and moves towards

another randomly selected intersection along the path in the map. Vehicles are driving with a random speed with fluctuation range of 5 miles/hr according to the road speed limit that ranges from 35-75 miles/hr. There are total 200 vehicles with a 250m transmission range in this area.

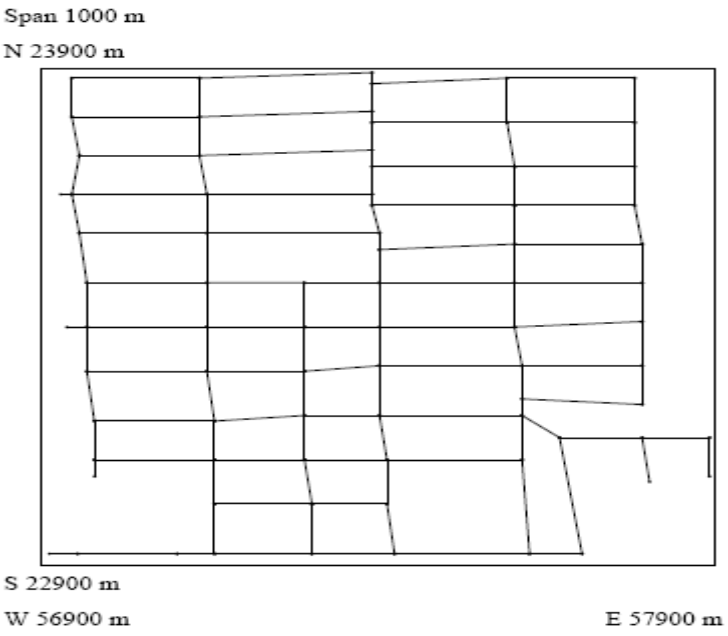


**Figure 3-4: The map used in simulation**

The file size is 5Mb/s. The file is divided into 6KB pieces. A piece is transferred using six 1KB packets. We define the download *delay* to be the elapsed time for a user to collect all the pieces of the file. We define $p$ is the *probability* that a neighbor in the network has the same file. The *interval time* refers to the elapsed time between two consecutive packets from the same neighbor.

The picture of the average download delay *vs* transmission time is shown in Figure 3-5. The picture of the average download delay *vs* probability is shown in Figure 3-6. In Figure 3-5, the three curves show the average delay under the different probabilities that the neighbors have the same file. The

smaller the probability $p$ is, the fewer neighbors transmit the file to the user. As we expect, the delay increases with the probability $p$ decreasing in the Figure 3-5. For each individual curve, we can see that when the interval time becomes longer, the delay for collecting the complete file increases. This is because the transmission rate between a user and a neighbor is conversely proportional to the time interval. When the time interval is 2s and the probability that the neighbors have the file is 0.4, it takes a vehicle about 56s to collect the complete file. This is reasonable. The similar analysis is explained in Figure 3-6.

