Analysis and detecting of misbehaviours in VANETs

Shuxian Yan

Technical Report
RHUL–MA–2014–4
01 September 2014

Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX,
United Kingdom

www.ma.rhul.ac.uk/tech
Shuxian Yan

Department of Mathematics

*MSc in Information Security*
Royal Holloway University of London

Analysis and detecting of misbehaviours in VANETs

_Supervisor:_ Dr. Gerhard Hancke
Abstract

Vehicular ad hoc network (VANETs) allows vehicles to communicate to each other and to roadside units. This enables a lot of different applications which can bring safety, efficiency, convenience and other benefit to users and the traffic system. Therefore, it received huge attention from academic area, government and manufactary. This paper focus on the security issues of the system. We are going to build a basic model for the system and analysis the attacks that may happen to it.

Keywords: System model, attack tree analysis, CL-PKC framework
# Contents

1 **Introduction** ................................................................. 8  
   1.1 Motivation ................................................................. 8  
   1.2 Content outline ......................................................... 8  

2 **Introduction of VANETs** .................................................. 9  
   2.1 Overview of VANETs ...................................................... 9  
   2.2 Applications .................................................................... 11  
   2.3 Related standards .......................................................... 12  

3 **System requirements** ........................................................... 14  
   3.1 Characters of VANETs .................................................... 14  
   3.2 Security requirements ..................................................... 15  
      3.2.1 Access control and authorisation .................................. 15  
      3.2.2 Confidentiality ....................................................... 15  
      3.2.3 Authentication ....................................................... 15  
      3.2.4 Accountability and liability ....................................... 16  
      3.2.5 Anonymity and privacy ............................................. 16  

4 **System model** ..................................................................... 18  
   4.1 Cryptography in VANETs .................................................. 18  
   4.2 Reputation system .......................................................... 19  
   4.3 Modelling the VANETs .................................................... 20  
      4.3.1 Components in VANETs system ................................... 20  
      4.3.2 Architecture model .................................................. 23  
      4.3.3 Information flow model ............................................. 26  
      4.3.4 Geographic graph model .......................................... 27  

5 **Misbehaviours in VANET** ...................................................... 28  
   5.1 Misbehaving nodes .......................................................... 28  
      5.1.1 Malicious and rational .............................................. 28  
      5.1.2 Outsider and insider ............................................... 29  
      5.1.3 Single and multiple .................................................. 29  
      5.1.4 Analysis of adversaries ............................................. 29  
   5.2 Types of attacks ............................................................ 30  
      5.2.1 Attacks target messages in VANETs ............................. 30  
      5.2.2 Attacks target users in VANETs ................................... 31  
      5.2.3 Attacks target network in VANETs .............................. 32  
   5.3 Attack tree analysis ........................................................ 33
5.3.1 Attacks against cryptographic system of VANETs .................. 33
5.3.2 Message tampering ............................................................ 35
5.3.3 Position tracking ............................................................... 37

6 A certificateless cryptography based framework for VANETs 39
6.1 Motivation ............................................................................. 39
6.2 Introduction of the certificateless cryptography ......................... 40
6.3 Framework description .......................................................... 42
6.4 Analysis .................................................................................. 43
   6.4.1 Security analysis of the framework ................................. 43
   6.4.2 Advantages ................................................................. 43

7 Conclusion ............................................................................... 45
7.1 Our contribution ................................................................. 45
7.2 Future work .......................................................................... 45
List of Figures

1. The illustration of network stack in VANET [1, 2] ............................................10
2. Simple Illustration of V2V and V2I communication in the VANET . ..................11
3. Simple illustration of the architecture in VANETs ..............................................22
5. Simple illustration of the communication in a small VANETs . .................... 24
6. Simple illustration of architecture of OBU .........................................................25
7. Illustration of message growth for a traffic jam detection application in VANETs. Schematic bandwidth comparison between normal message dissemination and aggregation[13]. ..........................................................27
8. The topology of a virtual highway with 4 lanes[47]. ........................................28
9. The ID disclosure attack from [36, 39] ..............................................................31
List of Tables

1. Key Parameters in the DSRC Physical Layer Standard [57] .................12
2. Notations in section 4 .................................................................................18
3. Notations in ID disclosure attack .................................................................31
4. Notations in the introduction of a certificateless cryptography based framework for VANETs ..........................................................................................................................3

9
Abbreviations

ASTM American Society for Testing and Materials
BPSK Binary phase-shift keying
CAs Authorities
CL-PKC Certificateless public key cryptography
CRL Certificate revocation list
DoS Denial of Service attack
DSRC Dedicated short-range communications
ECC Elliptic curve cryptography
ECDSA Elliptic Curve Digital Signature Algorithm
ECIES Elliptic Curve Integrated Encryption Scheme
EDR Data recorder
FCC Federal Communications Commission
ID-PKC Identity-based cryptography
ITSs Intelligent transportation systems
KGC In CL-PKC: Key distribution center
MANETs Mobile Ad-Hoc Networks
NTRU This is a patented public-key crypto-system that uses lattice-based cryptography[52].
OFDM Orthogonal frequency-division multiplexing
PKI Public key infrastructure
QPSK Quadrature phase-shift keying
RCs Complex RSUs
RSs Simple RSUs
RSUs Roadside units
TCP Transmission Control Protocol
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCs</td>
<td>Trust components</td>
</tr>
<tr>
<td>TPD</td>
<td>Temper-proof Device</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>V2I</td>
<td>vehicle-to-infrastructure communication</td>
</tr>
<tr>
<td>V2V</td>
<td>vehicle-to-vehicle communication</td>
</tr>
<tr>
<td>VANETs</td>
<td>Vehicular ad hoc network</td>
</tr>
<tr>
<td>VRC</td>
<td>Vehicle-to-roadside communication</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless Access for the Vehicular Environment</td>
</tr>
<tr>
<td>WME</td>
<td>WAVE Management Entity</td>
</tr>
<tr>
<td>WSMP</td>
<td>WAVE Short Message Protocol</td>
</tr>
</tbody>
</table>
1 Introduction

After the development of wireless communication technologies, Vehicular Ad-Hoc Network (VANET) has received a lot of attentions in both research and standardisation field. A lot of applications have been developed for VANETs. These applications can help improve vehicle and road safety, efficiency, convenience and so on [43]. The importance of VANETs has already been recognised by governments and the industry. Audi, BMW, Daimler Chrysler, Fiat Renault and Volkswagen have united and created the Car2Car Communication Consortium to do research on it [35]. A larger amount of projects and academic conferences are funded by government and industry [54]. With increasing demanding of the development of VANETs, security issues in VANETs are inevitably getting attentions from academic researchers.

1.1 Motivation

Although the VANETs has been studied for decades, there are still no consistent conclusions on most of the issues. Till now, the system exists only in theory. As to most researchers, there are not only a lot of uncertainties but also a lot of ideas. Studies of VANETs have explored its' characters, challenges and security issues about the system [21, 28, 33, 43] as well as methods, protocols and countermeasures that useful to it [29, 46, 47, 58] etc. Their researches are like puzzle pieces, form every vivid pictures on a huge blueprint. In the process of the project, every idea is based on others researches. Without them, it is impossible for me to witness the attractive unknown world of VANETs. Among all the unsolved puzzles, what we are mostly interested in at the moment is the security related issues. The WAVE standard gives a framework of security service for VANETs [2] without providing any specific protocol or details. Therefore, we are going to do security analysis and attack analysis based on the basic model of VANETs built in the paper. Then we will propose a high level cryptographic system that may help deal with the security issues in the system.

1.2 Content outline

In this paper, we are going to have an overview of the VANETs and the security requirement for it in section 3 and 4. Then base on the function and security requirements of VANETs, we are going to build a basic model of VANETs in section 5. The model will cover main security issues that may happen to the system. Based on the model, we are going to do security analysis in section 6. The emphasis of the security analysis is privacy and anonymity problem. In section 7, we will introduce the certificateless cryptographic framework for VANETs and its security analysis.
2 Introduction of VANETs

In order to enhance the road safety, efficiency and convenience of surface transport, US government established the Intelligent Transportation Systems (ITSs) programme in 1991 through “The Intermodal Surface Transportation Efficiency Act” [41]. ITSs will be used to solve transportation problems, such as road safety and congestion, so as to improve benefits at large in social, economic, and political systems [23]. Since establishment, the programme has got a lot of attentions from both the academic and industry. Researches such as vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I) are undergoing with great support from US government [42]. ITSs requires a combination of different technologies such as engineering and information technology. With a lot of innovative benefits, researchers from different fields have great interests in it. Among those, VANETs is a very important component for constructing ITSs. In 1999, the United States Federal Communications Commission (FCC) allocated 75MHz of spectrum in the 5.9GHz band for Dedicated short-range communications (DSRC) used by VANETs communication [51].

