NTNU – Trondheim
Norwegian University of
Science and Technology

Identity management on VANETS

Ephraim Alemneh Jemberu

Master of Telematics - Communication Networks and Networked Services (2
Submission date: August 2012
Supervisor: Van Thanh Do, ITEM

Norwegian University of Science and Technology
Department of Telematics

NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY, MATHEMATICS AND ELECTRICAL ENGINEERING

Research on Identity Management in VANETs

Ephraim Alemneh Jemberu

Master of Science in Telematics
Submission Date: August 2012
Supervisor: Professor Van Thanh Do, ITEM

Norwegian University of Science and Technology
Department of Telematics

ABSTRACT

Vehicular ad-hoc networks (VANETs) have envisioned various applications that substantially improve traffic safety and efficiency along the roads and highways. There are on-going projects to standardize VANETs and to start off their real-life deployment. Despite the huge benefits envisioned by VANETs, they cannot be readily deployed due to serious security and privacy concerns. These security and privacy concerns should be addressed and thus VANETs require a sound Identity management architecture before their anticipated deployment.

Current research efforts on Identity management (IdM) in VANETs focus on employing Public Key Infrastructure (PKI) schemes to offer the well-known security and privacy requirements for VANETs. However, identity management is a far broader concept than offering security and privacy requirements.

This thesis proposed a novel Identity management (IdM) architecture for VANETs that makes a distinction between identity of the driver and the vehicle. To the best of our knowledge, our architecture is the first one to make such a distinction. Smartphones are used for establishing the identity of the driver while the IP Multimedia Subsystem (IMS) is used as an identity provider by establishing an OpenID provider within IMS. To preserve anonymity of users and to avoid location tracking, we tweaked OpenID so that it assigns different pseudonym OpenID identifiers for each user. Finally, we showed how our architecture can be used to realize interoperability across different VANET domains even in the absence of trust relationship among them.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Firstly, I am deeply indebted to my advisor, Professor Do van Thanh, for his support and for offering me a full freedom to explore my interest within the VANET IdM domain. Last, but not least, I praise God for the mercy that He has been bestowed upon me during my study, and indeed, throughout my life.

CHAPTER 1

INTRODUCTION

1.1 Overview

Traffic safety is a prime challenge that has to be addressed by automotive industries, governments and other concerned entities. According to reports by World health Organization (WHO) about 4 % of death toll is caused by traffic accidents in some industrialized countries [10]. Traffic jams are still costing many work commuters a considerable part of their golden time. All these have initiated both academia and industries to put their effort on tackling the problems related with traffic safety. On top of traffic safety, offering services such as in-vehicle internet access, traffic information, entertainment, payment services and many more services, to increase the drivers' driving experience is also envisioned by these research efforts.

Traffic accidents usually happen as the driver is not able to determine road situations and take appropriate actions in real-time. Mostly drivers do not have a complete picture about road conditions at given instance and they will make decisions such as breaking and lane changing in the absence of full information. This in turn is the main cause for accident occurrence. Real time communication among vehicles and road-side units can help the driver to have full information on road conditions and this will enhance traffic safety and efficiency. A vehicular ad hoc network (VANET) is a network that enables real-time communication between vehicles and road-side units.

VANET is an enabling technology for Intelligent Transportation Systems (ITSs). A typical VANET network comprises an on-board unit (OBU) installed on each vehicle, road-side units (RSU) deployed along the roads and trusted authority (TA) that control the network. TAs usually have many application servers at the backend of the network. The OBUs and RSUs communicate over the wireless channel using the Dedicated Short Range Communications (DSRC) protocol. On the other hand, the RSUs, TA, and the application servers can communicate using secure fixed network such as the Internet.

1.2 Motivation

IdM in VANETs is a major challenge that should be solved before deploying VANETs across the roads and highways. VANET inherits all of the challenges that are present in traditional IdM system but at the same time it brings a new set of challenges that are unique to it. A typical IdM architecture should offer privacy, pseudonym management, and effective identity life cycle management. In literature, there are many IdM proposals for VANETs. However, most of the proposals only offer the basic security requirements for VANETs: confidentiality, integrity and availability.

1.3 Contribution

In this thesis, we proposed a novel IdM architecture for VANETs. Our architecture satisfies the security and privacy requirements such as authentication, anonymity, unlinkability, and traceability. Our proposal, unlike other proposals, makes a distinction between the identity of a vehicle and a driver. The IP Multimedia Subsystem (IMS) and OpenID are the main cornerstones of our architecture.

1.3 Content Outline

The remainder of this thesis report is organized as follows:

- Chapter 2 presents background information on vehicular networks.
- Chapter 3 surveys identity management in VANETs.
- Chapter 4 gives a brief introduction to OpenID as it is one of the essential components in proposed IdM architecture.
- Chapter 5 analyzes the existing IdM proposals and identifies their limitations.
- Chapter 6 presents the proposed IdM architecture.
- The final chapter draws a conclusion and gives recommendations for future work.

CHAPTER 2

BACKGROUND ON VEHICULAR AD HOC NETWORKS

2.1 Introduction

Vehicular Ad-hoc Network (VANET) is a network in which Vehicles (equipped with wireless communication capability) can directly communicate with each other and with road side infrastructures. The idea is then to create both safety applications and non-safety applications that enhance the driving experience of a driver, on top of the network.

A vehicular ad hoc network comprises three main network entities as shown in Figure 1. These components are the Road Side Unit (RSU), Vehicles (Users) and Trusted Authority (TA). Let us describe the three entities briefly.

1. Road Side Unit (RSU)

RSU is a static component that serves as a gateway to a VANET and also allows connection to the Internet. It is involved in traffic associated Vehicle-to-Roadside Infrastructure (V2I) communication. RSUs are the main tools used by authorized authorities to carry out some administrative tasks such as solving disputes.

2. Vehicles or Users

The vehicles and the users are closely related in VANET context. The relationship between users and vehicles can come in three different roles. A given user may be an owner, a driver or a passenger to the vehicle in question. Usually there is a many-to many association between the vehicle and the user role, but at a given instant of time, only one

user is a driver. It is worth mentioning that the driver role is more important than the others because he is the one controlling the vehicle in the VANET. Each vehicle is equipped with a tamper resistant trusted component. This component can be installed during the manufacturing process (for recent model vehicles) and if the component is not installed by the manufacturer, users can buy and install it later.

3. Trusted Authority (TA)

TA is an essential entity in VANETs which provides identity for vehicles and monitors the network. TA is responsible to solve any dispute that happens in the network. It is not yet clear who should take the role of TA when VANETS are deployed to start operation. There are many possible candidates for TA: current road and transport authorities, automobile manufacturers, trusted third parties or a combination of them.

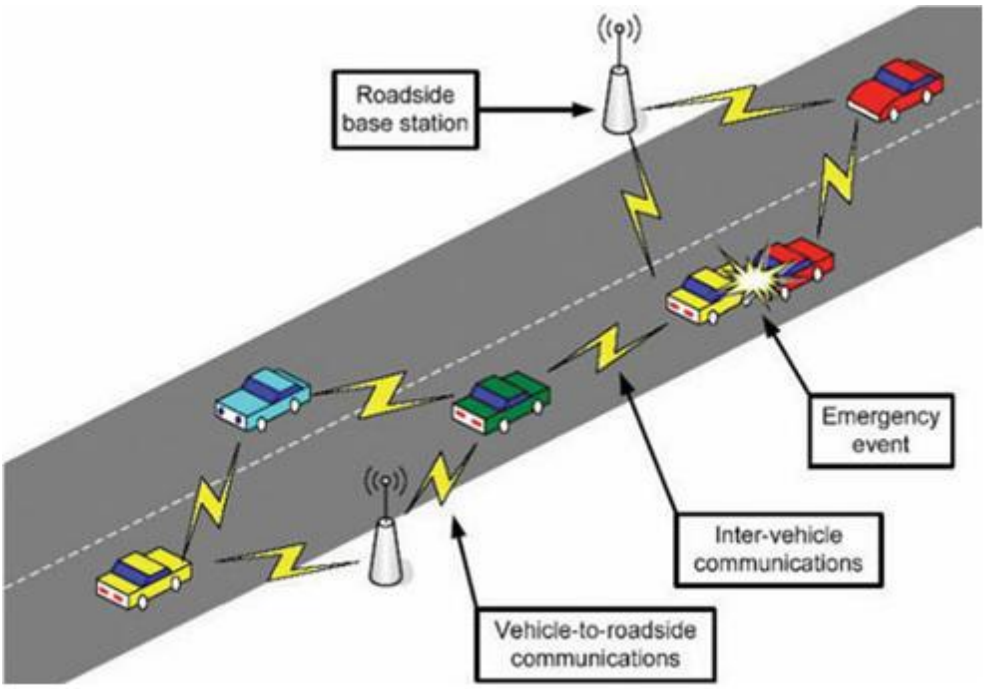

Figure 1 Vehicular Network Architecture [1]

There are two main types of communication in VANETs: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Roadside Infrastructure (V2I) communication. In V2V, a vehicle exchanges message with other vehicles. In V2V communication, all the vehicles engaged in the communication are mobile. V2I communication refers to a type of communication that involves Road Side Units (RSUs). This communication is usually used to get in contact with other networks such as Internet. For V2I, technologies such as WLAN, DSRC, WiMAX, cellular and satellite can be used. Figure 2 depicts the communication schemes in VANETs.

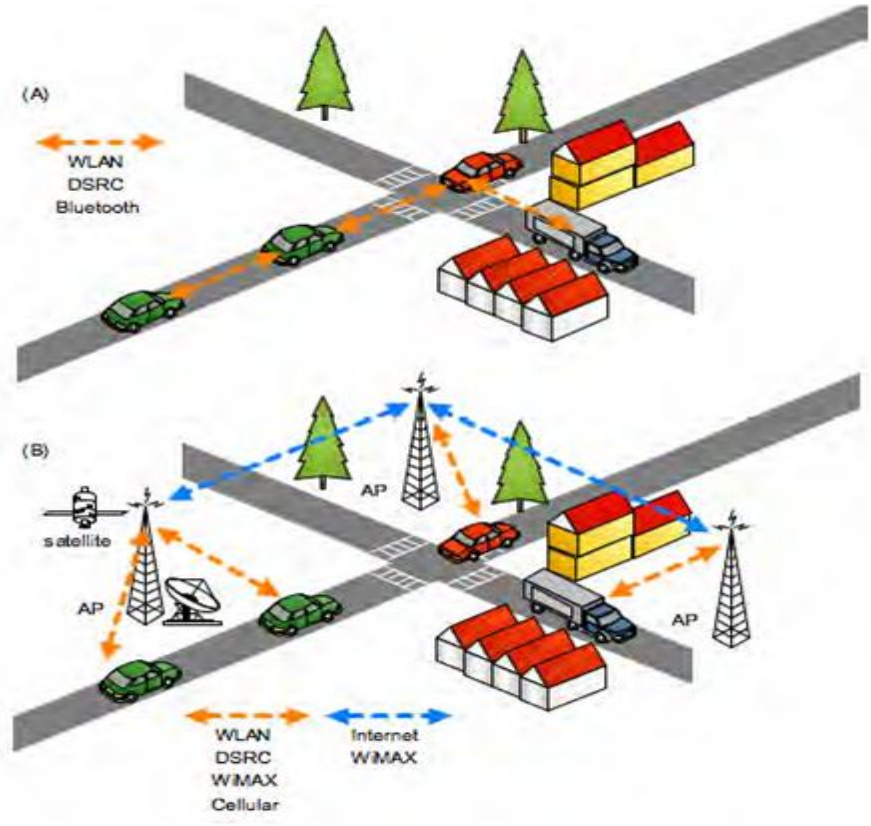

Figure 2 Communication schemes in VANETs, (A) Vehicle-to-Vehicle (V2V), (b) Vehicle-to-Infrastructure (V2I) [2]

2.2 Communication Patterns in VANETS

Schoch et.al. [3] classified communication patterns in VANETs in to five categories. Their classification is generic and independent of the employed underlying communication technology. We briefly present these communication patterns.

1. **BEACONING**

Beaconing is a periodic transmission of packets as a link layer broadcast to nearby vehicles or road-side units. The purpose of beaconing is to inform all neighboring nodes about the current status such as position, speed and heading direction of the sending vehicle. Beaconing is typically a single hop communication and thus the packets are not forwarded.

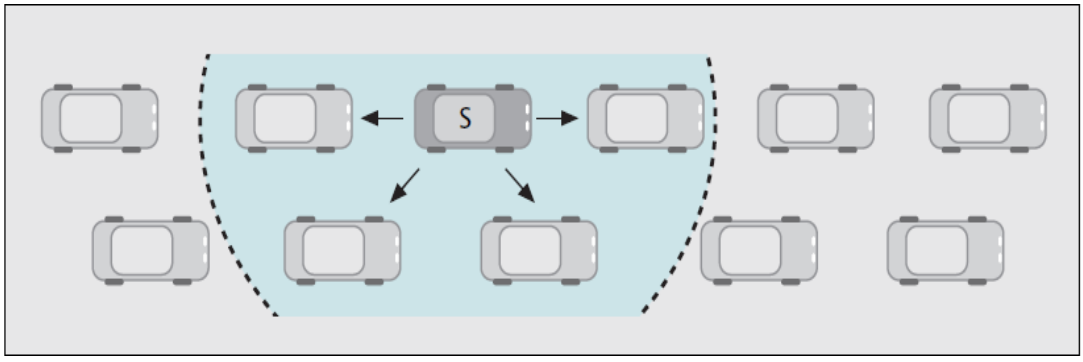

Figure 3 Beaconing in VANETs [3]

2. **GEOBROADCASTING**

It is a communication mechanism that distributes information to a given geographical region. The basic idea is to set the destination region and attach it to the message to be sent. The sender then broadcasts the message to its neighbor. Every

vehicle that receives a geo broadcast message will forward the message unless it is the end point of the specified region in the message.

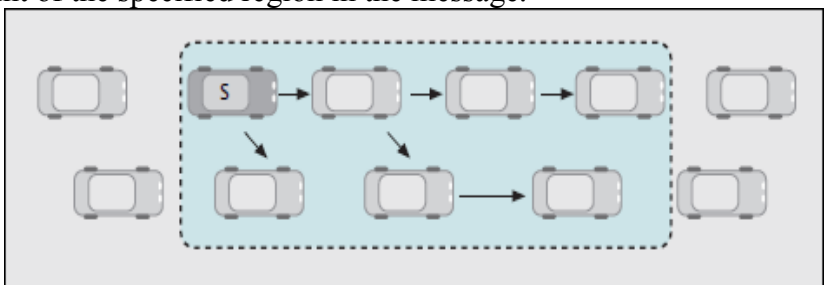

Figure 4 Geobroadcasting in VANETs [3]

3. UNICAST

In certain cases a vehicle may want to send a message that is only destined to a specific single vehicle or RSU. This is where the use of unicast messaging becomes useful. For example, Vehicular social network is one of the envisioned applications in VANETs. The idea is to allow vehicles to form a trusted network. Unicast routing is essential in this type of applications. The communication can be single hop if the communicating parties are neighbors otherwise a proper routing mechanism is required to deliver the message to the receiver.