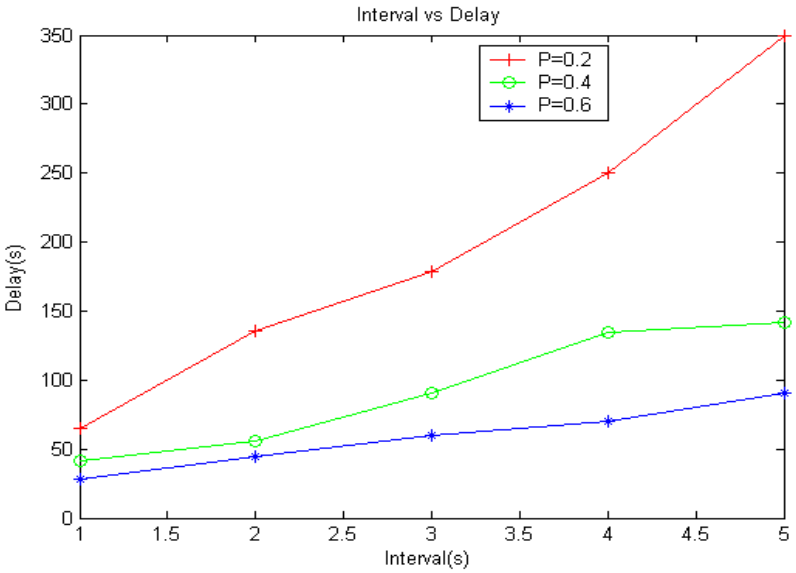


**Figure 3-5: Delay vs Transmission Interval**

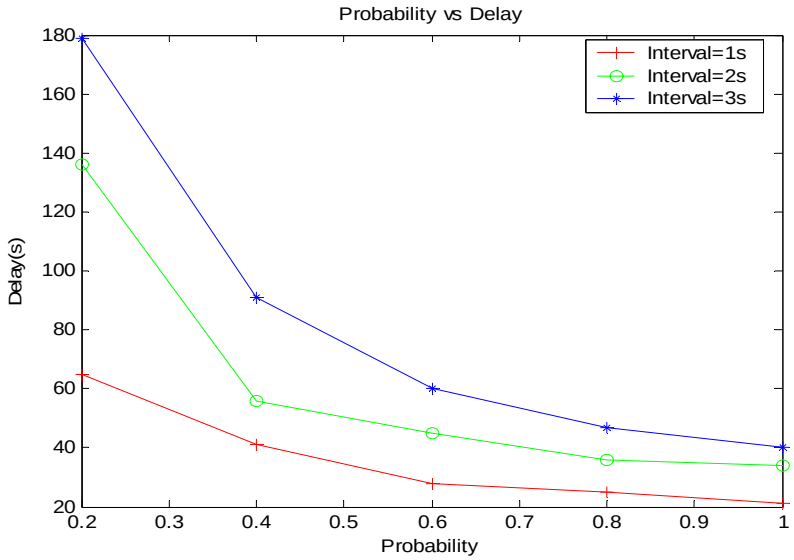


**Figure 3-6: Delay vs Probability**

When more and more vehicles are equipped with OBUs, the probability that the neighbors have the desired file will be large. This must enhance the feasibility of implementing our purchasing application. In summary, through the simulation, we can see that our system for the commercial application on a VANET is feasible and efficient.

# Chapter 4 Conclusion and Future Work

Vehicular ad hoc networks (VANETs) support vehicle-to-vehicle communications and vehicle-to-infrastructure (RSU) communications. Dedicated Short Range Communications (DSRC) protocol, which provides powerful radios and abundant spectrums, allows both safety-related and non-safety-related applications supported in VANETs. In this thesis, we have proposed a potential commercial application scenario that enables file purchasing through VANETs. In the proposed application, through V2I communications, a vehicle makes purchasing from an RSU which is connected to the Internet. Because of the high mobility of the vehicles, the contact period between the RSU and the vehicle may not be sufficient to download the complete file. Once out of the RSU's transmission range, the file acquisition can continue through V2V communications. To further enable the application, the security issues in terms of user privacy, secure billing, incentive for cooperation, and file copyright protection are handled. By using the micropayment approach and the tamper-proof device equipped in each vehicle, we stimulate the neighbors to cooperate with each other and prevent an unauthorized user from distribution of a file. With security analysis and extensive simulations, we have demonstrated that our solution is secure and efficient.

In the future research, we will further study on incentive mechanisms during V2V communications. In addition, we will study on other security issues existing in VANETs.

## Bibliography

[ABD2006] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmuller. Attacks on Inter Vehicle Communication Systems - an Analysis. *3rd International Workshop on Intelligent Transportation (WIT 2006)*, March, 2006.

[ANSI X9.62-2005] American National Standards Institute. Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). *ANSI X9.62-1988*, January, 2005.

[ASV] http://www.its.go.jp/ITS/2002HBook/appendix/6-5e.html

[BF2001] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *Proceedings of Crypto 2001*, LNCS, Vol. 2139, pp.213-229, 2001.

[BS1995] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, Vol.44, pp. 1897-1905, 1998.

[C2C] Car2Car Communication Consortium, http://www.car-2-car.org/.

[CHP2007] J. Camenisch, S. Hohenberger and M. Pedersen. Batch Verification of Short Signatures. In *Proceedings of EUROCRYPT*, Vol. 4515, pp. 246-263, 2007.

[CM2000] G. Cohen, S. Encheva and Gilles Zémor. Copyright Protection for Digital Data. *IEEE communications letters*, Vol. 4, No.5, May 2000

[D2002] J. Douceur. The Sybil attack. In *First International Workshop on Peer-to-Peer Systems (IPTPS)*, March 2002.