2.1 Overview of VANETs

The concept VANETs is developed based on Mobile Ad-Hoc Networks (MANETs). In VANETs there is no centralised authority or server. Nodes in VANETs are communicating directly without relying on any dedicated infrastructure for building network communication, contrary to earlier vehicular networks. Moving cars are used as nodes to create mobile network. They act as senders, receivers and routers to create or transmit information for other vehicles or infrastructures [11]. The network communication architecture of VANETs is similar to MANETs. The network stack as shown in figure 1 of VANETs can be found in Wireless Access for the Vehicular Environment (WAVE) [1, 2].

At application layer, there are usually three types of applications: safety, traffic efficiency and infotainment, we classified them as safety related and non-safety related applications. Transport layer includes message handily, transport protocol and TCP/UDP. Network layer has the database, service tools and extension. The WAVE defined short messaged protocol is also worked at transport and network layer. The physical layer is radio layer [57].

There are two types of communications in VANETs, V2V and V2I and three ways of communication pattern: beaoning (single-hop broadcast), restricted flooding
Figure 1: The illustration of network stack in VANET [1, 2]

(multi-hop broadcast) and unicast.[43]. The illustration of VANETs can be found in figure 2.

**Vehicle-to-vehicle (V2V)** In V2V communication, vehicles use multi-hop multicast/broadcast to transmit traffic related information. An example in figure 2, the first car (Bugatti) see a banner ahead on the road, maybe the highway is under construction. The related application in Bugatti will try to inform other cars about this situation. In intelligent transportation systems, vehicles just need to concern about the issues ahead of them. This means that they only receive messages from ahead. Therefore, Bugatti will send messages to the car behind him to inform the situation. There are two type of messages in V2V communication: naive broadcasting and intelligent broadcasting [43]. Naive broadcasting means that vehicles send messages regularly under certain frequency. Intelligent broadcasting is usually for safety related applications. It will detect the emergency event and use less messages. The communication range of Bugatti is limited. The only car within its range is the yellow posh car (Lamborghini). After getting the message from Bugatti, Lamborghini will try to transmitted the message to the back as well. In this way, all the cars along the road can be informed about the situation in front.

**Vehicle-to-infrastructure (V2I)** In V2I, also called VRC (Vehicle-to-roadside communication), the roadside unit (RSU) broadcasts messages to all vehicles within the range of signal. The RSUs are places at regular intervals ideally. This enable the signal to be maintained. For example, in figure 2, the speed limit of this highway is 70 miles per hour. The blue circles are RSUs’ signal range which cover
Figure 2: Simple Illustration of V2V and V2I communication in the VANET

almost every car in the picture. The RSU will detect the speed of vehicles and send a warning message if any vehicle is speeding. V2I communication is also an important channel to maintain the security issues in VANETs. For instance, revocation of cryptographic credential and maintain the reputation system, etc. This will be discussed later.

2.2 Applications

Overall, the applications provided in VANETs can be described as safety related applications and non-safety related applications. Safety related applications are mainly about the driving actions. For example, the collision warning, emergency warning, lane merge assistance, etc [13]. Safety message and “safety of life" messages from safety related applications have the highest priority in the communication channel in the network [56]. The messages of no life critical problem have the lowest priority. For instance, messages from parking applications. The network will allow the safety related messages to be processed first based on their priorities.
2.3 Related standards

In order to support VANETs, some standards and frameworks were set by communities and governments. Among those, IEEE 802.11p and DSRC are of great importance.

**Dedicated Short Range Communication (DSRC)** Dedicated Short Range Communications (DSRC) is a short to medium range communication service. This can be used to support vehicle-to-vehicle and vehicle-to-roadside communications. DSRC is designed to provide high data transfers and low communication latency within a limited zone. Dedicated Short-Range Communications (DSRC) is 75 MHz of spectrum at 5.9 GHz allocated by the Federal Communications Commission (FCC) to increase traveller safety, reduce fuel consumption and pollution, and continue to advance the nation’s economy [55]. In 2003, the American Society for Testing and Materials (ASTM) approved the ASTM-DSRC standard which was based on the IEEE 802.11a physical layer and 802.11 MAC layer [5]. DSRC is a free but licensed spectrum. This means that people can use the DSRC without paying any fee to the United States Federal Communications Commission (FCC) but the usage of DSRC is limited [12]. The DSRC is organised to seven 10Hz-wide channels. Among them, one is for safety purpose and two for special use, and others can be used for other applications [57, 5].

| Data rate  | 3, 4.5, 6, 9, 12, 18, 24, 27 Mbps |
| Modulation | BPSK, QPSK, 16-QAM, 64-QAM        |
| Coding rate| 1/2, 2/3, 3/4                      |
| Number of Subcarriers | 52                             |
| Number of Pilot Tones  | 4                                 |
| OFDM Symbol Duration  | 8 µsec                            |
| Guard Interval       | 1.6 µsec                          |
| Subcarrier Spacing   | 156.25 KHz                        |
| Signal Bandwidth     | 10 MHz                            |

**IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) (IEEE 802.11p)** Vehicular wireless network is highly dynamic due to the speed of vehicles, the situation of traffic and the driving environment. Therefore, the old standard of IEEE 802.11 Media Access Control (MAC) operations is unsuitable for the VANETs scenario. The wireless communication in
VanETs requires faster data exchange, i.e. a very quick hand shake. In order to address these problems, Wireless Access in Vehicular Environment (WAVE) is made by ASTM[17]. The WAVE standards define an architecture and a complementary, standardised set of protocols, services and interfaces that collectively enable secure V2V and V2I wireless communications [30]. It also describes applications that resides on the RSU with access to the OBU[16].

- IEEE Std 1609.2\textsuperscript{TM} - 2013 - Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages
- IEEE Std 1609.3\textsuperscript{TM} - 2010 - Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services
- IEEE Std 1609.3\textsuperscript{TM} - 2010/Cor 1 - 2012 - Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services Corrigendum 1: Miscellaneous Corrections.
- IEEE P1609.3\textsuperscript{TM},2010/Cor 2 - Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services Corrigendum 2: Miscellaneous Corrections.
- IEEE Std 1609.4\textsuperscript{TM} - 2010 - Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operations
- IEEE P1609.4\textsuperscript{TM} - 2010/Cor 1 - Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operations Corrigendum 1: Correct Identified Errors.
- Draft IEEE P1609.6 - Remote Management Services
- IEEE Std 1609.11\textsuperscript{TM} - 2010 - Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS)
- IEEE Std 1609.12\textsuperscript{TM} - 2012 - Identifier Allocations.

Although the WAVE family of standards have defined a lot in terms of the framework of VANETs and communications, on security issues, the IEEE Std 1609.2\textsuperscript{TM} doesn’t provide specific protocols for revocation of certificates and keys.
3 System requirements

In this section, we are going to analysis VANETs in its characters and security requirements.

3.1 Characters of VANETs

Network Scale The amount of nodes in VANETs is determined by the number of vehicles. As there may be millions cars in a city, the number of nodes in a VANET can be numerous. This causes the problem of network scale. As [31] described, scalability problem may affect reliability, system load, administration and heterogeneity in a distributed network. Therefore, the scalability is defined as “the ability to handle the addition of nodes or objects in a network without suffering a noticeable loss in performance or increase in administrative complexity”[22]. Concisely explain the scalability problem respectively as following: as to the reliability, because of the bandwidth limitation in VANETs, it is very likely to cause network congestion with presence of a large number of nodes. This may cause connectivity problem in the network [24]. The number of nodes have the greatest influence on the number of messages in the network. Rebroadcast of certain messages, such as safety messages, aggravate the network load problem in VANETs. Central administration needs to be in place to manage nodes and maintain common information. Although the scale of VANETs is huge, the administration problem may be addressed by government authorities. Extensive infrastructures, such as CCTVs, have already been developed by governments. It can be used to track and administrate nodes in the network. Heterogeneity refers to that given such a large amount of vehicles, a variety of equipments or systems exist in different cars [24, 27]. For example, both GPS and Galileo receiver can provide geographic information. There may be security issues arises because of the heterogeneity of the network. As an example, there may exist a certain attack for Galileo receiver but not for GPS. This means, the Galileo receiver may become a weak link in the network.