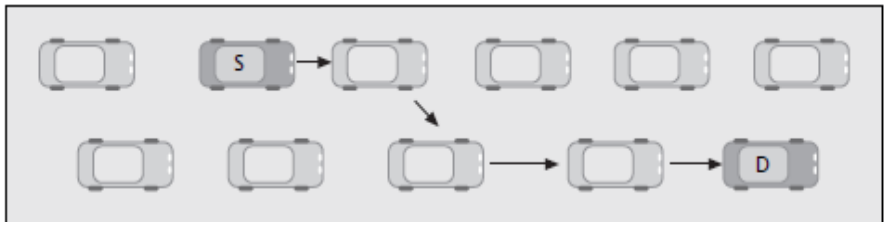

Figure 5 Unicast messaging in VANETs, Vehicle S sends message destined for vehicle D [3]

4. Advanced information dissemination

Information dissemination is one of the challenging tasks in VANETs as the network topology changes more frequently due to higher moving velocity of vehicles. The main aim of this communication pattern is to ensure that vehicles that arrive late or were unable to receive previous messages because of network partitioning get the message. Single-hop broadcasts, store messages, and multiple forward is used in this communication pattern.

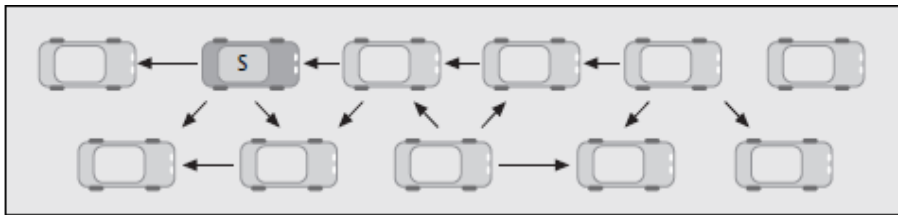

Figure 6 Advanced information dissemination [3]

5. INFORMATION AGGREGATION

In this communication pattern communicated data is processed and merged before being forwarded. The main aim is to reduce overhead communication and to increase reliability of the exchanged data. For some applications like traffic jam reporting information aggregation results in better accuracy.

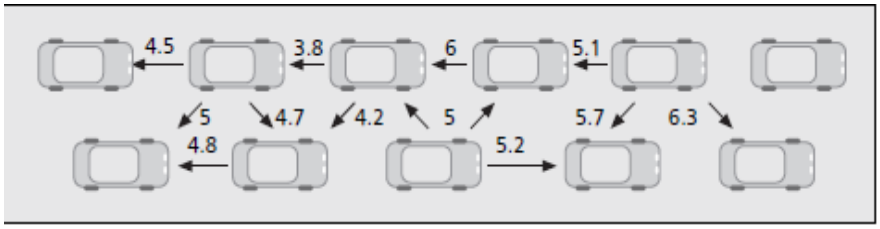

Figure 7 Information Aggregation [3]

2.3 VANET Standards

In this section, we present wireless network standards related to VANETs.

2.3.1 Dedicated Short Range Communication (DSRC)

Dedicated Short Range Communications (DSRC) is a short to medium range communication service that supports V2V and V2I communications. The special features of DSRC are large radio range (with line-of-sight distance of less than 1000 meters), multi-channel usage, and high speed transmission rate between 3 to 54 megabits per second.

Organizations that are involved in DSRC standardization include ASTM (American Society for Testing and Materials), CEN (European Committee for Standardization), and ARIB (Association of Radio Industries and Businesses). The standards set the frequency, bandwidth, channel numbers, transmission rate, and transmission coverage of DSRC, as shown in Table 1[4, 5].

Criteria	North America	Europe	Japan
Standard	ASTM	CEN	ARIB
Frequency band	5.850-5.925 GHz	5.795-5.815 GHz	5.770-5.850 GHz
Bandwidth	75MHz	20MHz	80MHz
Channels	7	4	Downlink: 7 Uplink: 7
Channel separation	10MHz	5MHz	5MHz
Transmission rate	3-54Mbps	Downlink:500Kbps Uplink: 250Kbps	1-4Mbps In ETC is 1Mbps
Transmission coverage	1000 meter	15-20 meters	30 meters

Table 1 DSRC standard in North America, Europe, and Japan

2.3.2 WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS (WAVE) STANDARD

Wireless Access in Vehicular Environment (WAVE) is defined by a suite of IEEE P1609.*x* standards that deals on the WAVE architecture and communications models, network protocols, security mechanisms, and Physical Layer access. Four of the IEEE 1609 family of standards are trial-use standards (IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, and IEEE P1609.4) while the rest two are unpublished standards (IEEE 1609.0 and IEEE 1609.11).

- IEEE 1609.1 [6] "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager" describes the management activities required for the proper operation of the applications.
- IEEE 1609.2 [7] "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and

Management Messages" describes secure message formats, security mechanisms and processes.

- IEEE 1609.3 [8] "Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services" details services in network and transport layer. It also describes addressing and routing for secure WAVE data exchange.
- IEEE P1609.4 [9] describes the enhancements to 802.11 MAC to support WAVE.
- IEEE 1609.0 [5] describes the WAVE architecture and services that enable multi-channel DSRC/WAVE devices to communicate in VANETs
- IEEE P1609.11 [5] envisions to design to standardize essential security services and message format to support an electronic payment system.

2.4 Types of Applications in VANETs

Many potential applications can be covered in VANETs. Here is the description of some of them [11].

1. Safety applications

Safety is the major driving force that initiated the research efforts in VANETs. Safety applications closely monitor events such as weather and road conditions and report them to the vehicles via a broadcast message. Since such messages are critical, security mechanisms have to be employed to keep their integrity and to check their origin. Example applications in this category are:

a) Slow/Stop Vehicle Advisor

A vehicle must broadcast warning messages when it is slow or stationary.

b) Emergency Electronic Brake Light

This application is essential to avoid crash. The immediate two cars might not prevent the crash but all the subsequent cars can escape from the crash.

c) Post-Crash Notification

A vehicle that already experienced an accident t broadcast a warning message that contains its current position to its neighbors. It also sends the message for involved authorities.

d) Road Hazard Control Notification

This application notifies vehicles in its surrounding when it encounters road hazards such as landslide, road curves and sudden downhill.

e) Cooperate Collision Warning

This application is supposed to send a warning message for vehicles which are going towards a collision.

2. Convenience Applications

These applications, which are not related with safety, offer drivers with better driving experience at the same time they maximize the traffic efficiency. Some example applications in this category are:

a) Congested Road Notification

Traffic congestion is a main threat in many cities that wastes users' valuable time. These applications detect road congestion and inform to vehicles so that a driver can take another route.

b) Toll booth collections

These applications make tollbooth collection easy and they do not require the vehicle to stop for collection.

c) Parking availability Notification

This application assists the drivers by suggesting empty parking slots in a given surrounding.

3. Commercial Applications

There is a room for service providers to introduce applications that benefit drivers and road authorities. These applications can range from commercial advertisements to location based services. Some example applications in this category are:

1. Remote Vehicle Personalization/ Diagnostics

These applications shall enable remote vehicle diagnostics.

2. Service announcements

There are already existing businesses in the highways such as petrol stations and shops. This application enables such businesses to advertise their services and offers for drivers when they are on the road.

3. Real Time Video Relay

Drivers can get access to real time videos of their choice while they are on the road. The list is not exhaustive and it is likely to see many commercial applications many commercial applications offered on VANETs in the coming years.

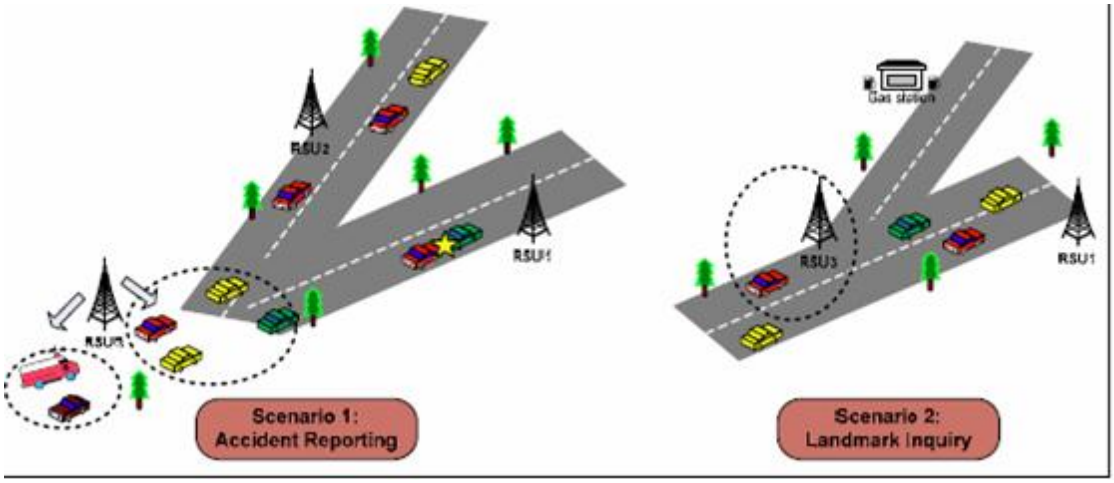

Figure 8 Example applications in VANETs adopted from [12]

2.5 Security Threats

There are many possible attacks that an attacker can launch in VANETs. In this section, we describe some of them.

1.Denial of Service (DoS) [13, 14]

DoS is a serious threat that is posed in VANETs. The main aim of this attack is to overload the communication channel in order to disrupt the normal functioning of the network. This in turn will prevent critical message from reaching to the desired party. The consequence of this attack can be catastrophic in VANETs as safety related message may be prevented to reach to the vehicles as stated in [13] and shown in Figure 9, DoS can be easily accomplished by jamming the network with a little effort and transmission power.

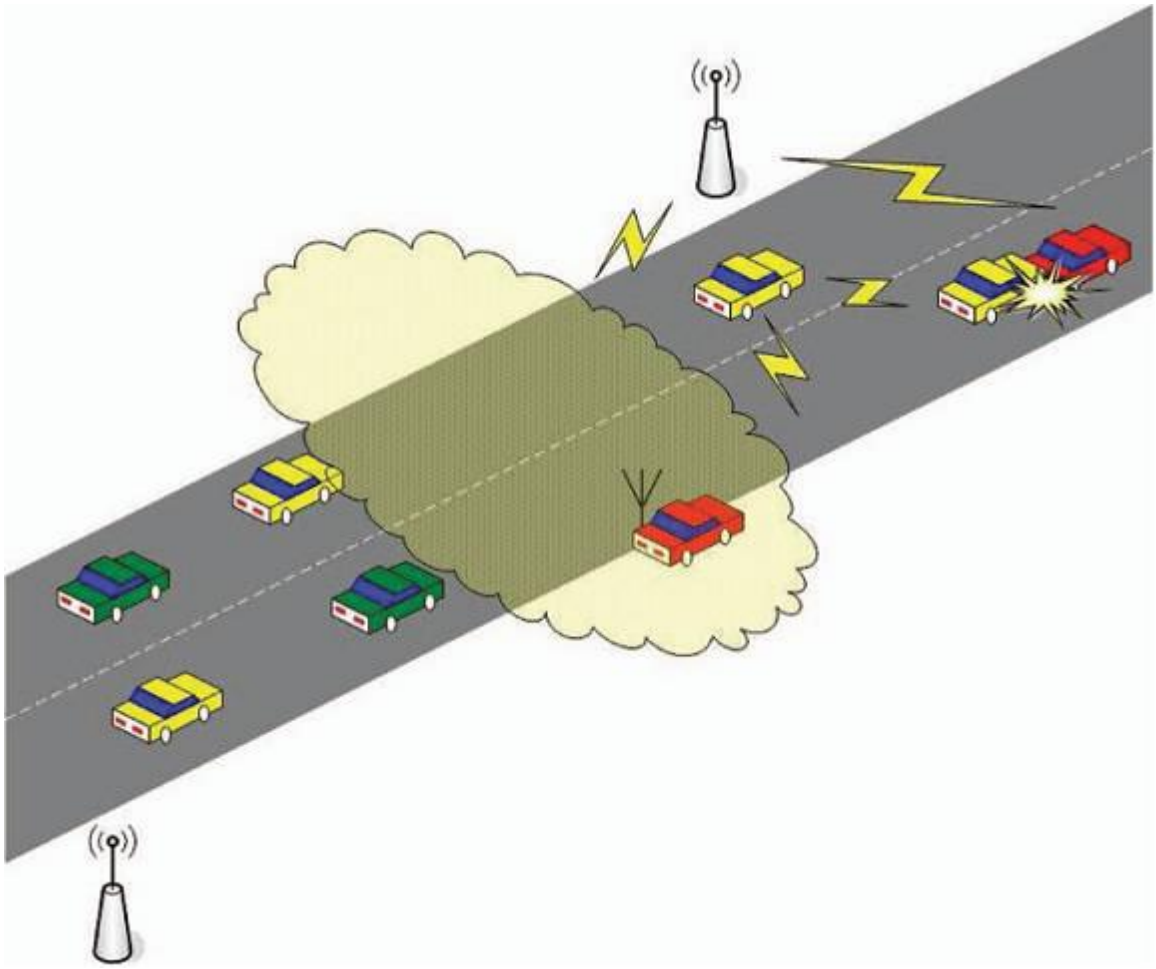

Figure 9 A jamming DOS attack [13]

2.Message Suppression Attacks [14]

A malicious driver may carry out this attack be selectively dropping packets (that were destined for other vehicles) from the network. A greedy driver may use this attack when she receives congestion notification. Instead of passing this message around for the neighboring vehicles, she may drop it to find a better route for herself.

3. Forgery Attacks [13]

An adversary can makeup false information and broadcast it to the network. For instance a driver may fake her vehicle as an emergency vehicle to gain a speed advantage. Counter attacking this attack, while keeping the privacy of the vehicles in the network is very challenging. Figure 10 shows a rapid propagation of fabricated false information from a single malicious driver.