[DoT2006] U. S. Department of Transportation. National Highway Traffic Safety Administration. Vehicle Safety Communications Project. Final Report, April, 2006.

[DoT_AppendixH] U. S. Department of Transportation. National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report. Appendix H: WAVE/DSRC Security, April, 2006. http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFs/AppendixH.pdf

[DOT_AppendixB] U. S. Department of Transportation. National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report. Appendix B: Vehicle Safety applications, April, 2006. http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFs/AppendixB.pdf

[DSRC] 5.9G DSRC. http://grouper.ieee.org/groups/scc32/dsrc/

[DSRC_Home] http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[FRF2007] J. Freudiger, M. Raya and M. Feleghhazi. Mix Zones for Location Privacy in Vehicular Networks. In *Proceedings of the 1st International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 07)*, Vancouver, Canada, August, 2007.

[GBW2007] J. Guo, J. P. Baugh, and S. Wang. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. In *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, Anchorage, Alaska, May, 2007.

[GM2001] P. Golle and N. Modadugu. Authenticating Streamed Data in the Presence of Random Packet Loss. *ISOC Network and Distributed System Security Symposium*, pp.13-22, 2001.

[H1994] N. Haller. The S/Key one-time password system. In *Proceedings of the Symposium on Network and Distributed Systems Security*, pages 151-157. Internet Society, February 1994.

[HAKL2005] Q. Huang, I. C. Avramopoulos, H. Kobayashi and B. Liu. Secure Data Forwarding in Wireless Ad Hoc Networks. In *Proceedings of IEEE International Conference on Communications (ICC 2005)*, Seoul, Korea, May, 2005.

[K2005] T. Kosch. Technical Concept and Prerequisites of CAR 2 CAR Communication. *The 5th European Congress and Exhibition on Intelligent Transport Systems and Services (ITS2005)*, Hannover, Germany, June, 2005.

[L1981] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, Vol. 24, Issue 11, pp. 770-772, November, 1981.

[LSHP2006] M. Li, K. Sampigethaya, L. Huang and R. Poovendran. Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy. *WPES'06: Proceedings of the 5th ACM workshop on Privacy in electronic society*, Alexandria, VA, USA, October 30, 2006.

[LH2004] J. Luo and J. P. Hubaux. A Survey of Inter-Vehicle Communication. *Technical Report IC/2004/24, School of Computer and Communication Sciences*, EPFL, Lausanne, Switzerland, 2004.

[LPAG2006] U. Lee, J. -S. Park, E. Amir, and M. Gerla. FleaNet: A Virtual Market Place on Vehicular Networks. *V2VCOM, 2006.*

[LPPG2007] S. Lee, G. Pan, J. Park, M. Gerla, S. Lu. Secure Incentives for Commercial Ad Dissemination in Vehicular Networks. In *proceedings of ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'07),* pp. 150-159, 2007.

[MLS2005] T. Mak, K. Laberteaux and R. Sengupta. A Multi-Channel VANET Providing Concurrent Safety and Commercial Services. *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pp. 1-9, 2005

[MNT2001] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, Vol.5, pp. 1234-1243, 2001.

[NAG2004] V. Namboodiri, M. Agarwal and L. Gao. A study on the Feasibility of Mobile Gateways for Vehicular Ad-hoc Networks. In *Proceedings of the 1st ACM workshop on Vehicular ad hoc networks (VANET04)*, October, 2004.

[NDZPG2005] A. Nandan, S. Das, B. Zhou, G. Pau, and M. Gerla. AdTorrent: Digital Billboards for Vehicular Networks. *V2VCOM*, 2005.

[NOW]: Networks-on-Wheels, http://www.network-on-wheels.de/documents.html

[NS2] University of South California. The Network Simulator ns-2. Available at http://nsnam.isi.edu/nsnam/index.php/User_ Information

[PNM2006] K. Plossl, T. Nowey and C. Mletzko. Towards a Security Architecture for Vehicular Ad Hoc Networks. *The 1st International Conference on Availability, Reliability and Security (ARES2006)*, pp. 374 -381, April, 2006.