Network Volatility The majority of nodes in VANETs are vehicles. They have different speed along different roads. When travelling on highways, the speed of vehicles can reach 70 mile per hour or more. This means that the connection among nodes changes rapidly. The changes are not only because of the speed, but also because of the density of nodes. The amount of nodes within their transceiver range can vary a lot during a short period of time. The dynamic property of the network makes the gradual development of trust among acquaintances impractical [27]. Comparing to MANETs, the routing of nodes is more predictable. Majority
of the nodes are going to travel within the road network which is static and easy to track. Therefore, there is high degree of volatility of VANETs in terms of the speed of nodes, which may result in frequent topology change, but limited changes in terms of the geographic positions of nodes. This makes nodes in the network vulnerable to position tracking.

### 3.2 Security requirements

The security service provided by WAVE framework is confidentiality, authentication, authorisation and integrity. All these generic services are provided by cryptographic schemes, i.e. encryption and signature scheme [2]. In this section, the security requirements of VANETs will be discussed in details.

#### 3.2.1 Access control and authorisation

Vehicles as users that wish to access VANETs services must be authorised by authorities (CAs). Vehicles will be given cryptographic credentials and under the constrain of security policies. Some other nodes in the VANETs, such as RSUs and public vehicles, have different levels of trustworthiness to private vehicles. They have different privileges in the network. Nodes without authorisation should not be able to access services or get the content of messages exchanged by legitimate nodes in the VANETs. Therefore, certain access control must be in place.

#### 3.2.2 Confidentiality

Confidentiality is needed to prevent eavesdropping of cryptographic credentials by adversaries. However, confidentiality in VANETs is not as important as in other systems such as mobile network. This is because in VANETs, the majority of messages are not about privacy issues but public issues. There are no specific receivers that those messages are sent to. For example, if there is an emergency on road, the messages should be transmitted to users nearby as many as possible and as quick as possible. The important issue of messages in VANETs is authentication of the messages. Receivers need to confirm whether the messages came from legitimate users in the network in stead of attackers.

#### 3.2.3 Authentication

In the VANETs system, the authentication of messages are important for reducing attacks, such as message forgeries. If achieve the authentication of messages, it implies that the integrity of the message has not been violated. Therefore, integrity of message is not going to be mentioned separately.
**Data origin authentication** This is required in every message exchanged in the system. There should not be any alteration, modification on the content of messages including the geographic and time information. Reaction of any event in the system should be from legitimate users. The system should also be able to authenticate the sender of the message. However, this doesn’t mean that the identity of the user can be exposed to others.

**Entity authentication** The communication in VANETs are frequently. It is necessary to check the liveness of senders in the network. Entity authentication usually achieved by freshness in protocol. In the scenario of VANETs, as DSRC specified, the time interval of messages from each vehicle is about 300 millisecond within range from 110 meter to 300 meter and sometimes less than 100 millisecond [5]. The tolerable processing delay per message is between 2.5 milliseconds to 2.78 milliseconds [36]. The verification of liveness must be done within a very short period of time. This requires that the computational speed of the verification scheme should be very high.

**Non-repudiation** This means that the sender cannot deny of sending the message. In VANETs, there are safety related messages transmitted. It is important to have the assurance of the senders of these messages. This can be achieved by digital signature which will be discussed later.

### 3.2.4 Accountability and liability

With safety-critical nature of VANETs, accountability and liability are important. Users should be responsible for their deliberate or accidental actions which may disrupt the operations within the network. The evidences for identify the disrupter should be provided by the network at the mean time, the system should not leak information about users’ identities.

### 3.2.5 Anonymity and privacy

Every node has a unique ID. The ID can be assigned by government authorities based on the registration information of vehicles. They can also be assigned by manufacturers based on vehicle’s unique chassis number or engine number. The unique IDs of vehicles are very sensitive information in the VANETs. It directly related to privacy issues such as user’s registration information and security issues such as acceptability and revocation of public-private key pairs. This makes anonymity and privacy the harshest requirements in VANETs. Anonymity and privacy are related but different in VANETs.
**Anonymity** If the user’s anonymity in the network is maintained, it means that an observer cannot distinguish which node performs the actions. To be precise, as explained in [18], the most minimally anonymous is that the observer $j$ cannot be sure that node $i$ actually performed the action. However, node $i$ may be the “prime suspect” to $j$. A stronger version is that in a set consists of $k$ nodes, as far as the observer is concerned, anyone in the set may have performed the action [18]. Total anonymity means that the action could have been performed by anybody in the system [18]. It is impossible to achieve totally anonymous in VANETs given such a large scale of the network.

**Privacy** Privacy is typically for hiding personal or private information from others [18]. The requirement for privacy in VANETs can be described as that there should be no more exposure of private information with the VANETs than without it [32]. The license plates and chassis numbers on cars can be easily observed by attacker. However, without VANETs, it is difficult for attackers to track vehicles based on their ID information remotely. VANETs should not be the weakest link in people’s privacy demands on road. There are some attacks that target at the privacy of users in the VANETs, mostly for finding out their identities or track their geographic information, for example, the ID disclosure attack[36, 39]. Therefore, anonymous public keys may be used for hiding such information. This will be discussed in the next section.
4 System model

The standardised system model of VANETs are still under development. In order to analysis the attacks of the system in later sections, we need to have a framework of VANETs. We are going to discuss the model from cryptography perspective, reputation system applied in the network and the system architecture.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N_i$</td>
<td>User $i$</td>
</tr>
<tr>
<td>$ID_i$</td>
<td>Identity of user$_i$</td>
</tr>
<tr>
<td>$R_i$</td>
<td>Communication range of user$_i$</td>
</tr>
<tr>
<td>$PK_i$</td>
<td>Public key of user$_i$</td>
</tr>
<tr>
<td>$SK_i$</td>
<td>Private key of user$_i$</td>
</tr>
<tr>
<td>$Sign_i$</td>
<td>Signed by user$_i$</td>
</tr>
<tr>
<td>$Cert_i$</td>
<td>The certificate of user$_i$</td>
</tr>
<tr>
<td>$VER_i$</td>
<td>Verification process of a certificate</td>
</tr>
<tr>
<td>$Geo_i$</td>
<td>The geographic information of user$_i$</td>
</tr>
<tr>
<td>$TS$</td>
<td>Timestamp</td>
</tr>
<tr>
<td>$Event$</td>
<td>Event information in the message</td>
</tr>
</tbody>
</table>

Table 2: Notations in section 4

4.1 Cryptography in VANETs

In order to meet the security requirements of VANETs, i.e. authentication, accountability and liability, public key infrastructure (PKI) is necessary. One advantage for VANETs is that the vehicles in the network have enough computational capability for PKI including public-key encryption and digital signature related computation [35]. Given the scenario of VANETs, in order to maintain certain level of privacy of users, the life time of short-term public key, for signature and encryption, is around 50 seconds to 72 seconds, and the lifetime of certificate is about one day [36]. The rapid change of keys and certificate means a considerable storage space. Therefore, the smaller the key size is, the better for the system. The only signature algorithm supported by IEEE 1609.2 (WAVE) is the Elliptic Curve Digital Signature Algorithm (ECDSA) using either the P-224 or P-256 curves and the only asymmetric encryption algorithm supported is Elliptic Curve Integrated Encryption Scheme (ECIES) [2]. As explained in the standard, the reason for choosing elliptic curve cryptography (ECC) variant is because of the small size of key and signature. However, comparing to RSA and NTRU, ECC is faster in signing, but slower in verification [36]. Therefore, IEEE 1609.2 also suggests a variant described
as "Accelerated verification of ECDSA signatures" [2] in order to increase the speed for verification.

The main foreseeable issues of cryptographic in VANETs are key management and certificate revocation problems. In order to prevent ID disclosure attack, as mentioned before, the life-time of a anonymous key per vehicle is about one minute [36]. The anonymous key pairs can be derived from a master short-term key. However, it is not clear yet that how the authorities distribute certificates for the anonymous public keys. In the given scenario of VANETs, there can be two ways to distribute and renew the key pairs and certificates. One of them is that the cryptographic credentials, including anonymous key pairs and certificates, can be preload in the trusted devices on the vehicles. Then the OBUs can broadcast the messages with the corresponding certificates. However, there are still problems for this method. For example, it is hard to determine how many anonymous key pairs should be reloaded in the vehicles. A more straight forward solution is that the authorities authorise local authorities (i.e. RSUs with additional function) distribute certificates based on the long-term ID of nodes [33]. To be precise, the authorised RSUs are placed along roads, this enable them to have quick access to vehicles. RSUs can communicate with authorities through back bone network. Vehicles generate anonymous key pairs themselves then send them with their long-term ID to the local authorities. The authorities will check their ID and then sign the corresponding certificates of their anonymous key pairs. The new certificates will distributed to vehicles through RSUs. However, it will need a method for RSU to authenticate the vehicles. Issues may arise if one of the RSUs being compromised. The certificate revocation list (CRL) will be distributed by infrastructures.