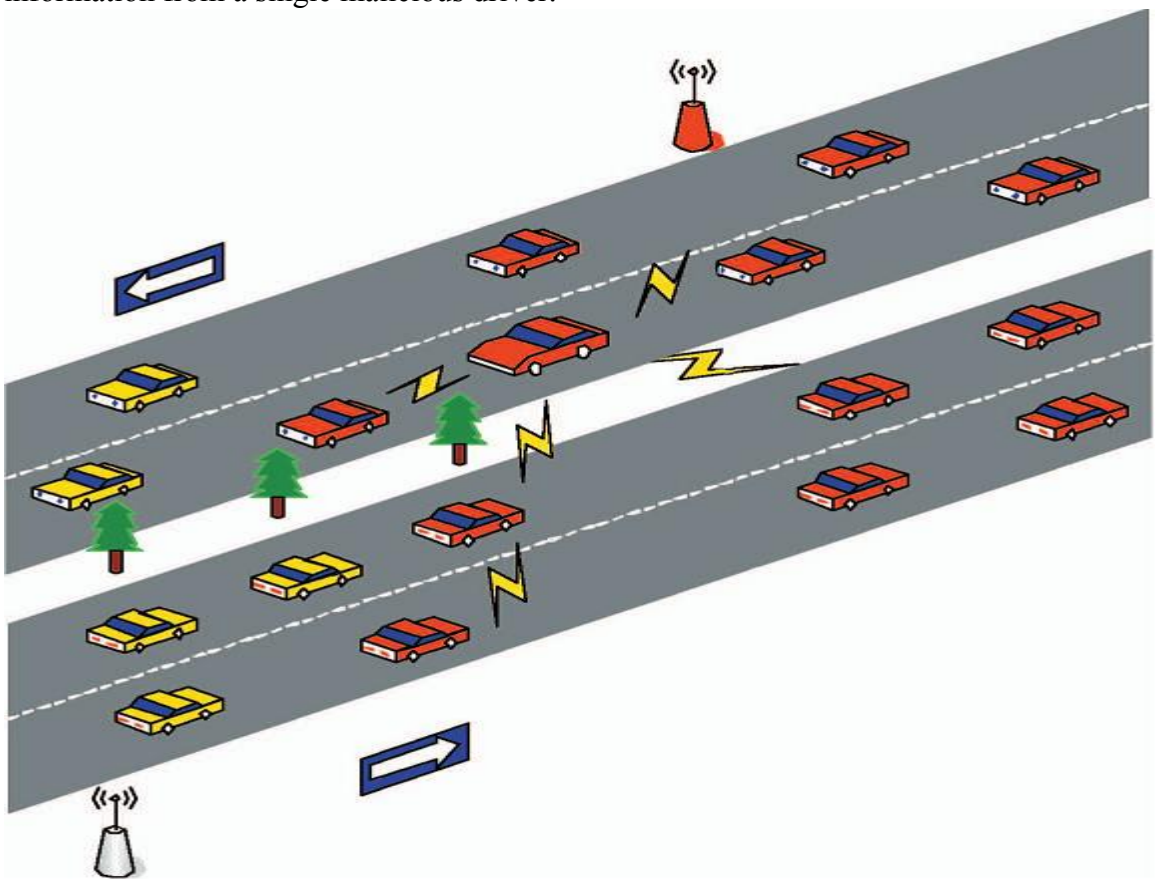

Figure 10 Message forgery attack [13]

4. Alteration Attacks [14]

An adversary may deliberately alter a message. Moreover, she may delay the transmission or replay a message from earlier transmission.

5. On-board Tampering [13]

The adversary may choose to tamper the on-board unit rather than attacking the communication protocols. Velocity, location status and installed identity certificates are good candidates for the adversary to tamper. This attack can be counteracted by strengthening the tamper proof devices installed in vehicles.

6. Sybil attack [15, 16]

An adversary orchestrates multiple identities to cause a devastating threat either by stealing or forging them. In this attack a vehicle may pretend to be several vehicles.

CHAPTER 3

IDENTITY MANAGEMENT SCHEMES IN VEHICULAR AD HOC NETWORKS

3.1 Identity in VANETs

Identity of a given entity is an attribute of a subject that uniquely identifies it. Let us see what constitutes identity in VANETs. Papadimitratos et al. [17] analyzed identity in the context of vehicular communication.

Traditionally, license plate numbers have been used as a main identifier for a given vehicle. Transportation authorities have been doing their administrative processes using the license plates as key identifier. For example, if a certain driver violates the speed limit, he will be caught and penalized by the authorities. To identify him, the authorities use the license to infer his identity. Usually, it is assumed that the driver is the owner of the vehicle. However, this is not usually the case. License plate, a plate attached to a vehicle for identification purpose, is used to bind a vehicle with the owner or the driver. The identifier in the license plate should uniquely identify the vehicle.

License plates in Norway are administered by the Norwegian Ministry of Transport and Communications. The registration numbers of vehicles contains two letters followed by five numbers. The first two letters are based on the geographic location of

the region where registration of the vehicle is performed. The exception to the above is the use of special prefixes such as:

- CD: Corps Diplomatique
- EL: Electrically powered vehicles
- GA: autogas LPG (Liquefied petroleum gas) or other gas powered vehicles
- HY: Hydrogen powered vehicles

The Driver-to-vehicle relationship is not always one-to-one. A person may own or drive multiple cars and many drivers may drive the same car at different times. One example, for the latter is a public bus which is operated by many drivers in a given day. The relationship between the vehicle and the user is further linked with the presence of driving license. Every driver needs a driving license to operate a vehicle. Figure 11 sketches the relationship between the vehicle, the license plate and the driver (owner). The right arrow in the figure represents the relationship between a vehicle and a license plate while the down arrow shows that the driver is legally allowed to operate the vehicle.

Figure 11 Relationship between vehicle, license plate and driving license.

In the emerging VANETS, all the identifiers that are used in the current traditional system are expected to keep their role. The license plate, the driving license, the vehicle itself are all the source of identifiers in the emerging VANETs. Vehicle manufacturers assign a unique vehicle identification number (VIN) and this can serve as an identifier along with attributes such as manufacturer, date of production, model and color.

It is interesting to consider the identity of the passengers as well. Unfortunately, most of the research works conducted in VANETs only consider identity and privacy concerns of the driver. Safety applications (such as Emergency Electronic Brake Light) and convenience Applications (such as Congested Road Notification) are targeted merely to the driver. However, the consumers of commercial applications are both passengers and drivers. For Service provisioning in vehicular networks to passengers, it is essential to maintain and manage the identity of passengers as well.

The identity employed in VANETs has to witness the holder's identity without revealing any sensitive information. But at the same time, it has to be possible to trace the real identity of a vehicle in some situations such as accident. The authorities should be able to trace the real identity of vehicles to enforce their responsibilities.

3.2 Privacy Requirements

Data exchanged in VANETs contains critical information. Thus it is essential to make sure that the exchanged data is legitimate. If a vehicle acts maliciously by sending

fake information, it has to be isolated and punished for the wrong act. However, this is only possible if there is a mechanism to identify vehicles. Moreover, it is essential to authenticate vehicles to make sure that they are the one who claim they are. Identification and authentication makes it possible to track a malicious vehicle and to take a corrective measure.

However the identification and authentication should preserve the privacy of drivers. If a vehicle sends its identity in every message it send, then it is straightforward to track its movement. This is something that has a serious privacy implication. VANETs face a challenging authentication-privacy tradeoff that should be addressed.

Location privacy is especially a prime requirement for location based services (LBS). Here we present proposed mechanisms to realize privacy requirements in VANETS. These are as follows:

1. ***Time-based pseudonyms [18]***

Pseudonyms are temporary identities that changes periodically. Time-based pseudonyms use a time metric to update the pseudonym. The level of privacy achieved is dependent on the renewal frequency of the update. The higher the renewal rate the higher the level of achieved privacy. Another approach is to use the speed of the vehicle to determine the pseudonyms renewal frequency.

2. ***Mix-Zones [19]***

This scheme aims to offer location privacy. The basic idea is to update the pseudonyms of all vehicles in a given geographic area at the same time. Location change cannot be easily tracked as all vehicles within a given area perform the pseudonym update together.

3. ***Geo-bound Pseudonyms [20]***

In this scheme the pseudonyms assigned to vehicles depend on the geographic location. Thus renewal frequency of pseudonym changes is dependent on the movement patterns of a vehicle. This in turn implies that location tracking is minimized. Generally, all approaches make use of pseudonyms to achieve privacy. The difference among the approaches is in the way pseudonyms are updated and distributed.

3.3 Identity Management in VANETs

IdM in VANETs brings a new set of challenges that are not normally present in traditional IdM systems. Thus solutions from traditional IDM cannot be readily adapted to VANETS. VANETs require a sound solution for the challenging issues like privacy, pseudonym management, and effective identity life cycle management. Especially, IdM in VANETs raises a serious security and privacy issues that should be addressed.

1. **Identity management in VANETs needs to be scalable**

Managing identity in VANETs is challenging. The fact that vehicle movements are dynamic with a high speed forces identity management to be done in real-time. Moreover, the potential number of vehicles in a given road can be very large. This is especially true in rush hours in which employees commute to work or from work. Therefore, there is a strict requirement for the communication to be scalable when the network is overloaded.

2. **VANETs are decentralized**

One of the key challenges in VANETs is that VANET is a decentralized system. Vehicles may join or leave the network at any time. IdM in decentralized systems is much more difficult to achieve than centralized systems.

3. **IdM in VANETs should preserve privacy**

Privacy is a prime requirement in VANETs. If privacy measures aren't implemented, private information of drivers will be leaked. Attackers can trace drivers in a daily basis and this has a serious life-threatening implication. Achieving privacy, while keeping auditability is very challenging.

4. IdM in VANETS should be interoperable

Each vehicle will only be registered with the road authorities in its region. Upon registration, the vehicle will get an identity and after that it can communicate with all vehicles in the region it registered with. The problem arises when this vehicle crosses its region and finds itself on another region. The vehicle cannot communicate with the vehicles in the new regions as it not registered.

As a running example let us take the following scenario. Suppose vehicle "A" which is registered with a Sweden road authority travels to Norway as shown in Figure 12. Let us further assume that vehicle "A" has a digital certificate $certA_{sw}$ from the Sweden road authority. Now Vehicle "A" can only communicate with Vehicles in Norway if there is an agreement between the road authorities of Sweden and Norway. The interoperability will be even difficult to achieve if the IdM used in Norway is Certificate based and if Sweden employed identity based IdM.

Figure 12 A vehicle from Sweden driving to Norway

For the success of VANETs interoperability between CA's, across different regions of the world, is one of the key factors. Otherwise, there will be a fragmented VANET network in each region that has its own proprietary IdM system.

3.4 Identity Management Schemes

In this section the existing proposals for IdM in VANETs are examined.

3.4.1 GSIS: A Secure and Privacy-Preserving Scheme for Vehicular Communications

Lin et.al. [21] Proposed Group Signature and Identity-based Signatures (GSIS) scheme offers security and conditional privacy in VANETs. This scheme offers desirable security requirements such as authentication, integrity, and anonymous user

authentication, vehicle anonymity, and RSU ID exposure, prevention of RSU replication, vehicle ID traceability, and efficiency.

GSIS tackles the security problems by taking a different approach to secure communication between vehicles and communication between vehicles and RSUs as they have different security requirements.

Lin et.al. pointed out that traditional public key encryption scheme cannot be used in signing the safety messages, as the ID information is contained in the public key certificates. Thus, for V2V communication, group signature is employed and messages can be securely and anonymously be signed by the senders, while the road authorities can reveal the identities of the senders when required. The privacy requirement of V2I is not as sensitive as V2V communication. Thus GSIS chooses a signature scheme using ID-based cryptography (IBC) to digitally sign each message sent by the RSUs to ensure origin authentication and this greatly minimizes the signature overhead. GSIS exploits the fact that, any string can serves as a valid public key in IBC. The location of the RSU, the unique number and the code of the RSU are proposed to be used as a public key and this leads to a simplified certificate management in VANETs.

V2V communication

The scheme for V2V communication comprises five phases as shown in Figure 13. The first step is vehicle registration in which a membership manager (MM) generates and distributes a tuple for every vehicle that will be used as vehicle's private key. The MM archives the association between vehicles and the tuples for later use. The next

phase is message signing. To sign a given message, a vehicle uses both the group public key and its private key. The third phase is message verification. First of all, a timestamp is checked, if it is ok then the message's signature is verified using the group public key and some system parameters. If the message fails to pass the verification tests, it will be dropped.

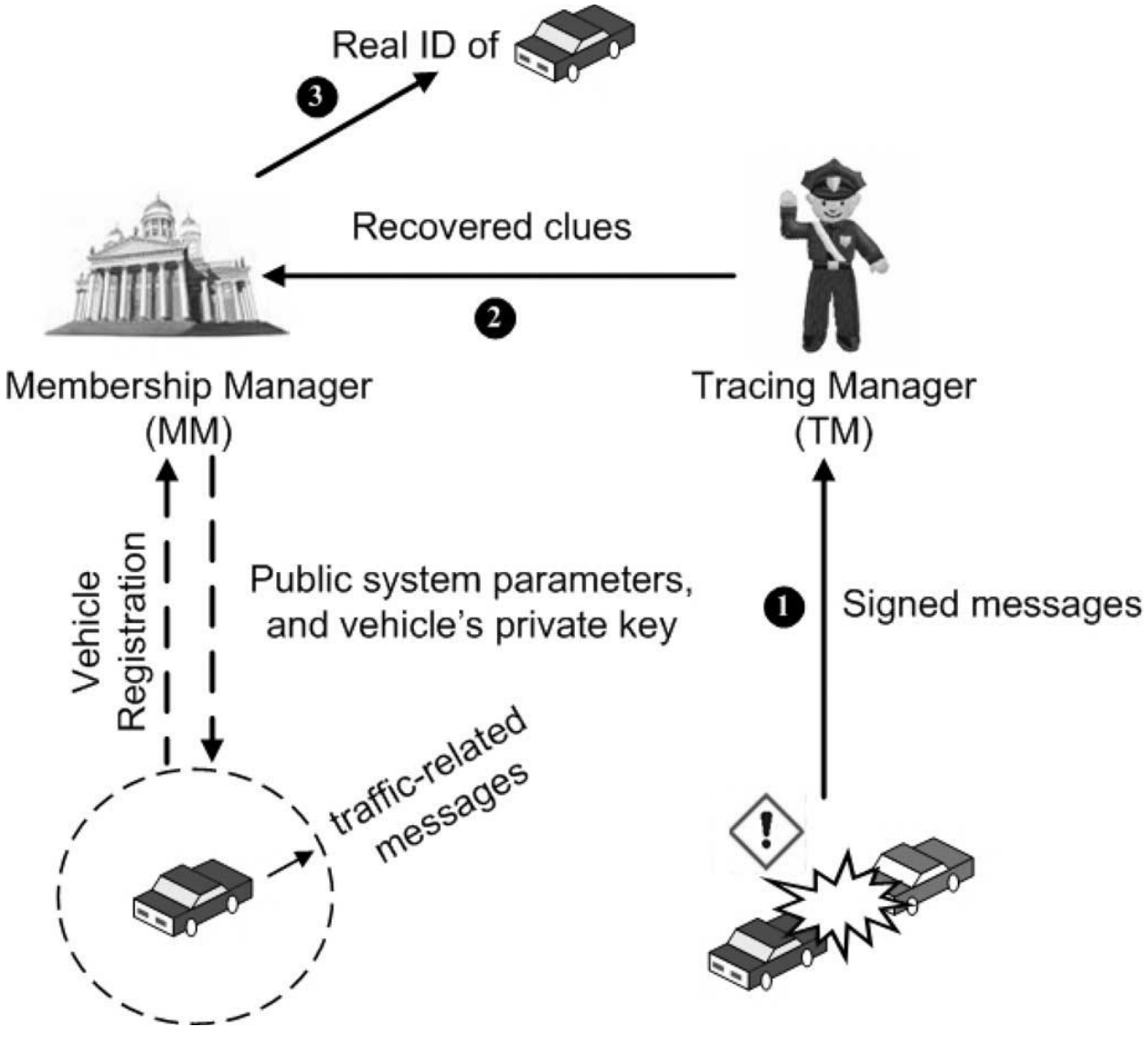

Figure 13 GSIS scheme [21]

The fourth phase is membership traceability. In certain cases, for example accident liability, the road authorities need to trace the real identity of the vehicle that sent a given message and GSIS has a remedy for traceability. A tracing manager (TM) checks the validity of the signature and generates a part of the tuple that was generated during vehicle registration. The tracing manger then sends the recovered clues to the membership manager who can easily look up the real ID of the associated message signer.