[PGH2006] P. Papadimitratos, V. Gligor and J. P. Hubaux. Securing Vehicular Communications - Assumptions, Requirements, and Principles. *Workshop on Embedded Security in Cars (ESCAR)*, Berlin, Germany, November 14-15, 2006.

[PP2005] B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. In *Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets-IV)*, November, 2005.

[RAH2006] M. Raya, A. Aziz and J. P. Hubaux. Efficient Secure Aggregation in VANETs. In *Proceedings of the 3rd International workshop on Vehicular ad hoc networks (VANET06)*, pp. 67-75, September, 2006.

[RH2005] M. Raya and J. P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN 2005)*, November, 2005.

[RH2007] M. Raya and J. P. Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, Vol. 15, pp. 39 - 68, 2007.

[RPH2006] M. Raya, P. Papadimitratos, and J. P. Hubaux. Securing Vehicular Communications. *In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, October, 2006.

[RS1996] R. Rivest and A. Shamir. Payword and MicroMint: Two simple micropayment schemes. *In Proceedings of International Workshop on Security Protocols*, ser. LNCS, Vol. 1189, pp. 69–87, 1996.

[SJ2004] A. K. Saha and D. B. Johnson. Modeling Mobility for Vehicular Ad Hoc Networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, Oct. 2004.

[SXSSZ2006] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang. Adaptive Privacy-Preserving Authentication in Vehicular Networks. In *Proceedings of IEEE International Workshop on Vehicle Communication and Applications,* Beijing, Oct 27, 2006.

[SURH2007] S. U. Rahman and U. Hengartner. Secure Crash Reporting in Vehicular Ad hoc Networks. In *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm2007)*, Nice, France, September, 2007.

[TC2003] J. Tian and L. Coletti. Routing approach in CARTALK 2000 project. In *proceedings of the IST Mobile & Wireless Communications Summit 2003,* Vol. 2, 2003.

[TO2003] H. Tewari and D. O'Mahony. Real-time payments for mobile IP. In *IEEE Commun. Mag.*, Vol. 41, No. 2, pp. 126–136, 2003.

[VII] http://www.vehicle-infrastructure.org/

[VSCC] http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm

[VSF2007] A. Viejo, F. Seb´e and J. D. Ferrer. Secure and Private Incentive-Based Advertisement Dissemination in Mobile Ad Hoc Networks, *IWSEC*, pp. 185-198, 2007.

[WTWL2004] M. Wu, W. Trappe, Z. Wang, and K.J.R. Liu. Collusion Resistant Fingerprinting for Multimedia. *IEEE Signal Processing Magazine, Special Issue on Digital Rights Management*, pp.15-27, March 2004.

[WWZTL2005] Z. Wang, M. Wu, H. Zhao, W. Trappe, and K.J.R. Liu. Collusion Resistance of Multimedia Fingerprinting Using Orthogonal Modulation. *IEEE Trans. on Image Proc.*, vol.14, no.6, pp.804-821, June 2005.

[XMKS2004] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-to-Vehicle Messaging in DSRC. In *Proceedings of the 1st ACM Workshop on Vehicular Ad Hoc Networks(VANET)*, pp. 19-28, 2004.

[YASM2005] R. M. Yadumurthy, C. H. Adithya, M. Sadashivaiah and R. Makanaboyina. Reliable MAC Broadcast Protocol in Directional and Omni-directional Transmissions for Vehicular Ad hoc Networks. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET 05)*, September, 2005.

[ZF2007] Y. Zhang and Y. Fang. A secure authentication and billing architecture for wireless mesh networks. *Wireless Networks*, vol.13, pp.663-678, 2007.

[ZLLF2007] Y. Zhang, W. Lou, W. Liu, and Y.-G Fang. A secure incentive protocol for mobile ad hoc networks. *Wireless Networks*, vol.13, pp.569-582, 2007.

[ZLLH2008] C. Zhang, X. Lin, R. Lu and P.-H. Ho. RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks. *IEEE International Conference on Communications (ICC'08)*, Beijing, China, May 19-23, 2008.

[ZLLHS2008] C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen. An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks. *The 27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona.

[ZL1998] J. Zhou and K. Lam. Undeniable billing in mobile communication. In *ACM MobiCom'98*, Dallas, TX, Oct. 1998.