In order to deal with the key pairs and certificates revocation problem, we will proposed a high level method based on the certificateless cryptography in the last chapter.

4.2 Reputation system

Reputation system is a tool that can work together with cryptography to detect malicious nodes in the system. There are several different mechanisms which have same effect as reputation system, such as revocation-based mechanism [58]. Revocation-based mechanism is used to evict the selfish or malicious insiders from the network. It is first proposed in [37]. The protocol of revocation game was designed in [38]. However, the existing works, which depends on the identity of the nodes, still have problem in the anonymous property of VANETs.
The idea of the reputation system is that the reputation value of each nodes is based on the feedback of other nodes [25]. Reputation of a node is presented as a number. If a node’s reputation value lower than the threshold, then his message will be regarded as unreliable. The reputation system is made and maintained by CA and RSUs. If a RSU is compromised by attacker, the attacker is able to broadcasting wrong reputation value. This may cause users reject valid messages from legitimate nodes or accept wrong messages from unreliable nodes even attackers. Therefore, it is important to maintain and keep the reputation system in secure.

4.3 Modelling the VANTEs

In this chapter, we will try to build a comprehensive model for VANETs. There are three parts that construct the hole picture of VANETs. Architecture of the system, information flow model in the system and the geographic graph model for the system.

4.3.1 Components in VANETs system

The architecture of VANETs system has not been specified and still under development. Different architectures have been proposed with different characters and purposes, as well as different security challenges[33, 19]. The most basic architecture of VANETs is going to be discussed and adopted in this paper. The analysis and detection of misbehaviours are based on the basic architecture. There are roles indispensable in the basic VANETs system: Authority, Roadside Unit (RSU) and On Board Unit (OBU). The three components are necessary for the functionality in VANETs.

 Authorities They are public agencies or social organisations with administrative powers[32]. The role of authority in this architecture is to distribute cryptographic credentials. It may also be responsible for key management issues, such as certificate and key revocation. They can be from government transportation department or vehicle manufacturers. Because of the requirement of anonymity in VANETs, multiple authorities may co-exist to deal with the distribution of sensitive information.

 RSUs They are important for constructing the network and supporting services. RSUs are regards as more trustworthy than other nodes in the network [32]. They can provide reference information to users such as geographic information or help sync clocks on user’s vehicle. Ideally, RSUs should be placed evenly along roads.
However, this is very hard to archive. The complexity of RSUs can vary a lot. They may used just for beacon. They can have sophisticated functionality as well, such as checking vehicles’ trustworthiness through reputation system.

**OBUs** They are equipped on all the legitimate vehicles by default in VANETs. They are responsible for executing the protocols and storing data. OBUs on car can be easily accessed by owners of vehicles. Therefore within OBUs, trust components (TCs) are necessary for protecting cryptographic credentials and critical memory. They can be temper-resistant hardwares. This means the credentials are bounded with this vehicle. The function of temper-resistant can also be simplified as that just signed or encrypted audit trails so as to detected and prevented access to critical information [32]. In order to enhance the security of OBUs, [39] proposed two hardware modules for OBUs: Data Recorder (EDR) and the Temper-proof Device (TPD). EDR acts like 'black box', a temper-resistant storage. TPD is used to possesses cryptographic processes and protect cryptographic credentials. TPD is also required to have own clock and battery. These two modules clearly explain the required functions for TC. However, they cannot control whether the data received is correct or not. For example, a greedy user can compromise sensors and modify the data sent to the OBU. Because of the vital importance of VANETs, the services and applications are designed to have very limited interaction with drivers of vehicles. However, users should be considered apart from vehicles because of the human factor. Users cannot be the weakest link in the security of the networks.

**Private vehicles and public vehicles** The roles of vehicles are different in VANETs. Vehicles are regarded as private vehicles and public vehicles according to [39]. This setting will be adopted in this paper. Public vehicles can be police car, ambulance or even buses. Public vehicles are more trustworthy than private vehicles. They can help support the functionality in VANETs. The public vehicles may help to support the network functionality. For example, if there are conflicting messages of the same event, the message from public vehicles are more reliable. Their messages can help users summarise the messages they have received. Public vehicles with government authorisation, such as police car, may help authorities process some cryptographic credentials such as issue of a anonymous certificate for limited amount of nodes.

**Other stockholders** In VANETs, there are some other stakeholders. In [3], the role of "Home" was mentioned. When parking at home or other regular parking spaces, the OBUs can join the static network or communicate with home facilities. It is reasonable to take static wireless connection into account. Some applications
are designed for car-to-home communication. For example, there can be media synchronisation between car and home facilities. However, the security issues of car-to-home communication can be simplified as home network security. Therefore, in this paper, we didn't discuss it. For VANETs, database and service providers are also needed. The communication among them and authorities are not exactly using VANETs, therefore, their own security issues are not going to be discussed either. However, they are important for some VANETs security functions, for example, the location database may be used in certificate revocation[27].

In summary of the components in VANETs system is that authorities, RSUs and OBUs construct the network. They are all considered as nodes in the network. Figure 3 is the illustration of there relationship.

![Figure 3: Simple illustration of the architecture in VANETs](image)

**Setup** Authorities in this model are responsible for distribution of cryptographic materials. It is assumed that the authorities are trusted by all the nodes in the network. The authorities are notated as CAs.

Similar to the setup of authorities, RSUs also have ID, Public key and private key pair, signature and certificate. In order to differ from complex RSUs and simple RSUs, we will use RC and RS respectively.

OBUs are equipped in both public vehicles and private vehicles. We consider pri-
vate vehicles as the main users in the network, donated as $N_1, N_2, \ldots, N_i$.

It is worth noting that the users, i.e. the owner or driver of the vehicle, cannot extract cryptographic credentials from TC in OBUs [2]. As the figure 4 shows, the process will initiated by a request for encryption or signature to the TC, i.e. the "security service" in the picture. TC will do the cryptographic process with the cryptographic credentials stored in it then reply the request.

![Figure 4: Process flow for use of 1609.2 security services from[2]](image)

### 4.3.2 Architecture model

With the setup of nodes in the network, we are able to construct a basic architecture of the system. In order to have a clear picture of the network, the architecture is divided into three parts: whole picture of the network, architecture of OBUs and the communication model between authorities and RSUs.

**Overall structure** From the view of the whole picture of the network. First of all, authorities will distribute the long-term unique IDs, authorities’s signature verification key and corresponding certificates to the nodes in the network, including RSUs and OBUs. As soon as OBUs are on roads, they start to construct Ad-Hoc network and broadcasting messages. In order to authenticate to the network, they will need to attach the certificate to every message they send. All the nodes will function according to the applications set in the system and geographic information they have.

Figure 5 is a simple illustration of a small VANETs which only have one RSU and three OBUs. From the the scenario in the figure 5, node $N_1$ encounters an
Figure 5: Simple illustration of the communication in a small VANETs

event. It broadcast the notification of the event within its communication range $R_1$. The RSU and $N_2$ are in the communication range. This means that they can get the message. In order to authenticate the message, they need to verify the signature in the message. After successful authentication of the message, $N_2$ broadcast the event within its range which contains $N_3$. RSU will report the event to the backend through back bone network if necessary. The process can be expressed as following:

1. $N_1 \rightarrow R_1^*$: $Geo_1 || TS_1 || Event || \text{Sign}_1(Geo_1 || TS_1 || Event) || \text{Cert}_1$
   This message include the geographic information $Geo_1$ of $N_1$ and timestamp $TS$ to help other nodes decide whether this message is useful for them. If the message is from the nodes behind them or long time ago, they will reject the message without check the signature of the sender.

2. $N_2 \rightarrow VER_{Cert_1}(\text{Sign}_1(Geo_1 || TS_1 || Event))$
   After deciding accept the message, receiver $N_2$ needs to check the validation of the message by verifying the signature of sender $N_1$

3. $N_2 \rightarrow R_2^*$: $Geo_2 || TS_2 || Event || \text{Sign}_2(Geo_2 || TS_2 || Event) || \text{Cert}_2$
   If the message is valid information, $N_2$ needs to summarise the event and broadcast to other nodes. The process of summarisation is defined by message aggregation mechanism.

4. The broadcast will stop when the event end.
The example can give us an impression of the architecture of VANETs. However, it has simplified the message and information flow mode. To be precise, the content of the message and the broadcast mode depend on the type of event. For some safety related message, rebroadcast are required. In order not to affect the connectivity, the system mechanism will try to aggregate messages. This will be discussed in the next section.