The fifth and the final phase is membership revocation phase. When a vehicle is found compromised or when it misbehaved it should be excluded from the system. GSIS considered two different approaches for revocation. The first obvious approach is to update the group public key and private keys of all unrevoked vehicles. However, this approach incurs a huge performance penalty as it is required to change the group public and private keys of each vehicle from time to time. The second approach proposed is the traditional CRL-based verifier-local revocation (VLR) [30-32] in which only verifiers are needed in the revocation check-up process.

To maximize the efficiency of the revocation process, GSIS employed a hybrid scheme which combines both revocation ways. The idea is that, when the number of revoked vehicles is less than a predefined threshold, the VLR revocation scheme is used and when the threshold is reached the group public and private keys of all unrevoked vehicles are updated.

V2I communication

For securing V2I communication GSIS uses a three phase protocol. The first phase is private key generation. A unique identifier string is generated for each RSU that

comprises a unique serial number, the physical location of the RSU and an attribute of the message. This identifier string is used as a public key of the RSU and the corresponding private key will serve as a private key of the RSU. The second phase is a message signing phase. To every message it sent the RSU attaches a type ID, a timestamp, its signature and its identifier string. In the final phase, Verification phase, the vehicles check whether the physical location of the RSU agrees with the value specified in the RSU's identifier string. If the message passes the first check, then a further verification is performed on timestamp and signature of the message. If the message fails to pass the verification tests, it will be dropped.

Analysis

Strong sides

- This scheme takes in to consideration the fact that V2V and V2I communication have different security requirements.
- It proposes a security solution for both communication types.
- It also supports traceability of vehicles by authorized authorities and revocation of vehicles.
- Since there is a separation between V2V and V2I communication, vehicles can communicate in area that has minimal infra-structure support.

Weak sides

- This scheme failed to cover group formation, election of group manager and other related issues.
- This scheme is not suitable for realizing interoperable vehicular networks.

3.4.2 TACKS: TACKING TOGETHER EFFICIENT AUTHENTICATION, REVOCATION, AND PRIVACY IN VANETS

Temporary Anonymous Certified Keys (TACKs) [22] is a scheme that offers authentication, privacy, short-term linkability, traceability, revocation, and efficiency. TACK mainly employs group signatures to satisfy its security requirements.

The design of TACKs groups the roads into geographic regions and assumes that in each geographical region there are Regional Authorities (RA)s which can serve as a certificate authority. Moreover, the federal transportation authority will be the root of the key hierarchy. This assumption is reasonable and it makes TACKs suitable for easy interoperability.

TACK employs the group signature scheme proposed in [23]. The idea is that each member of a group has a group user key, a long-term private key, issued by a trusted group manager, such as the Department of Motor Vehicles (DMV). When a vehicle wants to obtain a certificate for short-lived TACK from its respective RA, it signs the request message with its group user key. The short-lived TACK is used for signing messages. The vehicle periodically broadcasts its certificate, so that others can verify the signed message it sends.

The TACK has a very short life time and it has to be updated when the lifetime ends or when the vehicle joins a new geographical region. The update of TACK is performed as follows. The vehicle's OBU randomly generates a new TACK public/private key pair and uses the group user key to sign the TACK public key and then it sends the signed public key to the RA for the region to certify it. The RA first verifies

the group signature on the received TACK public key and checks the requestor against the revocation list. If the verification is successful, the RA signs a certificate for the requester's TACK public key, stores the associated values locally for later use and sends the certificate back after some t seconds. The delay is intentionally added as a thwart against linkability.

The main drawback of this approach pointed out in [22] is that a vehicle which has been revoked can still maliciously communicate with a valid certificate as revocation in this scheme only prevents the node from getting a new certificate.

Analysis

Strong sides

- It is well suited for realizing interoperability
- Users can control the level of their privacy and anonymity by generating a short-lived TACK as frequent as they want
- It supports traceability and revocation

Weak sides

- The revocation mechanism is imperfect as a revoked vehicle can still communicate with a valid certificate acquired earlier
- The scheme highly depends on infrastructure support

3.4.3 SRAAC

Fischer et.al. [25] proposed Secure Revocable Anonymous Authenticated Inter-Vehicle (SRAAC), a scheme that intends to improve the following security limitations of

Wireless Access in Vehicular Environment (WAVE) a standard defined in IEEE 1609.2 security standard .

- Usage of weak encryption to protect message unlinkability.
- Dependence on a single certification authority for issuing all anonymous certificates may lead to linkage of certificates and vehicles.
- High memory and bandwidth consumption because of certificate revocation list (CRL) usage.

Figure 14 depicts the general overview of SRAAC.

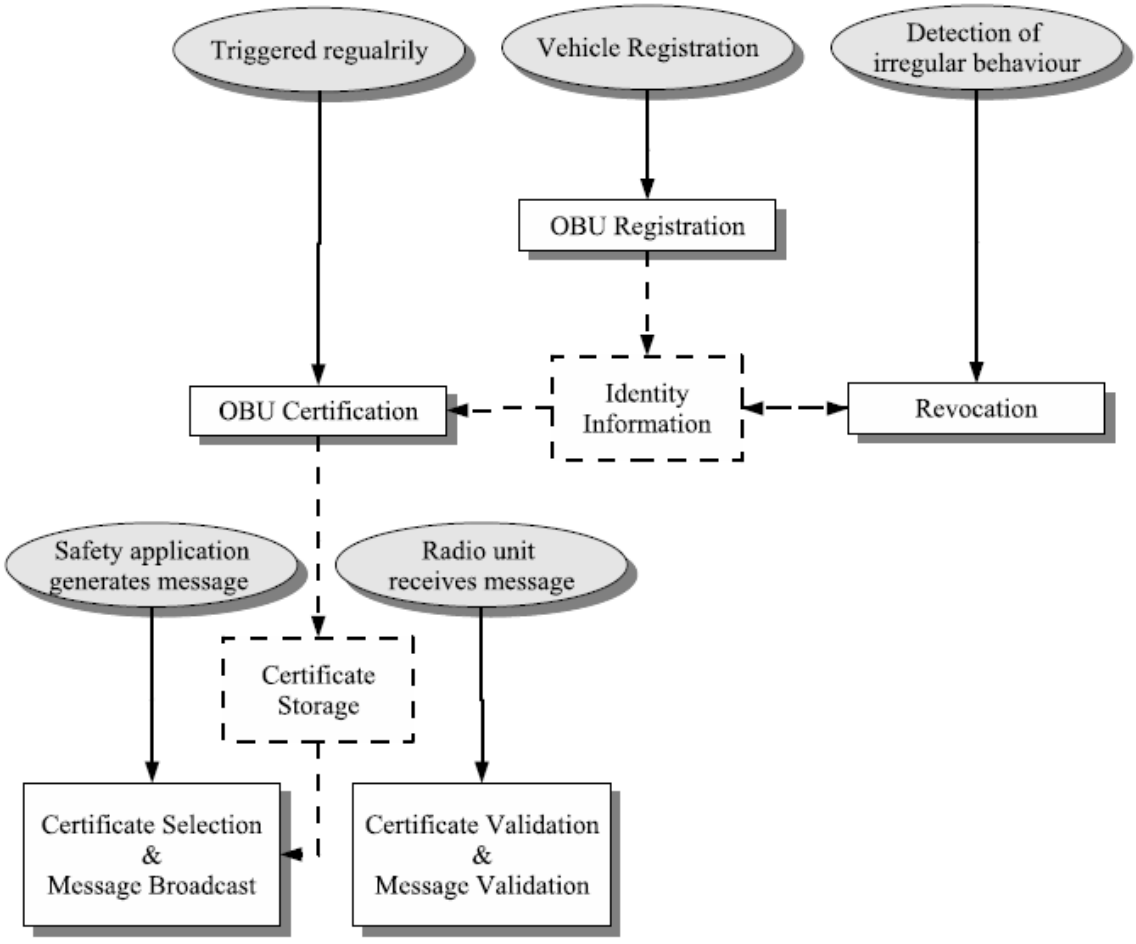

Figure 14 SRAAC scheme overview [25]

SRAAC is similar with WAVE in many aspects. Like WAVE, every Vehicle's OBU gets a pool of inter-vehicle communication (IVC) certificates from the CA. Thus, a vehicle can use each certificate for a short period of time and this makes the vehicle untraceable even if location information is contained in the message.

In SRAAC certification is not performed by a single CA. Rather, a quorum of n intermediate IVC certification servers (ICS) participate in the certification process. These servers collaboratively issue certificates using a cryptographic scheme called magic-ink signatures with shared secrets (MI-DSS).

A vehicle can periodically create a set of IVC certificates and requests the Identity Authority to authorize its request to the IVC certification servers (ICS). Once the Identity Authority authorizes the request, the ICSs blindly sign the certificates. The motivation to use blind signatures is to ensure anonymity by preventing the traceability of vehicles.

SRAAC has also a mechanism in place for road authorities to reveal the identities of vehicles when needed. This is possible as ICSs produce a tag when they sign certificates. The tag is saved along with the vehicle's identity with the Identity Authority. If a certain message is found malicious, the tag associated with the message's certificate can be extracted after determining the value of the revocation key x_t. As x_t is guarded by a (t_s, n) secret sharing scheme, t_s out of n ICSs need to agree on the revocation to recover the value of x_t. After the value of x_t is recovered, the tag can be found and the Identity Authority can reveal the identity of the vehicle and revoke it. Once revoked, a

vehicle is not entitled to get new certificates. Thus, SRAAC does not require CRLs and this greatly enhances the memory and bandwidth consumption.

Analysis

Strong sides

- It improves the security limitations of WAVE
- It offers better anonymity for users as traceability is not only done by one party
- This scheme does not require CRLs

Weak sides

- It is not well suited for realizing interoperability
- The revocation is not perfect as a revoked vehicle can still use the certificates it holds before revocation.

3.4.4 AN IDENTITY-BASED SECURITY FRAMEWORK FOR VANETS

Kamat et.al. [26] proposed a security framework for vehicular networks that employs Identity-Based Cryptography (IBC), to offer authentication, confidentiality, message integrity, non-repudiation and pseudonymity. The authors argue that schemes that use public-key cryptography are not efficient when it comes to bandwidth utilization and they suggest Identity-Based cryptography is a good choice to achieve identity management in VANETs. The fact that IBC it avoids PKI is their main argument.

The main idea is to give each vehicle and RSUs a unique e identifier. This framework assumes that these identifiers are periodically certified by a Trusted Authority and the TA distributes revocation lists periodically. In the first setup phase the TA

calculates different system parameters and keys then sends the system parameters, master secret key and a random secret key to each RSU. The vehicles, on the other hand, get system parameters, identifiers and a public/private key pair from the TA.

To get a new pseudonym, a vehicle will contact RSUs. The RSU first check whether the vehicle's credential is not revoked and if the check succeeds the vehicle and the RSU will exchange secure messages using a series of IBC, public-key and symmetric-key cryptographic operations. After the message exchange, the vehicle will get a new pseudonym containing a timestamp that assures the time in which the vehicle's credential was validated.

Since pseudonyms have an associated timestamp, vehicles can determine the trust level they will accept. The trust level is determined based on the time elapsed since the certification of the pseudonym.

For verifying a received message, the vehicle validates the identity-based signature on the message to check that the vehicle using the pseudonym has the corresponding private key to it. To achieve traceability, this framework requires vehicles to log messages in to some black-box device and to send them to the TA which can reveal the identity of the vehicle from the messages. To recover the identity of the vehicle the TA needs to compute a series of IBC and symmetric cryptographic operations.

Analysis

Strong sides

- Users can control the level of their privacy and anonymity by getting a new pseudonym as frequent as they want
- Users have a means to determine the trust level they are willing to accept

Weak sides

- The authors did not provide performance analysis results
- The revocation is not neat
- The scheme highly depends on infrastructure support

3.4.5 PAIM: PEER-BASED AUTOMOBILE IDENTITY MANAGEMENT IN VEHICULAR AD-HOC NETWORK

Squicciarini et.al. [27] proposed an IdM framework for VANET called Peer-based Automobile Identity Management (PAIM) that supports dynamic event-based moving zones formed by vehicles that have common interest. PAIM offers authentication, non-repudiation, message integrity, and confidentiality.

The authors in [27] identified that most identity management proposals for VANETs highly rely on road side infrastructures and they argued that these schemes are not well suited in rural areas which are characterized by minimal infrastructure support. Moreover, RSUs may become unavailable or compromised by attackers and thus putting all trust in RSUs is not practical. PAIM aims to greatly minimize the infrastructure dependency by using an identity-based system where public key certificates are not required for authentication.

Vehicles are only required to communicate with the road infrastructure only once; the first time they want to join the VANET to obtain a global identity. The global identity of a vehicle does not include any sensitive private information (such as driver license number and name of the driver). The basic idea in PAIM is then to enable other vehicles in the group to verify the identity of a vehicle without disclosing any information and without contacting the road side units.