**Inside OBUs** In order to process messages, OBUs have several components as illustrated in figure 6. The most security sensitive component is TC which stores the cryptographic credentials. Message storage stores the messages it has sent and received from other nodes. When the OBU is triggered by an event or messages from outside, it will start to process the message. The component that analyses the message, we call it "decision maker", will check with the message storage then decide whether to react to the event. Once it decide to send the message, it will send it to the information processor to process the message. The information processor will first aggregate messages if necessary, then ask TC for security service including signature and certificate. After TC reply the security request, the message will be broadcasted to the network attach with the signature and certificate.

![Figure 6: Simple illustration of architecture of OBU](image-url)
Communication between backend facilities  The communication model between backend, i.e. authorities and database, and RSUs is straightforward. They communicate through back bone network. The only problem need to solve here is how to keep audit trail of nodes in the network. As described in the previous sections, the only information that can identify the node is the unique ID of every vehicle. However, in order to maintain anonymous and privacy, nodes in VANETs use anonymous keys to do communication. This means, it is very difficult to identify nodes through anonymous keys. In theory, authorities have the ID of corresponding anonymous keys. Considering the scale of the network and the amount of anonymous keys for every node, the authorities will need to store very large amount of information for audit trail. Another possible solution for this problem is encrypted the audit trail locally with long term public private key pair issued by authorities for every message created by the node and stored in TC. If there is any need for accountability, the RSUs will request the TC to reply with the encrypted trail. Then authorities can check it.

4.3.3 Information flow model

Because of the scalability of VANETs, the information flow in it can grow very rapidly. Therefore, many researchers have proposed massage aggregation mechanism for VANETs [29, 26]. As explained in [13], take traffic jam detection as an example, the messages disseminated in the network grows with increase of vehicles. We can get the impression from figure 7. The vehicles in the figure are broadcasting their speed information in the network. The above situation is without aggregation. The node \( n \) will receive \( n \) messages from the cars in front. It is a large overhead for node \( n \) to process all the messages. It also put stress on the network in terms of limited bandwidth. The latter scenario is with message aggregation. Message aggregation is a mechanism that help OBUs summarising messages received from other nodes. There are several proposals about it have been made. For example, [53] suggested that using fix segments of roads can solve the problem. More and more researchers have focus on hierarchical aggregation [26, 7]. Hierarchical aggregation is a mechanism that help solve not only the message expansion in VANETs but also provide accuracy of the messages based on the geographic information. As for many applications, for example, congestion warning, are sensitive to geographic information. It means that the further the node is, the message is more inaccurate. As described in [26], the further away the region is, the coarser the information will be. Therefore, in this mechanism, the messages will be aggregated based on the geographic information of the message. However, most of the mechanisms are efficient for specific circumstances, such as fix road segments or certain application. There
are no mechanism that can generally solve the message aggregation problem. The ideal scenario is showed in the figure 7. The message can be efficiently summarised by each node then broadcast to the network.

Figure 7: Illustration of message growth for a traffic jam detection application in VANETs. Schematic bandwidth comparison between normal message dissemination and aggregation[13].

4.3.4 Geographic graph model

Geographic information is important in VANETs. The position information can be found almost in every message transmitted in the system. Applications want to take advantage of geographic information from users in the network. But users won’t be glad if their position information is leaked or tracked by any other party except for emergency reasons. The definition of geographic graph model can help process application messages in VANETs.

There are several ways to define a geographic graph model. In [53], it define geographic information by using average distance. In order to simplify the model, we are going to put our system on highway. The movements of nodes on highway are more organised and predictable than city road. The virtual highway has 4 lanes, two lane for each direction. The topology is showed in figure 8. The average speed of vehicles on highway is 70 mph. The density of nodes on road is about 64 cars per mile.
5 Misbehaviours in VANET

As long as a technology is related to safety issues, no one wants to see any mistake happen. However, mistakes, whatever rational or malicious, are inevitable. In VANETs, it is called misbehaviour. Modern vehicles increasingly depend on the computer system to provide accurate control of the performance on road and services inside the car. Due to the life-critical nature of the VANETs, this new technology will raise new threats against the traffic system, if the security issues are not properly handled, it will even endanger people’s lives.

5.1 Misbehaving nodes

5.1.1 Malicious and rational

Before talking about the rationale of misbehaving nodes, it is necessary to mention that the accidental misbehaviours are inevitable. Among intentional misbehaviour nodes, there are two types of attackers in terms of their objectives: malicious and rational. Malicious adversaries just want do damage to the users or the system instead of seeking for benefit from the attack as rational attacker [40]. They don’t consider the cost or consequence of their attacks. This make them more crazy and dangerous than rational attackers.
5.1.2 Outsider and insider

Outsider means that the misbehaving nodes (adversaries) are not in the network. They don’t have legitimate access to the network. In contrast, an insider lives in the network. They may have certain control of cryptographic materials. This enable them to participate in the communication among legitimate nodes in the network [32]. Insiders are usually more powerful than external adversaries.

5.1.3 Single and multiple

There may be just single node being compromised. For example, a greedy driver modified its OBU. There can also be multiple adversarial nodes in the network [32]. As for multiple adversaries, they can act independently or they can collude. If the group of adversaries are fixed during the attack, then they can be viewed as "non-adaptive adversary" [32]. It is also possible that the members in the adversary group change over time. The main adversary in the group can choose which node to compromise. It makes the adversary group an adaptive adversary group [15, 8]. Although the type of collective adaptive adversary exists in theory, it is difficult to become real threat in VANETs. Because in the VANETs, the topology of nodes changes rapidly. The messages broadcasting in the VANETs contain position information. Given a sufficiently dense network, there will be multiple message transmission routes. It will give nodes enough data to determine whether there are wrong messages in the network. If an adaptive adversary group wants to conduct a successful attack targeting one node, the group need to maintain a certain topology. It is very hard in the VANETs. Therefore, according to [15], for multiple adversaries, it is more likely that the group of adversaries act independently.

5.1.4 Analysis of adversaries

First of all, we assume that adversaries have the knowledge about the protocols and algorithms used in the system. What they don’t know is the cryptographic credentials and users’ permanent ID. The limitation of them is that for all adversaries in VANETs, it is believed that they are computational bounded adversaries [32]. This means that the PKI is strong enough to against adversaries in terms of the public key cryptography scheme. Furthermore, with computational bounded adversaries, for legitimate messages in the network, certain amount of noise can be tolerated [50]. The other limitation for adversaries is that it is believed that resources, i.e. memory, that the adversaries can access are limited. This means that it is infeasible for adversaries to collect enough related messages to summarise valuable credentials, for example, secret keys that used in the messages. We need
to assume that it is possible for adversaries to compromise private vehicles, public vehicle even RSUs. However, given such a large scale of the network, the fraction of adversaries in it should be very small.

5.2 Types of attacks

There are a lot of attacks can happen in the VANETs as well as in the normal network. In spite of the rationales behind attacks, sometimes there is even no rationale for some attacks as malicious adversaries, we must consider every possible attacks in the VANETs. In order to have a clear understanding of the attacks in VANETs, we classify them by the targets. There are three main targets for the attacks: messages transmitted in the network, nodes in the network and the networks communications.

5.2.1 Attacks target messages in VANETs

Message tempering is the most common type of attack target message integrity. It includes modification, deleting, forgery etc. They can be more easily conducted by insiders than outsiders, because they have legitimate use of the network services. For outsiders, it maybe very difficult to modify or forgery a message without cryptographic credentials. However, they can still delete the messages. In VANETs, there is a special type of message tempering called message suppression attack [35]. This attack is done by delay the broadcasting of some messages so that the attacker can get benefit from it. For example, as to the parking space searching application, a selfish node may not be willing to broadcast the messages to others so that he can definitely get the parking spot.

It is inevitable that there maybe accidental failure in the network, i.e. omission failure, commission failure and timing failure[32, 49]. If there are certain amount of misbehaving nodes emulate those failures by conducting message tempering attacks, Byzantine failure may occur. It is hard to solve Byzantine fault tolerance problem in VANETs because of the highly dynamic network. However, for the same reason, it is not easy to conduct Byzantine failure either.