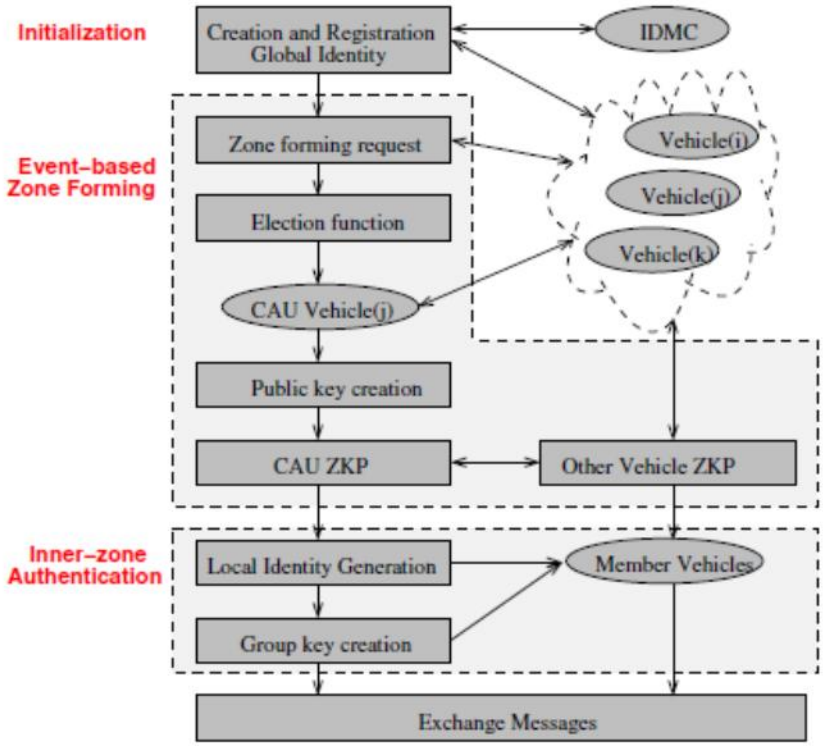

Figure 15 PAIM Overview [27]

An overview of the PAIM system is depicted in Figure 15. PAIM has three main phases: (1) initial registration; (2) event-based zone forming; and (3) inner-zone authentication.

In the first registration phase a vehicle is required to register at authorized IDentity Management Center (IDMC) and obtains a signed certificate that contains a global identity. The global identity is just a dummy identifier that does not contain any identifier information of the user at all. Note that only the registration phase needs support from infrastructure.

When a vehicle wants to obtain a global identity, it sends an encrypted message to the IDMC using IDMC's public key. This enables the vehicle and the IDMC to agree on a session key.

After the key agreement, the remaining communication will be encrypted by the shared secret key. The vehicle sends its identity information (such as driver license number or social security number) and the VIN of the vehicle. The IDMC then verifies the identity and if the verification is successful, it will generate a global identity. Pedersen commitment [28] is used for generating the global identity and the global identity has a very interesting property. This property is that the global identity does not contain any explicit information about the identity of the user, yet the user can prove that it knows the committed value in the global identity; this fact is, in fact, used by vehicles to obtain temporary local identities.

Once the vehicle obtained the global identity, it can communicate with other vehicles by forming an event-based zone or joining an existing zone. PAIM assumes that groups are dynamically created when there is an event of interest that requires

communication of vehicles and each zone is administered by Captain Authentication Unit (CAU).

To join a zone a vehicle is required to present its global identity to obtain a temporary local identity from Captain Authentication Unit (CAU) in the zone. Once obtaining the local identity, the vehicle can communicate with the group members. PAIM has a defined protocol to dynamically select the CAU.

Analysis

Strong sides

- This scheme avoids high dependency on infrastructures
- Supports a dynamic event-based group based authentication

Weak sides

- The Captain Authentication Unit (CAU) can track vehicles after collecting some data as they always present the same global identity to the CAU
- The CAU election protocol is susceptible for DOS attacks
- The scheme does not support revocation of vehicles

CHAPTER 4

BACKGROUND ON OPENID

OpenID is one of the several identity management solutions for the web which supports single-sign on (SSO). Its openness and flexibility accelerated its widespread adaptation. According to OpenID.net, there are over one billion OpenID enabled user accounts and over 50,000 websites which support OpenID based authentication**.** Moreover, many organizations such as Google, Yahoo, AOL, Verisign, Paypal, IBM, Microsoft, and so on [24] serve as OpenID providers. In this chapter we aim to provide an insight for the reader on the basics of OpenID as OpenID is later used in our proposal.

4.1 OpenID Identifier

An OpenID Identifier is a unique string in the OpenID domain that serves as an identifier for the user to get an access to OpenID-enabled web site. The identifier is usually represented in the form of the form of an HTTP or HTTPS URL as shown in Figure 16. The HTTPS URL is preferable as it strengths the security of OpenID.

Figure 16 An OpenID Identifier example

OpenID has an interesting feature that enables users to use their existing web site address that they own as an OpenID identifier. Users can also use any URL that they control as their OpenID identifier. A user, without an existing URL under his control, can sign up for an OpenID identifier with an OpenID Identity Provider (OP). There are many OpenID Identity Providers (OPs) that let users to have their own OpenID identifier free of charge. Among these providers, myOpenID [33], claimID [34], and myID.net [35] can be mentioned. Actually, most users have an OpenID already and they might not be even aware of it. This is because both Google and Yahoo serve as an OpenID Identity Provider (OP) [36]. Google and Yahoo have a large user base among the estimated 1 billion OpenID-enabled users.

4.2 Entities

In the OpenID framework, we can identify three involved parties: End user, OpenID Identity Provider (OP) and Relying Party (RP). The end user (U) requests a service from the Relying Party (RP) and OpenID Identity Provider (OP) offers the required identity information about the user to the Relying party (RP).

1. End User

The end user is the human user who has one or more OpenID identities. The user is responsible for creating, managing and maintaining his OpenID identity. The user first needs to contact the OpenID Identity Provider (OP) in order to get an OpenID identifier. The OP may require the user to present a credential such as a password. Yet, password is not strong level of assurance.

Some service providers may not need high level of assurance. For example, a news website may not require a high level of assurance about the user from the OpenID Identity Provider (OP). Usually user name and password authentication and simple registration method is adequate for the purpose. However, if we take an electronic voting service run by a certain state, we can apparently observe that a high level of assurance is needed. The organization who is running the election wants to have a very high confidence in the voter's identity. The degree of level of assurance is determined by the method used in the registration phase. This implies that OpenID needs a strong registration phase in order to be used in critical services like electronic voting.

2. User Agent

Any Internet browser that supports HTTP/1.1 protocol can serve as a user agent. The user agent functions on behalf of the user and it takes care of requests, responses and redirects between the relying party (RP) and OpenID Identity Provider (OP).

3. Relying Party

The Relying Party (RP) offers services to users but it mandates them to authenticate themselves using the OpenID protocol before allowing them to get the services. The term service provider (SP) is common but OpenID standard opted to use the term Relying Party (RP) instead. Upon receiving the OpenID identifier, the RP discovers the OP and redirects the UA to the OP for authentication.

4. OpenID Identity Provider

The OpenID Identity Provider (OP) is an identity provider which provides an identity to the end user. It is important that the OP is trusted by both end users and relying parties. A user can maintain multiple OpenID identities with a given OP. The OP is responsible to authenticate a user with a given OpenID identifier and must provide assertions when requested by an RP.

4.3 OpenID Protocol in detail

The OpenID protocol comprises seven main steps [37]. These steps are shown in Figure 17 and described in brief consequently.

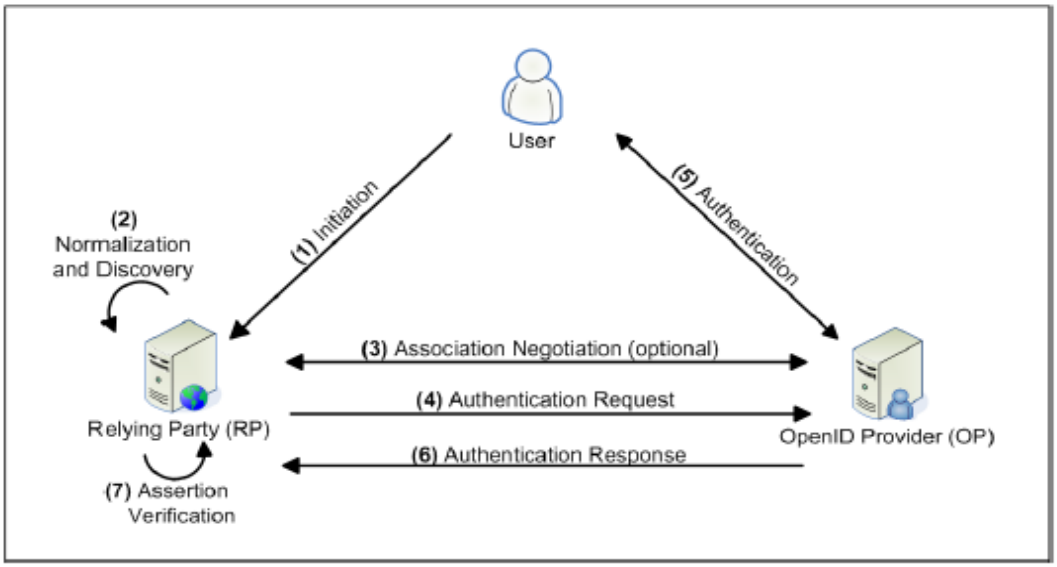

Figure 17 An OpenID Protocol authentication flow [37]

1. **Initiation**

This is a step in which the user transfers its identifier to the relying party. This step signals the starting of the login process. A user opens the website of an OpenID enabled service provider (RP) and passes his OpenID identifier instead of credentials such as user name and password.

2. Normalization/Discovery

This is a step in which the relying party changes the OpenID identity entered by the user to a standardized form. The RP also extracts information from the entered OpenID identifier and learns which OpenID provider is responsible to process the request. The RP first normalizes the identifier entered by the user**.** The prime purpose of the normalization is to avoid any irregularities that the user might have included with the input he entered.

Once the normalization process is completed the RP will continue to the discovery process. In this process, all information needed for creating authentication request is collected from the claimed identifier. The following information is the output of this process:

- The location of OpenID service on the part of the OP (OP endpoint URL)
- The supported OpenID protocol version
- The name of the claimed identity (Claimed identifier)
- An alternative representation of the identifier (OP-Local identifier).

3. Association Negotiation

This is an optional step that creates a secured communication channel between relying party and OpenID provider. RP and OP agree on a shared secret that is later used for digital signature generation and verification. Thus step enables the integrity of the exchanged subsequent OpenID messages. If a RP does not support creating or saving associations, another mode called “stateless” is employed. In this mode, the OP generates its own private secret for signing OpenID messages. The RP later checks OpenID messages received from OP to verify the authentication.

4. **Authentication Request**

This a step in which the relying party requests the OpenID provider to authenticate the user. The RP forwards the user's web browser along with the associated OpenID authentication request to the OP.

5. **Authentication**

This is the step in which the actual verification of the user's identity is performed. The OP finds out whether the user is in control of the OpenID identity and whether he or she wants to perform the current authentication. The OpenID standard does not specify the method of authentication**.** The OP is free to use any authentication mechanism. But user name and password is a commonly employed mechanism for authentication.

6. **Authentication Response**

In this step the OpenID provider informs the relying party about the result of the authentication. The OpenID provider forwards the user back to the relying party with either a positive (if the authentication is successful) or a negative response.

7. **Assertion Verification**

In this last step the relying party makes sure that the authentication response is actually received from the OpenID provider and it is unaltered. To check this, the relying party tests the OP's response against the pre-established association if the operating mode is statefull. If stateless mode is used the relying party directly queries the OP to verify the integrity of the received response. If the verification is successful, then the user is allowed to get access to the service of the relying party and the authentication process is completed.

CHAPTER 5

ISSUES IN EXISTING VANET IDENTITY MANAGEMENT SCHEMES

A robust Identity management system is an essential prerequisite before the deployment of VANETs. In this chapter, we argue that IdM in VANETs still remains a challenge that needs to be addressed. We identify the shortcomings of current VANET IdM proposals.

5.1 There is no Separation between the Identity of the Driver and the Identity of Vehicle

Almost all research works on IdM do not make a distinction between the identity of the driver and the identity of the vehicle. This may seem a reasonable assumption at the first glance. However, if we consider some scenarios, it will be apparent that distinction between them is required in some cases.

First of all, consider a family vehicle that is operated by any of the family members at a given time. Then, assuming that the identity of a vehicle is the same as that of the driver's identity is not simply valid.

Secondly, it is worth to realize that the vehicle has many built-in sensors to enable it to have a view of its surrounding environment. The future vehicles will have even more sensors. Thus, the sensor can detect a situation and may send a message without the consent or awareness of the driver. For example, a sensor may sense a sudden downhill and sends a Road Hazard Control Notification. The driver on the other hand may want to query the RSU about the availability of parking lots or may even want to chat with a driver.

Let us assume that one of the sensors in a vehicle failed and started to send a wrong message to its neighbors about sudden downhill or congestion notification. The other vehicles realize that the message they received from the vehicle is wrong and report it to the road authorities. The road authorities can penalize the driver for the offence even if he or she is not guilty.

Of course, a greedy driver can prepare a fake message and send it to the neighbors for its own advantage. But, a sensor failure can also be the reason. However, this cannot be distinguished if there is no separation between the identity of the user and the driver.

Current research efforts in IdM schemes for VANETs do not consider the passengers. In fact, Safety applications (such as Emergency Electronic Brake Light) and convenience Applications (such as Congested Road Notification) are targeted merely to the driver. However, the consumers of commercial applications are both passengers and drivers. For Service provisioning in vehicular networks to passengers, it is essential maintain and manage the identity of passengers as well. Therefore further research effort is required to integrate passengers in the IdM of VANETs as well. From the service provider's point of view, passengers are the most attractive customers than a single driver. For example, if there is a company which offers multimedia services in a vehicle, then the passengers should also be able to use the service. IdM in VANETs, therefore, should also support the identity of passengers in some way. A further example can be an accident situation. If an accident occurs, then it is desirable to know about the passengers who are on board.

5.2Different VANET Applications have Different IdM Requirements

One of the factors that amplify the challenge in IdM of VANETs is the existence of different applications that have completely different requirements. Safety applications were the first envisioned VANET applications. In fact, the very first reason of deploying VANETSs is to enhance safety in the road. But later, Convenience Applications and commercial applications came along the way. The current state of the art in VANETs is too vague on how these applications are offered.

Criteria	Safety Applications	Convenience Applications	Commercial Applications
Purpose	To reduce accident	To enhance driving experience	To offer variety of services
Audience	Drivers	Drivers	Drivers and passengers
Integrity requirements	High	Medium	Medium
Data dissemination technique	Usually beaconing	Beaconing, single hop or multi-hop	To a specific user(unicast)
Communication type	Typically V2V	V2V or V2I	Typically V2I
Criticality	High	Medium	Low
Payment	Free	Probably free	required
Subscription	Not required	Not required	Typically required

Road authorities monitoring	required	required	Typically not required
Latency requirement	High	Medium	Medium

Table 2 Requirements of different applications

5.3 The Absence of Complete IdM framework

Tuhan [29] identified the functions that should offered by a typical IdM system. Some of these functions are identity administration, provisioning & authorization, user self-service, authentication, access control, federation, etc.

Almost all of these functions should also be a present in a VANET IdM schemes. However, all IdM proposals for VANETs only consider a few of the above listed identity management functionalities. Most proposals are aimed to provide the well-known security requirements for VANETs: confidentiality, integrity and availability. However, identity management is a far broader concept than authentication and authorization.

CHAPTER 6

OUR PROPOSAL

6.1 Introduction

This chapter explains our proposed identity management architecture which has the following features.

- Our architecture makes a distinction between identity of the driver and the identity of the vehicle. To the best of our knowledge our approach is the first one to make such a distinction.
- Our architecture utilizes the smartphones as a tool for establishing the identity of the driver.
- In the Initial deployment stage of VANETs it is not realistic to expect abundant road side infra-structure along the roads. Moreover, it is unlikely that every CA will build a trust relationship with every other CA. By taking these in to consideration, our architecture is designed in a way that enables drivers to freely move across domains managed by different CAs even if the CAs do not have an agreement on cross-certification.

6.2 VANET Model and Assumptions

We consider the following generic model of VANETs, shown in Figure 18, throughout this work. The model comprises the CAs, RSUs, and Vehicles. The CA is responsible for registration and administration of vehicles and RSUs. We assume that the CA is equipped with huge storage capacity and processing capability. The communication link between the CA and RSU can be wired or wireless, but it has to be a secure and reliable link. RSUs may communicate directly or via a CA. DSRC mandates IEEE 802.11p to be used as a

communication mechanism for both vehicle to vehicle and vehicle RSU communication.

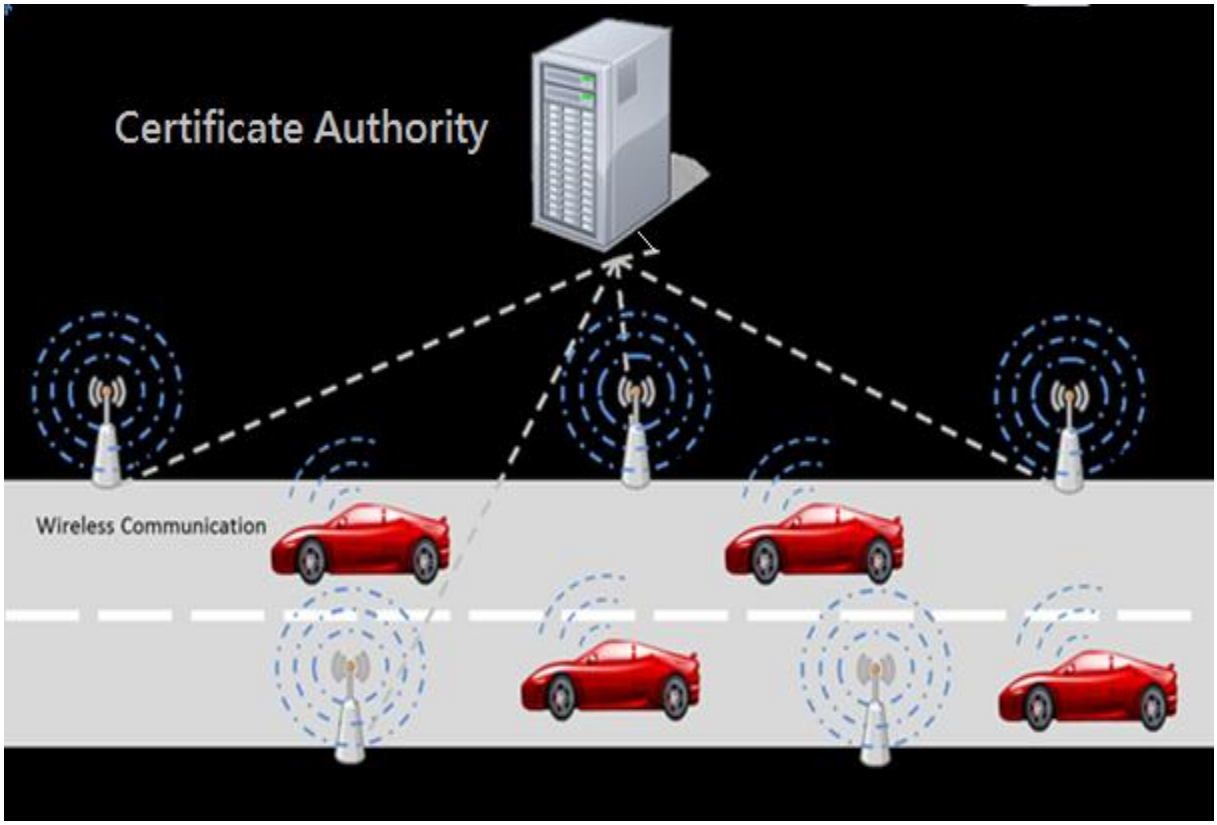

Figure 18 Generic model of VANET

We further assume the presence of a certificate authority (CA) that issues pseudonym certificates to vehicles periodically. The CAs are organized in a hierarchical manner to simplify certificate management. The organization of CAs is usually location based. Figure 19 shows a certificate authority with three regional CAs. Practically, the hierarchy is extended both upwards and

downwards. Thus, CAs need to establish trust and collaboration among them so that vehicles can travel outside the domain governed by their CA.

We make the following assumptions on the model:

- CAs are trusted by all the other entities.
- It is infeasible for an attacker to control or compromise a CA.
- RSUs are not as abundant as vehicles in the roads and some of them can be compromised by an attacker.
- CAs engage in cross-certification with other CAs.
- Vehicles are the less trusted entities as they may act maliciously.
- Both vehicles and RSUs are equipped with hardware security module that performs secure storage and processing.
- CAs are organized in a hierarchal fashion. We assume country trusted authority (CTA) is a root level CA in a given country. Regional and city level trusted authorities are under CTA. Each city level trusted authorities are responsible to certify all RSUS and Vehicles in the corresponding city.

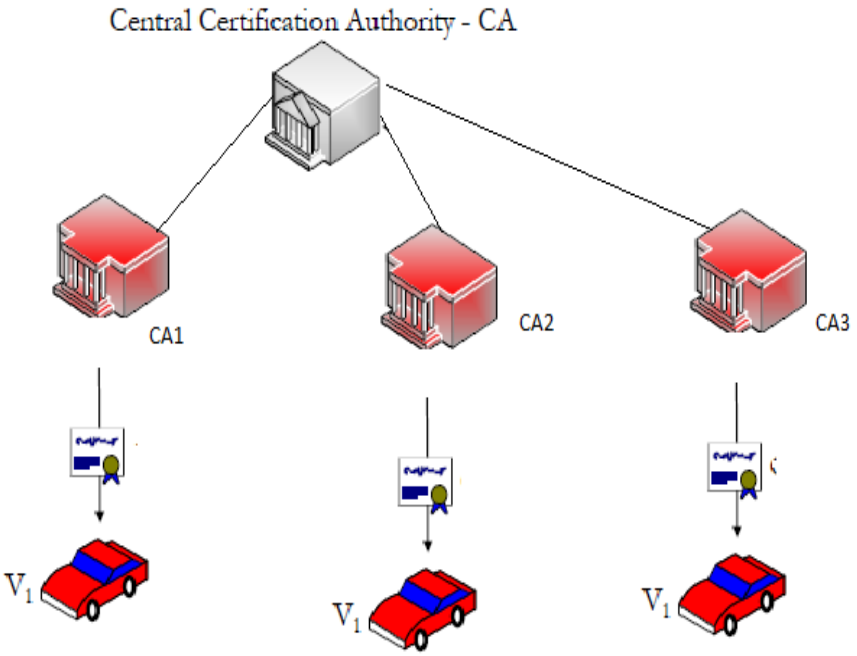

Figure 19 Certificate authority with three regional certificate authorities

- We further assume that drivers are equipped with smart phones. Smartphones are rapidly developing and enjoying market penetration. The 2012 survey [38] on Smart phone markets estimated that around 492 million smartphones were shipped worldwide in 2011 and this means that smartphones constitute 31.8 percent of all handsets shipped. Thus it is fair to assume drivers are equipped with smartphone.

  In our proposed architecture smartphones are used to establish the identity of a driver. We argue that smartphones are good solution to serve the above purpose. The following arguments can be given to support our claim.

1. Most smartphones have an integrated assisted GPS (A-GPS) receiver that makes them to be able to determine their location with an acceptable accuracy.
2. Smartphones support multiple communication capabilities such as 3G, Wi-Fi, and etc.
3. They have a good user interface in the form of touch panels.

4. There are friendly application development environments for smartphones. Major Smartphone platforms such as Apple's iPhone and Google's Android offer development environment that enables application development.
5. Most car manufacturers have included an interface for smartphones in their modern vehicles.

Figure 20 In-vehicle smartphone

6.3 Design Objectives and General Architecture

6.3.1 Design Objectives

The scheme we propose herein satisfies the following security requirements.

1. Anonymity

The real identity of a given vehicle should be only known by the CA.

2. Unlinkability

An adversary should not be able to link messages and figure out the real identity of the sender.

3. Conditional tracing

The CA should be able to trace the sender of a given message by extracting the real identity of a vehicle from its pseudo identity when required.

4. Scalability

Our scheme should work well when the network is overloaded.

5. Efficiency

Our scheme should provide an efficient way for vehicles to update their certificates and revocation should also be efficient.

6. Transparent roaming

Drivers should be able to roam between different network domains seamlessly.

7. Support for value-added applications

On top of safety-related applications, VANETs envisioned a broad range of value-added applications, such payment services (toll collection, parking Fee collection), location based services, infotainment etc. Our scheme should support both safety-related applications and value-added applications.

6.3.2 GENERAL ARCHITECTURE

We consider a basic PKI based identity management architecture.

- Each vehicle needs to register with a certificate authority in its domain. The driver is expected to show up in person and present private documents such as driving license and vehicle's plate number for successful registration. Upon registering, it will get a long term public\private key pair. This key pair is only used to communicate with the CA.
- Each vehicle's OBU is preloaded with a set of anonymous certificates from the CA. When the vehicle runs out of these short-term anonymous certificates, it will

request new ones from the CA. The CA first authenticates the vehicle and then provides it with new anonymous certificates. TA is the only authorized entity that is able to learn the real identity of a vehicle from a given certificate. Each vehicle needs to change its anonymous certificate periodically to reduce tracking.

- Road side units (RSUs) have a certificate which is signed by the TA. Their public keys are broadcasted so that the vehicles are able to use them.
- The TA has also a long-term public key that is known by all entities.
- The CA is responsible for certificate revocation.

As it can be easily seen, the above architecture is too general. We avoided going in to details for the sake of brevity. In the subsequent sections, we will extend this general architecture by adding new features on it.

6.4 Identifying Driver Targeted Applications

There are many applications that can be offered in VANETs and identifying the target consumer of the application is essential to design a sound IdM schemes. Existing IdM schemes for VANETs fail as they only take in to account a specific situation. It is difficult to devise a generic scheme that fits all scenarios, but understanding the requirement and properties of different applications is a good starting point for achieving a good IdM solution. Thus, we start by categorizing VANET applications in to two categories: vehicle targeted applications and driver (passenger) targeted applications.

The criterion we used for categorizing the envisioned VANET applications is based on the target of the application. Target of the application describes the audience of the application. The possible targets are Vehicles, Drivers, Passengers

or any of the combination. Note that we are making a separation between a driver and the vehicle. Determining whether the application is for the driver or the vehicle can be tricky. But, we used two criteria to make this distinction.

The first important criterion is the involvement of the driver. Every application requires message exchanges and we exploit the driver's involvement in message exchanges as a distinction factor for determining the target of the application. In some applications, the driver does not involve at all in any message exchanges and the vehicle reacts on all the messages autonomously and they can be considered as vehicle targeted applications. In some applications the message exchange is done by the vehicle autonomously, but the driver gets notified about it. The other criterion, for distinguishing driver-oriented applications from vehicle-oriented applications, is the type of application consumer. For example, a warning about uphill road is intended for the vehicle while a restaurant advertisement is intended for the driver.

Application	Target
Road hazard condition notification.	Vehicle
Cooperative collision warning	Vehicle
Slow/Stop Vehicle Advisor	Vehicle
Post-Crash Notification	Vehicle
Road Hazard Control Notification	Vehicle

Cooperate Collision Warning	Vehicle
Toll booth collections	Driver
Parking availability Notification	Driver
Service announcements	Driver and Passengers
Real Time Video Relay	Drivers and Passengers

Table 3 Categorization of VANET applications

Many applications are envisioned for VANETs. However, it is not clear what communication infrastructure is intended to support these applications. It is assumed that vehicles will be equipped with many wireless network capabilities. 3G networks, WIFI, WiMAX and M2M communication forms will be offered in VANETs. The infrastructure selected for a given application will have a huge say on the IdM system design. Since 3G networks enjoyed a wide coverage and the network is matured. We can predict that it will be a preferred choice. In this work, we assume that 3G networks are used by service providers to offer their services to drivers and passengers.

6.5 USING OPENID AS AN IDM SCHEME FOR DRIVER TARGETED VANET APPLICATIONS

This section presents our proposed approach for a privacy preserving IdM Single sign-on (SSO) solution for driver-targeted applications in VANETS. The proposed solution exploits an existing SSO solution for the web namely, OpenID.

OpenID, which is a popular web SSO solution, cannot be readily used to serve our purposes. Thus, we propose two tweaks for it so that it can satisfy the privacy and security requirements of driver-targeted applications.

Drivers, who are equipped with smart phones, need to authenticate themselves to service providers before they get an access to any service. Authenticating for every service puts a lot of burden on users. Moreover, the mobile phones which engage in authentication are constrained devices both in terms of processing power and battery life. Authentication typically involves computationally expensive cryptographic operations and thus SSO functionality is very important to decrease the burden on users and their smartphones.

Single Sign-On (SSO) is a solution that enables users to authenticate themselves once and then to use services from multiples service providers without the need of re-authentication. Unquestionably, SSO takes away a burden of re-authenticating now and then from the user.

In the context of VANETs, drivers and passengers can benefit a lot from SSO. A driver on the road does not want to authenticate himself for every service provider. In addition, since the devices used to get services are constraint devices, SSO saves computational resources and energy consumption.

OpenID is an open source identity management system that offers SSO service. In OpenID, IdP's provide their users with globally unique identifier that can be in

turn used to authenticate with any service provider. The identity of a given subject is represented using a Universal Resource Indicator (URI).

OpenID is maintained by the OpenID Foundation, and Google, Microsoft, Yahoo, PayPal, Pingidentity and Symantec are sustaining corporate members. There are 18 corporate members including Facebook, Intel, symplified, etc. According to the OpenID web site [24] there are more than one billion OpenID-enabled identities on the Internet.

Adopting OpenID as it is enables SSO in VANETs. However, the privacy requirements that we formulated in chapter will be violated. Let us use Figure 21 to illustrate the privacy concern.

A driver equipped with a smartphone was driving and he realizes that his vehicle's fuel reserve is too low, He decides to recharge his fuel reserve and thus wanted to know the closest gas station. Assume that there is a fictional service provider called "Location Finder". The driver used his Wi-Fi or 3G internet connectivity, and went to the webpage of the service provider. Assume that the driver has an identity X which he got from an identity provider called myIDP.