Another type of attack may cause malicious message is input controlling. For vehicles in the network, a lots of messages are trigged by the information get from sensors on the car. If the sensors on car are modified, then it enable the OBU to send legitimate but wrong messages.
5.2.2 Attacks target users in VANETs

The most obvious rationale for targeting users is to get their private information. There are two kinds of attacks that may violate users’ privacy: ID disclosure and posting tracking.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\nu_i$</td>
<td>The speed of the target vehicle</td>
</tr>
<tr>
<td>$d_{\text{att}}$</td>
<td>The distance between two attackers</td>
</tr>
<tr>
<td>$d_r$</td>
<td>Transmission range of the target vehicle</td>
</tr>
<tr>
<td>$d_v$</td>
<td>Within the distance that the speed of the target and its driving lane remain unchanged.</td>
</tr>
<tr>
<td>$T_{\text{key}}$</td>
<td>Time interval in which the key can remain unchanged</td>
</tr>
</tbody>
</table>

Table 3: Notations in ID disclosure attack

ID disclosure is proposed in [36]. In this attack, the behaviours of the target car is learned by key correlation. This attack requires certain density of attackers along the road. From the figure 9, the attackers reside by the road. The distance between two attackers (radio receivers) is $d_{\text{att}}$. The target vehicle has transmission range $d_r$. It’s speed is $\nu_i$. The speed and its driving lane remain unchanged within the range $d_v$. This means the vehicle has a predictable vulnerable window. If the vehicle’s public key always remain unchanged, then obviously, the attacker can correlate the public key with the node. However, because the route of the node is predictable, if the key is changed over a small distance, the attacker can still correlate the node with the key. Therefore, the paper define a range of the time interval $T_{\text{key}}$ for changing the key:

$$\min(T_{\text{key}}) = \frac{d_v + 2d_r}{\nu_i}$$

$$\max(T_{\text{key}}) = \frac{d_{\text{att}}}{\nu_i}$$

Figure 9: The ID disclosure attack from [36, 39]
After estimating the real conditions on road, [36] get the time interval which is between 50 to 72 seconds. This means that the life-time of users’ anonymous keys in VANETs is about 55 seconds. Anonymous keys mainly help maintain the level of anonymity in VANETs. However, as mentioned before, in order to change anonymous keys, the certificates of them must be changed as well. The revocation of keys and certificates is difficult issue in VANETs.

The other problem in VANETs may violate privacy is that the users’ position is learned or tracked by malicious adversaries. This may be done by compromise geographic message provider on car. For example, civilian GPS is not secure enough to protect the geographic information for users. There are several ways that can spoof or track GPS informations [6]. The information of users’ position can also be tracked based on the topology of the network [9]. Many parties are interested in users’ position information. For some unethical commercial organisations, the position information of potential consumers may help them make specific target market strategy or, even worse, differential price strategy. For example, an unethical petrol company may link the position information to some customers and then analysis their driving habit. Then they can target these customers for advertisements and promotion, etc [45].

Another type of attack need to be mentioned in this section is that the adversaries try to produce fake identities or impersonate other nodes. As in [14] states, if there are enough resources, it is possible for a faulty entity to produce several fake identities in a network. This type of attack is called as Sybil attack. In VANETs, the nodes have enough computational capability to do cryptographic scheme, therefore, the verification of their identifiers can be done by cryptographic check, i.e. signature.

5.2.3 Attacks target network in VANETs

Denial of Service (DoS) in VANETs can target single node or target part of the network. It can be done by overwhelm a vehicle’s resources or jam the communication channel [35]. DoS may help a greedy user get benefit from preventing other nodes getting some information.

Attackers may also choose to target routing protocol applied in the network [10]. It is still not confirmed by any academic institution or manufactory organisation that which type of routing protocol should be used in VANETs. There are some common attacks aim at routing protocol, such as wormhole attack. As in VANETs,
because the network is highly dynamic, it may be harder for attack to conduct wormhole attack than in other network system.

5.3 Attack tree analysis

Attack tree is invented by Bruce Schneier [48]. Attack tree can help analyse the threats in a system and help to find countermeasures. The attack tree can be presented in a tree structure. The root is the Goal of an attack, leaves are subgoals. As to subgoals, they have two relations, AND and OR. If there is an AND between two subgoals, it means that the attacker mush achieve both subgoals. OR means alternative. Details can be found in [44]. An example of attack tree can be found in figure 10.

![Attack Tree Example](image)

Figure 10: Example of attack tree [3]

As showed in the figure 10, assume someone wants to steal a car. Then he has two ways to achieve it. Get control of keys or start the car without key, i.e. short circuit. In order to start the car and bypass the trouble of getting the key, the attack need to complete three objective. Therefore, the relationship between these three subgoals are AND. The attack tree can also be presented as outline as shown in the figure 10. We are going to outline the attack tree analysis in this paper.

5.3.1 Attacks against cryptographic system of VANETs

As the cryptographic system in VANETs is critical. We are going to analysis the cryptographic system first. This subtree will be used by other attack trees later on.

A Goal: Break the cryptographic system of VANETs
1.1 Break the cryptographic scheme, i.e. ECC (OR)

1.1.1 Solve the discrete logarithm problem on elliptic curve (OR) (I)
   It is believed that discrete logarithm problem on elliptic curve is a
   hard problem. Therefore, we mark it as (I) "Impossible"

1.1.2 Quantum computer (OR)
   Quantum computer is a big threat for every public-key system in
   use. It cannot be marked as (I), because no one can tell when
   the computer can be produced. However, we don’t consider it as a
   serious threat.

1.2 Break the key management system of VANETs (OR)

1.2.1 Break the random number generation scheme (OR)
   By breaking the random number generation scheme, it is possible
   for an attacker to calculate the session key generated by it.

1.2.2 Get keys or unique IDs from TC of OBU or RSU (OR) (I)
   It is assumed that TC will be temper-resistant. Therefore, it is im-
   possible to get keys directly from TC. The unique long-term ID of the
   user is also stored in the TC. The attacker cannot get the ID either
   because of the same reason. As mentioned above, if the attacker can
   get the unique ID, he can ask for legitimate short-term key from CA.
   In this way, he can get control of the valid cryptographic credentials
   as well.

1.2.3 Get keys when it is transmitted or during revocation (OR)
   When the keys and IDs first put into TCs in OBUs, it is done by
   manufactories. It is assumed that the manufactory is trusted. Dur-
   ing the revocation of short-term keys, the credentials is encrypted
   with long-term public encryption key of OBUs, or long-term shared
   secret between CA and OBUs. Therefore, it is very difficult for the
   attacker to get keys when it is transmitted, or during revocation.

1.2.4 Reuse of old keys and certificates (OR)
   For key management perspective, old credentials are important and
   often neglected. Old keys and certificates are valid if the receivers
   don’t check the details on the certificate or CRL. For accountability
   in the network, the credentials maybe kept for a while by CA. It
   must be kept safe.

1.2.4.1 Get access to the old cryptographic credentials
1.2.4.2 Modify the CRL
   An attacker can depend on other users forgetting check CRL. If
he can modify the CRL, then it will make the old keys attack more powerful.

Appropriate using of cryptographic system will prevent a lot of attacks. The most important issue of PKI is the revocation of keys and certificates, especially in VANETs. Therefore, we are going to propose a framework of cryptographic system that can help solving the problem.

5.3.2 Message tempering

We are going to discuss three kinds of message tempering in this network: modification, deleting and forgery. Message tempering is the most basic attack. Many other attacks, such as impersonation, rely on successfully conduct message tempering. Therefore we put emphasis on the message tempering here.

Messages in VANETs are regarded as reliable if they have the following properties: pass the integrity check, from a legitimate user and pass the reputation system check [25]. In order to temper the messages, the attacker must let the message pass all the checks.

1 Goal: Message Tempering in VANETs

1.1 Message modification (OR)

1.1.1 Forgery the signature of the sender
If the attack can successfully forgery the signature of the sender, the malicious message will pass the integrity check and signature check.

1.1.1.2 Break the cryptographic system (OR) (Subtree A)

1.1.1.3 Get other node’s unique long-term ID (OR) (I) (Subtree 0.2.2)

1.1.1.4 Get physical control of OBU (OR)
Get control of OBU not only means that the attacker must get control of others’ vehicle, but also means that the attack can ask OBU to sign the wrong message for him.

1.1.2 Get access to the message

1.1.2.1 Within the transmission range of the message (OR)
It is easier than in other network for a node to get access to messages in VANETs. As in the VANETs, all messages are broadcasted to other nodes. As long as the attacker within the message transmission range, he can get access to the message. There are
two ways to stay within the range depends on the attacker’s target. If he is targeting a specific node, then he may need to follow the car. If he is targeting any node in the network, he can just located by the road.

1.2.2 Wormhole attack (OR) (Subtree C)

Wormhole attack is a kind of MITM attack. The attack will pretend to be a neighbour of a node in the network so that all the messages will pass through the attack. This is a kind of attack that targets the routing protocol of the network.

Above we discussed how to modify the messages transmitted in the system. The most important issue here is to successfully pass the integrity check, i.e. cryptographic check.

1.2 Delete message (OR)

Just simply stop transmitting one message is not actually deleting the message, because all the messages are broadcasting to other nodes. The message may be transmitted by other nodes on the other lane of the highway.

1.2.1 Prevent others from getting the message (OR)

1.2.1.1 DoS on communication channel (OR)

1.2.1.2 DoS on the sender (OR)

DoS attack is a very common attack. It can be done by many different ways. We are not going to discuss it in details.

1.2.2 Make other nodes reject the message (OR)

1.2.2.1 Rate down the sender’s reputation (OR)

1.2.2.1.1 Compromise RSUs (OR)

RSUs is in charge of distribute reputation system information. By compromising RSUs, an attacker may be able to broadcast forged reputation rate of the sender. If the rate is lower than the threshold, other nodes won’t accept the messages from the sender.

1.2.2.1.2 Spoof the messages of the sender (OR)

By constantly spoofing messages of the sender may successfully rate down its reputation value. However, this requires that the attack has control of the sender’s credentials. If the attacker have control of the user’s credentials, he can stop the user’s service by request for revocation. He doesn’t need to wait for the reputation system.
1.2.2.2 Invalid the sender’s signature (OR)

1.2.2.3 Change the position information or clock of sender’s vehicle component (OR)
   By physically damaging geographic information receiver or time information provider on sender’s car, an attacker can actually invalidate every message sent by this node. Because, as we described in the system model, nodes in VANETs only accept fresh messages from front.

1.2.3 Blackhole or greyhole attack (OR) Blackhole means that the attack in the network doesn’t forward any packets. There are also greyhole attack in which the attacker choose what to forward and what are not. This attack will be effective if the density of nodes are low. For example, on a suburban highway, within the communication range of a sender, there maybe only one OBU or RSU.

1.3 Message spoofing (OR)

1.3.1 Get legitimate cryptographic credentials (Subtree)

1.3.2 Get legitimate ID (OR)
   Every node with a car can do it. This can be done by enrolling with authentication centres. There may be several authentication centres. For example, the road and licence registration centre from government and manufactories.

1.3.3 Break the cryptographic system (OR) (Subtree A)

1.3.2 Get into the network

1.3.3 Tempering input messages
   By tempering sensors, the OBU will sign legitimate but wrong messages. Although it seems hard to be detected, this kind of insiders can be removed by reputation system.

1.3.3.1 Get physical access to the sensors
   Because this attack requires physical access to the vehicle, it is more likely to be conducted by the owner or machinist. This makes this kind of attack traceable.

1.3.3.2 Tempering the sensors

5.3.3 Position tracking

In this part, we are going to focus on tracking problem. It is not about physically tracking the node on road. The attack is going to be done remotely take advantage
of the vulnerability in the network.

2 Position tracking

2.1 Link ID with the user

Every node in the network has anonymous IDs. The unique IDs are not going to be used in the communication of the network. What other nodes can see is the anonymous ID which is going to be changed every day at least. According to [36], it should be changed every minute. The anonymous ID is going to be used at every layer of the network [34].

2.1.1 ID disclosure attack (OR)

As discussed before, ID disclosure attack is able to link anonymous ID with users if the ID doesn't change within short time interval.

2.1.2 Get the user's unique ID (OR)(I) (Subtree 0.2.2)

2.2 Monitor the user

2.2.1 Get position information of the user from its messages

Position information is going to be added in every message of the node. The attacker need to get messages from the target to identify its position.

2.2.2 Place enough monitors by roads (OR)

The monitors can be some compromised RSUs or radio receivers.

2.3 Hack into its geographic information receiver (OR)

Geographic information equipment on vehicles is vulnerable to hack [6].

Position tracking is an important issue in VANETs. It is not only about the privacy of users, but also threat homeland security. If the attack is successfully conducted by terrorists, people’s lives will hang by a thread. The position tracking problem may be solved by anonymous keys as analysis in the attack tree. However, we still need to solve the problem of revocation of ananymities.
6 A certificateless cryptography based framework for VANETs

6.1 Motivation

Encryption and signature provide confidentiality, acceptability, authentication and integrity in VANETs [2]. Cryptographic system is vital for the network. As analysed in subtree A, ECC is a fast and low computational overhead scheme, at the same time provide high security. Given the scenario of VANETs, ECC is a suitable solution. However, in order to achieve anonymity in the network, it is necessary to change public keys and certificates after about every minute. No mechanism has been suggested in IEEE 1609.2.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>A user in the CL-PKC</td>
</tr>
<tr>
<td>$i$</td>
<td>user $i$ in the VANETs</td>
</tr>
<tr>
<td>params</td>
<td>The public parameters of KGC</td>
</tr>
<tr>
<td>$e$</td>
<td>A bilinear map used in CL-PKC</td>
</tr>
<tr>
<td>$G_1$</td>
<td>An additive group of generator $P$</td>
</tr>
<tr>
<td>$G_2$</td>
<td>A multiplicative group with prime order $q$</td>
</tr>
<tr>
<td>$P$</td>
<td>The generator of additive group $G_1$</td>
</tr>
<tr>
<td>$q$</td>
<td>The prime order of multiplicative group $G_2$</td>
</tr>
<tr>
<td>$H_1$</td>
<td>The hash function used by KGC to produce partial-private-key $D_i$</td>
</tr>
<tr>
<td>$H_2$</td>
<td>The hash function that is used for encryption by users</td>
</tr>
<tr>
<td>$D_i$</td>
<td>Partial private key</td>
</tr>
<tr>
<td>$s$</td>
<td>Master key of KGC</td>
</tr>
<tr>
<td>$x_i$</td>
<td>Secret value selected by user $i$</td>
</tr>
<tr>
<td>$Q_i$</td>
<td>Identifier of user $i$</td>
</tr>
<tr>
<td>$S_i$</td>
<td>Private key of user $i$</td>
</tr>
<tr>
<td>$P_i$</td>
<td>Public key of user $i$</td>
</tr>
<tr>
<td>$M$</td>
<td>Plaintext</td>
</tr>
<tr>
<td>$M$</td>
<td>Plaintext space</td>
</tr>
<tr>
<td>$C$</td>
<td>Ciphertext</td>
</tr>
<tr>
<td>$C$</td>
<td>Ciphertext space</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>random number generated by KGC</td>
</tr>
</tbody>
</table>

Table 4: Notations in the introduction of a certificateless cryptography based framework for VANETs
6.2 Introduction of the certificateless cryptography

The certificateless public key cryptography (CL-PKC) is introduced by [4]. It was developed based on the idea of identity-based cryptography (ID-PKC). [20] proposed an ID-PKC based security framework for VANETs. It help solve the problem of anonymous key and certificate revocation problem. After considering the pros and cons of both cryptography system, we propose the CL-PKC for the following reasons. Firstly, just same as ID-PKC, CL-PKC doesn’t need certificate for receivers to verify a public key. There is an advantage compare to ID-PKC: the authorities can’t generate users’ private keys. In the CL-PKC, key pairs can be generated by users locally after getting a partial-private-key $D_i$ from authority. This means that less computational power is required for the authorities. This enable the complex RSUs become authorities in CL-PKC. Moreover, because the CA in ID-PKC is able to generate all the secret values of all the users in the system, the compromise of CA’s master key will cause the collapse of the whole system. Therefore, the application of ID-PKC is restricted to small, closed groups or those with limited security requirements [4]. As a contract, VANETs is a very scaleable network and have safety related applications. This makes CL-PKC more suitable for VANETs.

In order to explain the CL-PKC framework, we need to introduce how the CL-PKC scheme work. Following settings are from [4]. There is a map $e : G_1 \times G_1 \rightarrow G_2$ where $G_1$ is an additive group of generator $P$ and $G_2$ is a multiplicative group. They have the same prime order $q$. The map $e$ has following properties:

1. The map $e$ is bilinear: given $Q, W, Z \in G_1$, we have

$$e(Q, W + Z) = e(Q, W) \times e(W, Z)$$

and for any $a, b \in \mathbb{Z}_p$, there is

$$e(aQ, bW) = e(Q, W)^{ab} = e(abQ, W)\text{etc},$$

2. The map $e$ is non-degenerate which means $e(P, P) \in 1_{G_2}$,

3. The map $e$ is efficiently computable.

There are two similar schemes was introduced in [4], the basic CL-PKC and full CL-PKC. In order to have a quick feeling of the scheme, we will introduce the basic mode. In the CL-PKC, there are two roles, the authority and user, noted as Key generation centre (KGC) and $A$ respectively. Every user has a unique identifier $ID_A \in \{0, 1\}^*$. The notation means that the identifier can have any length consist
of 0 or 1.