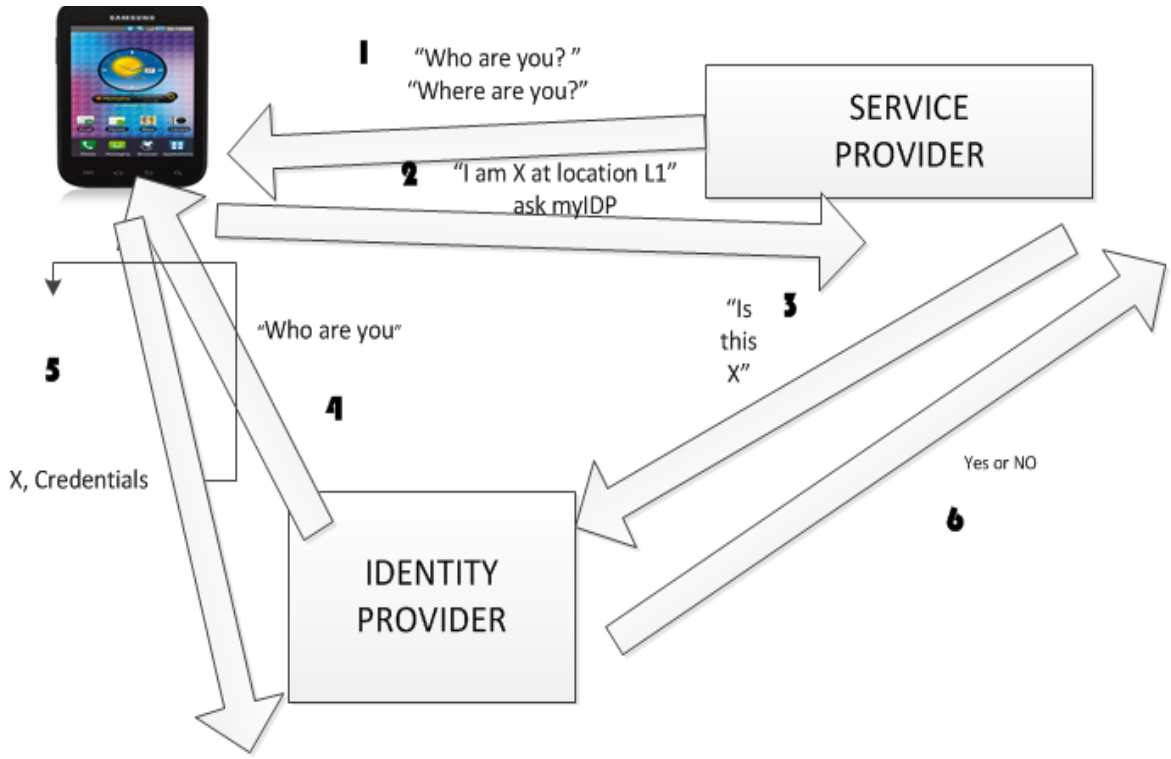

Figure 21 An Example of SSO system for VANET

As shown in the figure 21, the service provider first asks the service provider to identify himself and his location. He then replied I am "Mr. X" and my Idp is myIDP. From this response the service provider learns the following:

1. The location of the driver
2. The identity provider of the driver

In the third step, the service provider contacts the corresponding identity provider myIDP and query's it to verify the identity of Mr.X. Next, the IdP requests the Mr X to authenticate himself. Mr.X then can present the credentials (it can be password or certificate) to IdP. If the authentication is successful, then the IdP sends a confirmation back to the service provider. At this point, the service provider gets assured about the identity of the user and grants him to use the service

After 15 minutes, the same driver reaches to the destination and wanted to eat an Italian Pizza. The service provider "Location finder" can also locate the closest restaurants from a given location. Mr.X now can authenticate him the same way as he did for the previous service request. Of course, he does not need to authenticate himself again for the IdP. The whole point of SSO is to avoid repeated authentication.

Recall that the driver contacts "Location finder" two times at two different locations. The driver needs to reveal his location so that the service provider can determine the closest place the driver is looking for. In both cases, the driver authenticates himself using the same OpenID identifier. It is straightforward to see that the service provider can actually track the user and this is not desirable as it compromises the privacy of the driver. Figure 22, depicts this problem.

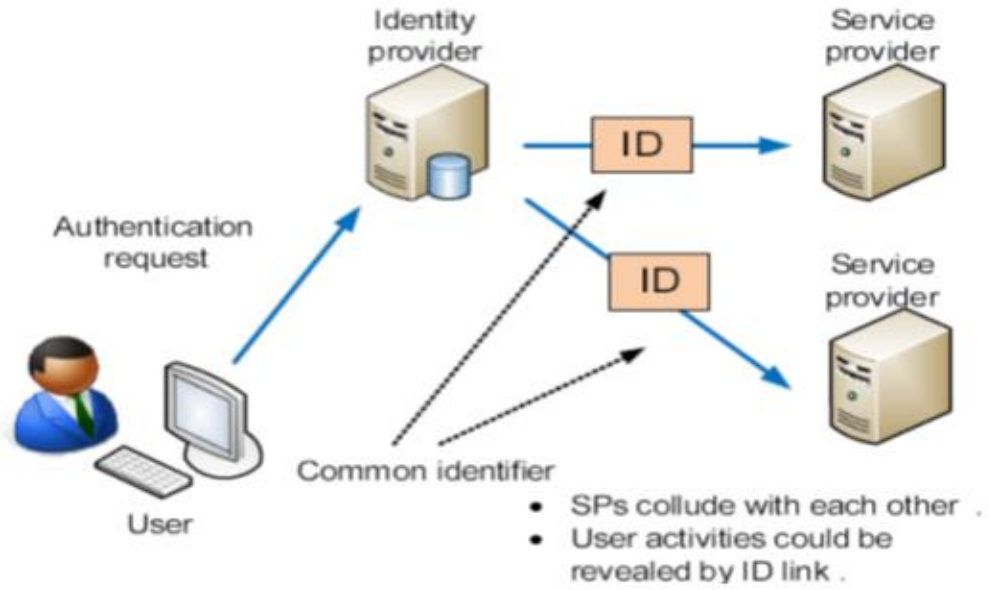

Figure 22 Linkability problems, adopted from [39]

The weakness of OpenID with respect to privacy stems from the fact that it requires users to use the same OpenID identifier (or a few more identifiers) with every service provider. This is absolutely undesirable for location based services in VANETs. Thus our proposal is mainly focused on improving this weakness of OpenID. The first tweak we propose makes OpenID capable to allow its users to enjoy anonymity by using different pseudonym identifiers as desired.

Secondly we propose to use the IP Multimedia Subsystem (IMS) as an identity provider by establishing an OpenID provider within IMS. The IP Multimedia Subsystem (IMS) architecture provides multimedia services based on Internet

technologies and SIP protocol. SIP is the main signaling protocol for the IMS architecture, and using SIP any IMS terminal can communicate with any SIP-based Internet terminal. Since IMS is access agnostic, users can their desired available communication technology such as Wifi, GPRS, UMTS, LTE, WiMAX, etc. Moreover, IMS offers strong authentication and authorization features using well-known protocols such as SIP, SDP, RTP and Diameter.

The IMS has an additional server that is capable of performing all OpenID related functionalities. Here after we call this sever as an OpenID server. The idea is that the OpenID server leverages the existing authentication mechanism within ISM to authenticate its users.

Figure 23, depicts our proposal. The components of our scheme are the smartphone of the user, the service provider and IMS with additional OpenID server. In a typical OpenID system a user uses a single identity with each service provider. Therefore a service provider can easily link the location reported by the user. We want the user to present different pseudonyms for the service provider so that location privacy is preserved. This way, the user avoids giving identifying information to the service provider.

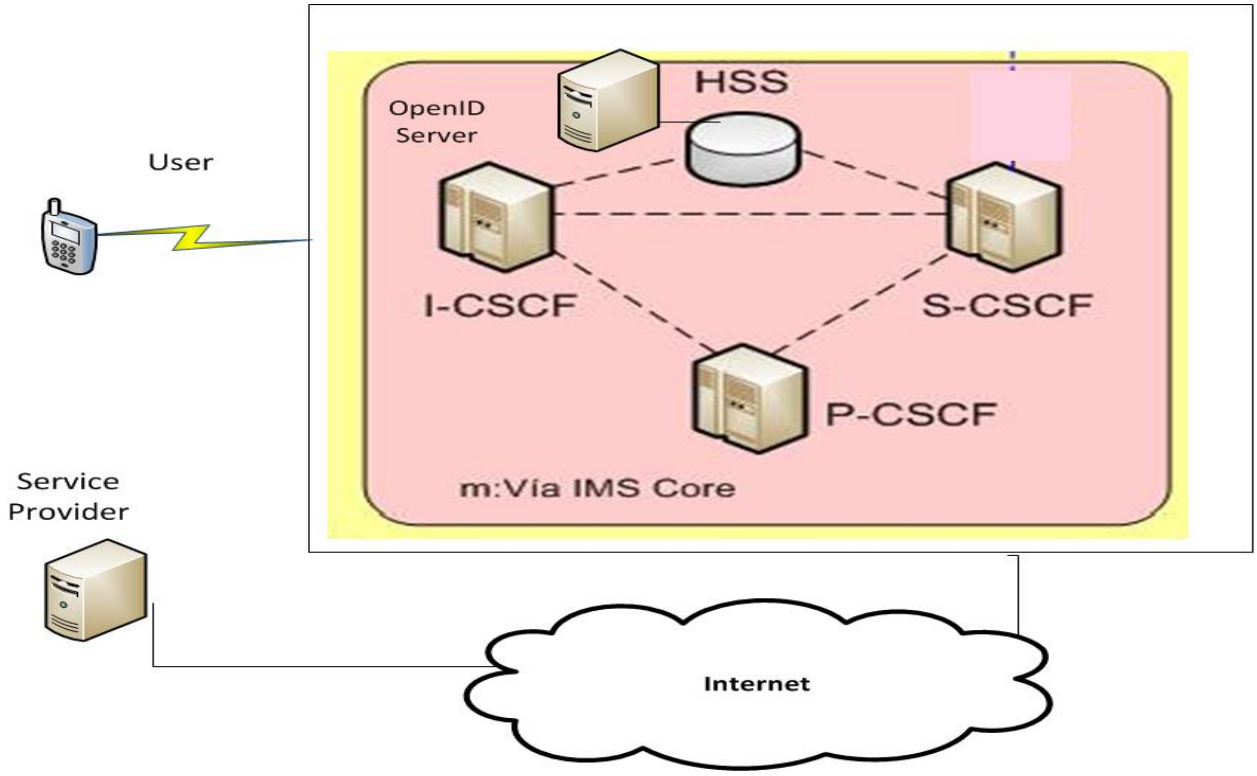

Figure 23 proposed architecture

6.5.1 AUTHENTICATION FLOW

The authentication flow of our scheme is as follows. A driver uses his smartphone and accesses a service provider

1. The service provider requests the user to authenticate using OpenID. In addition, it sends a challenge nonce n1. The service provider uses this to make sure that the assertion the client presents later is intended for it.

2. The smartphone of the driver discovers the OpenID server in the IMS.

3. In the fourth step, the OpenID Server asks the ISM to authenticate the user on its behalf. The authentication of a subscriber in IMS is performed using the IM Authentication and Key agreement procedure (IMS AKA). This

authentication is done using the IP Multimedia Private Identity (IMPI) and the shared key between the subscriber and the network. The details of (IMS AKA) can be found in [40].

4. If the authentication is successful, the IMS will send the identity "ID" of the user to the OpenID. At this stage, the OpenID server knows the identity of the user. Note that in typical OpenID systems the OpenID server is responsible to authenticate its user. But, in our scheme, the OpenID server delegates the authentication to the IMS network.

5. In the next step, the OpenID server generates a pseudonym identity for the user. We will describe the pseudonym generation in detail later. The Open ID server then forms an assertion tuple (PID,n1, SP,L) where

    - PID denotes the generated pseudonym identity
    - N1 is the challenge from the service provider
    - SP is the name of the service provider
    - L refers the location of the user reported by the cellphone provider

Our assumption here is that a cellphone provider must have to know a given user's location so that it can route the calls to the users. In addition, we put the same trust to the OpenID server which is basically part of the IMS architecture.

Exposing location in the assertion tuple may not seem appropriate at first sight. Even one can even argue that it is against the desired location privacy. However

as much as the user wants to enjoy tits location privacy, most VANET service providers want to make sure that the location reported by a given user is a genuine.

There is no any means for the service providers to check whether a location reported by a user is correct or not. Thus some service providers may want a proof whether the requesting user is really at the position he or she claims. Cellular networks can determine the location of a given subscriber with an acceptable accuracy. Thus, this can be exploited by IMS to get an estimated location of the user which will be then forwarded to the OpenID server.

The location reported by the user to the service provider may not be the exactly the same with the location proof which is obtained from the OpenID server. However, the service provider expects these two locations to be close to each other. The service provider can take its own judgment to accept or reject the claimed location of the user.

7. The OpenID server then signs the tuple (PID, n1, SP, L) with its private key. Then it forwards it to the user.

8. The user sends the signed tuple as authentication assertion for the service provider. The user also sends its current location.

9. The service provider first verifies the signature on the tuple. If verification is successful then it compares the location reported by the user with the location value in the tuple. If these values are reasonably close then authentication is completed.

6.5.2 REVISED AUTHENTICATION FLOW

The authentication assertion tuple has four attributes namely the pseudonym identity, the nonce challenge requested by the user, the service provider that requests the user to authenticate with OpenID and location.

An authenticated user who has an assertion tuple can only use it for the associated service provider. This implies that the user needs to request a new tuple for every service provider he wants to communicate with. These in turn will increase the communication overhead. Moreover a user may want to use the same pseudonym with another service provider when he is at the same location.

A simple remedy to solve the above problem is to allow the user to get a tuple that does not specify specific service provider and location. The authentication flow will change as follows.

1. A user uses his smartphone to discover the OpenID server in the IMS and to request the OpenID server to for an assertion with a pseudonym identity.

2. In the second step, the OpenID Server asks the ISM to authenticate the user on its behalf.

3. In the third step, the OpenID Server requests the ISM to authenticate the user on its behalf.

4. The IMS authenticates the user and it sends the identity "ID" of the user to the OpenID.

5. Next, the OpenID server generates a pseudonym identity, PID, for the user. Then it forms a tuple (PID,t1,t2) where

    - PID represents the pseudonym identity
    - t1 represents the time the assertion is generated
    - t2 represents the expiration date for the assertion

6. The server then signs the tuple with its private key and passes it to the user.

7. The user is now ready to use the assertion with any service provider.

Note that the service provider may want to contact with the OpenID server to check whether the assertion provided by the user is not valid or not.