There are two hash functions in the basic mode chosen by KGC: \( H_1 \) for KGC to produce partial-private-key, \( H_2 \) is used for encryption by users. There are two steps need to be done by KGC:

1. **Setup**: Select a Master key \( s \) randomly from \( Z^*_q \) and set \( P_0 = sP \). Public system parameters \( \text{params} \): \( G_1, G_2, e, n, P, P_0, H_1, H_2 \), where \( n \) is the allowed bit-length of plaintext: \( M = \{0, 1\}^n \). The ciphertext space will be: \( C = G_1 \times \{0, 1\}^n \). Publish \( \text{params} \).

2. **Partial Private Key Extract**: Calculate \( Q_A = H_1(ID_A) \). The partial private key \( D_A = sQ_A \). Then send \( D_A \) to user \( A \).

The following steps are done by user \( A \):

1. Check \( e(D_A, P) = e(Q_A, P_0) \), if true, accept \( D_A \) as his partial private key.

2. **Set Secret Value**: Select secret value \( x_A \in Z^*_q \) at random with referent to \( \text{params} \) and \( ID_A \)

3. **Set Private Key**: Computing private key \( S_A = x_AD_A = x_AsQ_A \)

4. **Set Public Key**: Computing \( X_A = x_AP \) and \( Y_A = x_AP_0 = x_AsP_0 \), the Public key \( P_A = (X_A, Y_A) \).

5. Publish \( Q_A \) and \( P_A \)

If a user wants to send message to \( A \), he will first check \( e(X_A, P_0) = e(Y_A, P) \). This step is equivalent to checking certificate in normal PKI. Ciphertext

\[
C = (U, V) = (rP, M \oplus H_2(e(Q_A, Y_A^r)))
\]

where \( r \) is a random number chosen by the sender.

For decryption just compute

\[
M = V \oplus H_2(e(S_A, U))
\]

The detail of CL-PKC and signature scheme can be found in [4].
6.3 Framework description

In VANETs, every node has a unique ID. It can be used to generate identifier $Q_i$ for nodes in the network. The KGCs in VANETs need to be stay locally instead of a central authority. This is because the information of KGC may reveal user’s ID. For example, if a user in England has published the params from a KGC located in German, it can be concluded by an oberserver that the anonymous key pairs issued by the German KGC belong to the same node. Therefore, it is better to have local KGCs. As mentioned before, complex RSUs (RC) can be used as local KGC. KGC need to have its own params. It can be computed in advance. KGC is authorised by central authority. Therefore, KGCs need to publish its own identifier $Q_{RC}$ and $P_{RC} = (X_{RC}, Y_{RC})$, as well as the authority’s params.

The unique ID of every node in the network is given by authority. When node $i$ wants to have anonymous keys, it must send $ID_i$ to KGCs. This can be done by encrypted its ID use KGC’s public key. The process of generate anonymous keys shows as following:

1. Check $e(X_{RC}, P_0) = e(Y_{RC}, P)$, if true, ask this KGC for anonymous keys.
   This check is for the user $N_i$ to confirm whether the RSU is a legitimate one.
   User check the public key of the RSU with the $params : P_0, P$ of the CA who certify the RSU. The long-term $params$ of CA can be preloaded to user’s OBUs in advance.

2. $N_i → RSU: Geo_i || TS_i || En_{(P_{RC}, Q_{RC})} \{ID_i\}$
   After confirming that the RSU is a legitimate one, $N_i$ sends its permanent unique ID to RSU together with his geographic information and timestamp. The unique ID is encrypted with the RSU’s public key.

3. At KGC: check $ID$ with backend authority through authenticated channel. If true, computer $Q_i = H_i(ID_i, γ) ∈ G_1$, where $γ$ is a random number generated by KGC. Then compute the partial private key for $N_i$, $D_i = sQ_i$.

4. $KGC → N_i : En_{P^i_i, Q^i_i}(Q || D || TS || params || Sign_i)$, where $P^i_i$ and $Q^i_i$ are old public key of user$_i$. The new $Q_i$ and $D_i$ together with $params$ of RC are encrypted by $N^i_i$’s old public key. The $params$ are needed for verification of the user’s public key by other nodes in the network.

5. KGC report the action to CA: $KGC → CA : TS || En_{SK_{CA}} \{ID_i, Q_i\}$
   After getting the unique $ID_i$ and identifier $Q_i$ of user $N_i$, the backend system is able to trace back to the user. This step provides the acceptability for the system.
6. $N_i$ computes $P_i$, then publish new public information $Q_i$, $P_i$ and $\text{params}_{RC}$. With one $D_i$, the node can generate several key pairs.

Comparing to the normal CL-PKC, for VANETs, the identifier $Q_i$ is computed by KGC then send to CA. In this way, CA is able to keep the audit trail. In order to check whether the KGC is a legitimate one, there must be a list of all authorities' $\text{params}$. It can be stored in advance in OBUs. Because CA's $\text{params}$ can be regarded as long-term credentials, the revocation of them can be done by vehicle-to-home communication through local network. The accountability is achieved by the $ID_i$ and $Q_i$ pairs stored in database at backend.

6.4 Analysis

6.4.1 Security analysis of the framework

Non-repudiation is the strongest requirement in authentication. If non-repudiation is achieved, message authentication is also achieved. As to the CL-PKC framework, because there are no one else, even not the authorities, knows about the private key of user, the user cannot deny the signature he signed. Because the temporary ID $Q_i$ is calculated and given by the authority, the signer can't deny his identity. Therefore, this framework provides non-repudiation. The identifier $Q_i$ is temporary used by the user. It is the anonymous that can be used to maintain anonymity.

6.4.2 Advantages

The advantage for this method is, firstly, by applying CL-PKC there is no need for certificates. Secondly, the KGC just need to do a very easy calculation for computer the $Q_i$ and $D_i$, thirdly, nodes can generate key pairs after getting $D_i$ form KGC. However, there are still some problems that need to be considered. Firstly, if regard $Q_i$ as the information that can be tracked by observers, it means that $Q_i$ need to change every couple of minutes. This can be solved by computing several $Q_i$ and $D_i$ at a time and send them all to the node. The node can choose when to use it by computing corresponding $P_i$ locally. The second problem is that when a node is compromised, it can computer legitimate key pairs as many as possible. The solution to it depend on the reputation system. Because of the TC in OBUs, it is believed that the cryptographic credentials cannot be learned by anyone. It is hard to prevent the car generating legitimate key pairs and send legitimate messages. However, with reputation system, if the node has too many misbehaviours, it will rate down the node’s reputation. The most serious problem is that if a KGC was compromised. This may cause two problems: one is that the ID information of nodes may be exposed, the other is that it can generate malicious nodes with right
cryptographic credentials. This has the same influence as in the normal PKI that if a CA is compromised. Therefore, we regard it has the same level of security as CA in normal PKI.
7 Conclusion

VANETs is a huge and difficult project for academic, industry and government. However, they all want to realise it because they can see the tremendous benefit from the system. It is not only for people’s safety, efficiency and convenience, but also for business opportunities and homeland security. People want a practical and almost invulnerable system. That’s why the development of VANETs is so cautious.

7.1 Our contribution

In this project, we have accessed to a large amount of literatures. Summerized the character and security requirements of VANETs. We built a model of the system and conduct an attack tree analysis of the major threats in the network. After all the previous work, we are able to propose a CL-PKC framework for VANETs system in order to help solve the revocation problem of the network.

7.2 Future work

VANETs has been developed for almost a decade, but it still stay in theory. There is no agreement on almost every practical issues of VANETs. This is not only because of the technology, engineering and society difficulties, but also because of the complex issues in security aspects. The future work in security of VAENTs can be the development of revocation system of the network, the reputation system mechanism.
References


[5] ASTM. Standard specification for telecommunications and information exchange between roadside and vehicle systems 5 ghz band dedicated short range communications (dsrc) medium access control (mac) and physical layer (phy) specifications. Technical report, ASTM E2213 - 03, September 2010.


[34] Panagiotis Papadimitratos, Antonio Kung, J-P Hubaux, and Frank Kargl. Privacy and identity management for vehicular communication systems: a position


[41] RITA. How did the federal its program become established, 2013.

[42] RITA. What are the current key activities of the federal its programme, 2013.