6.6 Pseudonym Identity Generation and Management

In our scheme, the OpenID server does not engage in the actual authentication process. The ISM is responsible for authentication. Moreover, users do not need to register with the OpenID server directly. The OpenID server gets user information from the HSS database. The main task of the OpenID server is generation and management of pseudonym identities.

In our scheme the OpenID server is responsible to generate the pseudonyms when requested by a registered user. There are many ways for pseudonym generation. The straightforward approach is to randomly generate pseudonym IDs. However, this will incur storage overhead for the server as it needs to store all the generated IDs until their life-time expires. Therefore, it is preferable to use cryptographical ID generation

methods. Especially, hash functions that can be used for generating pseudorandom numbers are a good choice.

6.7 Using Our Proposed Scheme for Realizing Interoperability

Consider the following scenario shown in Figure 24 where a driver from Norway goes all the way to Sweden with a vehicle which is registered in Norway. Further, assume that Norway and Sweden have their own VANET network and there is no cross-certification agreement between them.

Figure 24 a vehicle from Norway heading to Sweden

If the driver has a smartphone and an Internet connection, he can join the VANET network in Sweden using our scheme. The following are the steps required to join the VANET network in the new domain.

1. A driver uses his smartphone and visits the portal of the CA and informs its wish to be authenticated with OpenID.
2. The CA asks the smartphone to authenticate using OpenID.
3. Now the smartphone can discover its OpenID server and asks for authentication.
4. The OpenID server in turn will query the IMS to authenticate the user. The IMS will authenticate the user and forwards the identity of the user to the OpenID server.
5. Finally, the OpenID server generates a pseudonym ID and forwards it to the CA.

   At this point, the CA knows the identity of the driver. Note that the CA in Sweden is provided with a pseudonym identity that does not reveal any private information.
6. The CA will generate a secret symmetric key and it sends it to the smartphone.
7. The smartphone uses the public key of the CA and retrieves the secret key. At this point, the smartphone and the CA can communicate using the secret symmetric key.

It would be interesting if we can associate the identity of the driver and the vehicle. We have used smartphone as a way of establishing the identity of the driver. The OBU, on the other hand, is used to establish the identity of the vehicle.

Figure 25 Communication options between Smartphone and OBU

There are many possible communication options between the smartphone and the OBU as shown in Figure 25. Assume that the Smartphone and OBU have a certificate signed by the CA. Thus, the door is open for associating these two identities and mutual authentication between the smartphone and the OBU can be done using SSL.

Now let us go back to the description of our scheme. We have said that the CA in Sweden and the smartphone of the driver are able to communicate. Now, the smartphone serves as a bridge for vehicle to CA communication.

The following steps are executed by the CA, the smart phone and the OBU of the vehicle. Remember that the public key of the CA is known by both the smartphone and the OBU.

1. The OBU sends an authentication request and specify that it wants to be authenticated via the Smartphone
2. Then the CA asks the OBU which smartphone is associated with it
3. Now, the OBU will engage in mutual authentication with the smartphone. After the mutual authentication, the OBU and the smartphone agree on a shared secret symmetric key valid for short period.

4. After successful authentication, the smartphone will send its pseudonym identity (which is known by the CA) to the OBU. This message will be encrypted with the shared symmetric key between the OBU and the smartphone. After encrypting the message, the smartphone also signs the message with its private key.
5. The OBU then sends the pseudonym identity of the smartphone to the CA. At this point the CA learns the identity of the smartphone which is associated with the OBU. However, the CA needs to prove the association.
6. The CA will encrypt a random nonce n1 with the key that it shares with the smartphone and sends it to the OBU.
7. Now, the OBU forwards the challenge to the smartphone.
8. The smartphone decrypts the message and extracts the nonce n1. It will forward the message to the OBU.
9. Now, the OBU encrypts the challenge with the public key of the CA and sends it to the CA.
10. The CA decrypts the message received in step 9 and verifies it. If the verification is successful, the CA concludes that the OBU and the Smartphone are associated.
11. The CA and OBU will agree on a shared secret symmetric key that has a very short lifetime.
12. Now the CA can send pseudonym certificates to the OBU that can be used in the new VANET domain. After getting the certificates, the vehicle now can join the VANET network in Sweden.

6.8 Discussion

In this section, we briefly analyze our IdM architecture for VANETs. We have started from generic certificate based IdM scheme. Then, we used smartphone as

a tool for establishing the driver's identity. We proposed the use of IP Multimedia Subsystem (IMS) as an identity provider by establishing an OpenID provider within IMS. Our architecture satisfies the following criteria.

1. **It puts separation between the identity of the driver and the identity of a vehicle.**

   Unlike many other proposals that mix the identity of the driver and a vehicle, our proposal goes ones step ahead by separating them. In our proposal, the identity of the driver is established using smartphones while the identity of the vehicle is constituted using OBUs.

2. **It enables drivers to access driver-targeted applications in a privacy preserving manner.**

   Location is very sensitive information and thus the challenge is to offer driver-targeted applications in a way that preserves the location privacy of the driver. In [3] location privacy is defined as "the ability of an individual to move in a public space with the expectation that under normal circumstances their location will not be systematically and secretly used for later use".

   In driver-targeted applications the location of the driver has to be constantly reported to the service provider and this implies that the location of drivers can be tracked by the service provider. This in turn can endanger the private life of the driver. Thus it is essential that the whereabouts of a driver should not be licked by these applications. In fact, service providers should be deprived from any opportunity to trace drivers.

Our architecture preserves privacy as the OpenID server generates a pseudonym identity for the user in each authentication request. Thus, service providers cannot track a user and the privacy of drivers is preserved.

3. **It can be used to realize interoperability across different VANET domains**

   VANET networks are normally location based. For instance, Norway will have its own VANET network which will be further organized regionally. Thus CAs need to build a trust relationship among them in order to enable vehicles to move freely across domains which are governed by different CAs.

   At the initial deployment stage of VANETs, it is not realistic to expect CAs to build trust relationship among them. Even in the presence of the trust relationships, the time incurred for certificate verification may be too costly, to be used in VANETs which are characterized by a strict real-time requirement, as the trust relationship may consist long chains. In addition, revocation can turn out to be very difficult as it should be distributed to all regions as the vehicles may be at a different region when the revocation is issued.

   Our scheme helps different VANET domains to cooperate without having the need to establish trust relationship.

4. **The issue of lost or stolen smartphones**

   Smartphones may be lost or misplaced. They are a prime target for theft. In the absence of a proper security measure, the attacker can gain an access to sensitive

data that resides on lost or stolen smartphones. The attacker can also get an access to services that are accessible from the phones.

In our architecture, smartphones are used to establish the identity of the driver. Thus, losing the smartphones is equivalent to identity theft. If a smartphone is lost and falls at the hands of the attacker, the attacker can have an access to all VANET services subscribed by the user.

There is a possible remedy available for the users when they lost their phones. They can contact their cellular carrier about the lost or stolen smartphone and the carrier stops all the services. In our architecture, the OpenID server should be informed when users lost their phone. Since the OpenID server resides on the IMS, it will learn about lost smartphones from the HSS database.

CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

This chapter presents the conclusion of the thesis and suggests a direction for future work.

7.1 Conclusion

VANETs have a huge potential to radically improve safety and driving experience along the roads and highways. A sound Identity management system is a must have prerequisite that must be designed prior to deployment of VANETs, otherwise VANETs may be used by malicious parties in a way that would jeopardize the advantages of their deployment.

In this thesis, we have identified the limitations of current VANET IdM proposals. Considering these limitations, the thesis proposes IdM architecture that satisfies the security and privacy requirements and solves the limitations we identified. The achievements accomplished in this thesis can be summarized as follows.

- We proposed an IdM architecture that makes a distinction between identity of the driver and the identity of the vehicle. To the best of our knowledge our approach is the first one to make such a distinction. Smartphone is employed as a tool for establishing the identity of the driver.
- We used the IP Multimedia Subsystem (IMS) as an identity provider by establishing an OpenID provider within IMS. We also proposed tweaks on OpenID so that it can satisfy the security and privacy requirements of VANETs.
- Our architecture enables different VANET domains to cooperate without having the need to establish trust relationship among them.

7.2 Future Work

In this thesis, we have proposed an Identity management architecture that enables secure vehicular communications. However, we have not formally verified the security of the authentication flows. Thus, a possible future direction can be to use protocol verification tools to verify the authentication flows. We did not look at the IMS Authentication and Key agreement procedure (IMS AKA) in detail. This work can be further extended by researching ways to optimize the IMS Authentication and Key agreement procedure (IMS AKA) in our architecture.

REFERENCES

1. Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. Journal of Computer Security, 15:3968, January 2007.
2. G. Grilli, *Data dissemination in vehicular ad networks, PHD dissertation,* Department of Computer Science, systems and Production University of Rome, June, 2010.
3. F. K. M. W. a. T. L. E. Schoch, "Communication patterns in VANETs," *Communications Magazine, IEEE,* vol. 46(11), p. 119–125.
4. 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., American Society for Testing and Materials International, 2003.
5. U.S. Department of Transportation. *Research and Innovative Technology Administration: Intellgent Transportation Systems*. 2010 Available from:http://www.standards.its.dot.gov/fact_sheet.asp?f=80.
6. Institute of Electrical and Electronics Engineers, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager*, in *IEEE Std 1609.1-2006*. 2006. p. c1-63.
7. Institute of Electrical and Electronics Engineers, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) -security services for applications and management messages*, in *IEEE Std 1609.2-2006*. 2006, Institute of Electrical and Electronics Engineers. p. 1-105.
8. Institute of Electrical and Electronics Engineers, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) -networking services*, in *IEEE Std 1609.3-2007*. 2007, Institute of Electrical and Electronics Engineers. p. 1-87.
9. Institute of Electrical and Electronics Engineers, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation*, in *IEEE Std 1609.4-2006*. 2006. p. 1-74.
10. *WHO: Global Status report on road safety: time for action. Geneva: World Health Organization; 2009.*

11. F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar, Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective, in Proceedings of IEEE Workshop on Automotive Networking and Applications(AutoNet), Dec. 2006.
12. M. Al-Qutayri, C. Yeun and F. Al-Hawi, Security and Privacy of Intelligent VANETs, Computational Intelligence and Modern Heuristics, INTECH, pp.191-218, 2010.
13. M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. Wireless Communications, IEEE, 13(5):8 15, october 2006.
14. B. Parno and A. Perrig. Challenges in securing vehicular networks. Workshop on Hot Topics in Networks (HotNets-IV), 2005.
15. J.T. Isaac, S. Zeadally, and J.S. Camara. Security attacks and solutions for vehicular ad hoc networks. Communications, IET, 4(7):894 {903, 30 2010.
16. John Douceur. The sybil attack. In Peter Druschel, Frans Kaashoek, and Antony Rowstron, editors, Peer-to-Peer Systems, volume 2429 of Lecture Notes in Computer Science, pages 251{260. Springer Berlin / Heidelberg, 2002. 10.1007/3-540-45748-824.
17. P. Papadimitratos, A. Kung, J-P. Hubaux, and F. Kargl. Privacy and identity management for vehicular communication systems: A position paper. In WORKSHOP ON STANDARDS FOR PRIVACY IN USER-CENTRIC IDENTITY MANAGEMENT, 2006.
18. F. Dotzer. “Privacy Issues in Vanet”. Workshop on Privacy Enhancing Technologies, Croatia, 2005.
19. J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos and J.P Hubaux, “Mix-Zones for Location Privacy in Vehicular Networks,” ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiNITS) Vancouver, (2007).
20. Coronado, E.; Cherkaoui, S.; , "An AAA Study for Service Provisioning in Vehicular Networks," *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on* , vol., no., pp.669-676, 15-18 Oct. 2007 doi: 10.1109/LCN.2007.82
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4367900&isnumber=4367785
21. X. Lin, X. Sun, P.-H. Ho, and X. Shen, GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications," Vehicular Technology, IEEE Transactions on, vol. 56, no. 6, pp. 3442-3456, 2007.
22. Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. 2009. TACKing together efficient authentication, revocation, and privacy in VANETs. In *Proceedings of*

the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'09). IEEE Press, Piscataway, NJ, USA, 484-492.

23. Boneh, D., Shacham, H.: Group signatures with verifier-local revocation. In: Proceedings of ACM CCS 2004, pp. 168–177. ACM Press, New York (2004).
24. OpenID Foundation, OpenID Foundation http://openid.net/foundation/.
25. L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC)," in Proceedings of the 4th Annual Conference on Embedded Security in Cars (escar 2006), is-its, November 2006.
26. P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in Proc. 3rd ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'06, pp. 94-95, Sept. 2006.
27. Squicciarini, A.; Dan Lin; Mancarella, A.; , "PAIM: Peer-Based Automobile Identity Management in Vehicular Ad-Hoc Network," Computer Software and Applications Conference (COMPSAC), 2011 IEEE 35th Annual , vol., no., pp.263-272, 18-22 July 2011.
28. Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In CRYPTO, pages 129–140, 1991.
29. Do Van Thuan, Identity Management Demystified, Telektronikk 3/4.2007 11 ISSN 0085-7130 Telenor ASA 2007.
30. G. Atenies, D. Song, and G. Tsudik, "Quasi-efficient revocation of group signatures," in Proc. Financ. Cryptogr., Southampton, Bermuda, Mar. 2002, pp. 183–197.
31. D. Boneh and H. Shacham, "Group signatures with verifier-local revocation,"in Proc. ACM CCS, Washington DC, Oct. 2004, pp. 166–177.
32. A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable signature," in Proc. Adv. Cryptology—Eurocrypt, ser. LNCS, vol. 3027. New York: Springer- Verlag, 2004, pp. 571-589.
33. myOpenID. (2008). Welcome to myOpenID. Last Retrieved on August1, 2012, from myOpenID web site: https://www.myopenid.com.
34. claimID. (2010). claimID.com – Manage your online identity. Last Retrieved August 1, 2012, from claimID web site: http://claimid.com.
35. myID.net. (2010). myID.net – OpenID Service. Last Retrieved August 1, 2012, from myID.net web site: http://www.myid.net/.

36. Allen, T. (2009, September 25). OpenID: Now more powerful and easier to use Last Retrieved Augsut 1, 2012, from OpenID web site: http:/ openid.net/2009/09/25/more-powerful-and-easier-to-use/.

37. Feld, S., and Pohlmann, N. Security analysis of OpenID, followed by a reference implementation of an nPA-based OpenID provider. In Information Security Solutions Europe (ISSE) conference (Madrid, Spain, 2008).

38. IDC press release, http://www.idc.com/getdoc.jsp?containerId=prUS23299912, last accessed on August 1, 2012.

39. Ryu Watanabe and Toshiaki Tanaka. 2009. Federated Authentication Mechanism using Cellular Phone - Collaboration with OpenID. In Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations (ITNG '09). IEEE Computer Society, Washington, DC, USA, 435-442.

40. 3GPP TS 33.203: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, 3g security; Access Security for IP-based services.