Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Bassong,Fils Alain Aimé

A Feasibility study of lightweight security protocols for safety related car 2 car applications

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Bassong,Fils Alain Aimé

A Feasibility study of lightweight security protocols for safety related car 2 car applications

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. rer. nat. Dirk Westhoff
Zweitgutachter : Prof. Dr.Ing. Martin Hübner

Abgegeben am June 15, 2011

Bassong,Fils Alain Aimé

Thema der Bachelorarbeit

Eine Machbarkeitsstudie für leichte Sicherheitsprotokolle für sicherheitsrelevante Car 2 Car-Anwendungen

Stichworte

CGA,leichtgewicht,Einweg-Hash-Kette

Kurzzusammenfassung

Sicherheitsmechanismen, die auf einem Public Key Infrastruktur basieren, beeinträchtigen die Gesamtleitung des C2X Kommunikation und verhindern die Skalierbarkeit von VANETs.

Zur Bewältigung der strengen Zeitanforderung von Sicherheitsanwendungen,leichtgewichte Protokolle sind gebraucht.

Wir schlagen ein Leichtgewichtes Authentifizierungsprotokoll für I2V Anwendungen vollständig auf Einweg-Hash-Kette und CGA vor.Das Protokoll zielt auf der Verringerung des Gesamtoverhead,wenn Autos RSUs begegnen.

Die Leichtigkeit und die Sicherheitseigenschaften des Protokolls werden analysiert.

Die Analyse zeigt, dass das Protokoll insgesamt eine Verringerung der Overhead-Sicherheit im Vergleich zu der aktuellen Norm verursacht.

Zusätzlich wird durch die selbst zertifizierte CGA-Adresse eine starke Authentifizierung erreicht.

Bassong,Fils Alain Aimé

Title of the paper

A Feasibility study of lightweight security protocols for safety related car 2 car applications

Keywords

CGA,lightweight,one-way hash chain

Abstract

Security mechanism based on Public Key Infrastructure take a toll on the overall performance of C2X communication and hinders the scalability of VANETs.

To cope with the stringent time requirement of safety application,lightweight protocols are needed.

We propose a lightweight authentication protocol for I2V applications entirely based on one-way hash chain and Cryptographically Generated Address.

The protocol aims at reducing the overall C2X overhead when cars encounter Road Side Units.

The lightness and the security properties of the protocol are analyzed.The analysis shows that the scheme incurs an overall reduction of the security overhead compared to the actual standard.

Additionally, strong authentication is provided through CGA which are self certified address.

Still I Rise...

Just like moons and like suns,With the certainty of tides,
Just like hopes springing high,
Still I’ll rise.
b*y Maya Angelou*

Contents

List of Tables

List of Figures

1 Introdruction

1.1 Motivation

As stated by the World Health Organization (WHO) there are about 1.2 million People killed in traffic accidents every year,10 Million People are injured,costing an estimated $520 Billion!.This alarming situation has prompted governments and car manufacturers worldwide to address issues related to traffic safety and efficiency. Consequently, there have been extensive effort firstly to educate the public and secondly to create strong partnership between academia and industry to decrease the impact of traffic accidents and injuries. As a result, cars are more safer today than they were a decade ago: active and passive safety systems such as ABS (anti-lock braking system), ESC (Electronic Stability Control) and TCS (Traction Control System) as well as airbags and belt tensioners are standard almost everywhere. Additionally, sensor and GPS units are even Incorporated by some manufactures enabling thus the vehicle to become aware of its geographic position and surroundings.

The recent advance in wireless communication technology have introduced vehicular communication as a new way to enhance traffic safety and efficiency. Indeed, the C2X communication technology promises to expand the horizon of drivers through cooperative communication-referred to as VANET-among vehicles and fixed infrastructure, making it easier to predict potential hazard situations. In Fact, through analysis of broadcasted heartbeat message called beacons containing vehicle's movement status, drivers are able to make better decisions. For instance, if after a curve, there is a broken down vehicle, there will be a warning signal, if another vehicle is approaching from the opposite direction.

There are a plethora of safety applications envisaged for VANETs, however, they depend heavily on the accuracy and the reliability of data exchanged among VANETs's entities. A corrupted data could have tremendous impact on the life of users.Therefore security issues have been recognized as a critical point and emphasized within the C2X research communities.

1.2 Overview of Car 2 X Communication

The Car-2-Car (C2C) respectively Car-to-Infrastructure (C2I) communications technology (short: C2x) is the interaction between vehicles and between vehicles and infrastructure by means of short range wireless communication (Wi-Fi standard, IEEE 802.11) aiming at warning drivers of potential hazards or risks on the road. For instance,if an accident occurs or the vehicle's sensors detect a hazard situation, then this information is forwarded to other vehicles within the same proximity per multi-hop forming thus a decentralized self-organizing network of cooperating vehicles called Vehicular Ad hoc NETworks(VANETs) .

Infrastructure ,which VANETs are scattered intermittently along city streets and highways Infrastructure,which consist of stationary units termed as Road Side Units(RSUs) and wireless hotspots (HS),while cars are equipped with On-Board Unit (OBU) and Application Units(AUs). An OBU is equipped with wireless communications devices for both safety(IEEE 802.11p*) and non-safety(IEEE 802.11a/b/g/n) applications;these communication units enable the communication among vehicles (V2V)and with RSUs(I2V|V2I); Alternatively other communication like cellular radio networks (GSM,GPRS,UMTS,4G..) can be utilized if they are integrated in the OBU.The Application Unit (AU) runs applications that can take advantage of the OBU?s communication capabilities . A RSU is a physical device located along road and highways and equipped with the same communication capabilities as an OBU.It can serve for the OBU as a gateway(GW) to the Internet backbone or run applications that provide OBU with general safety information such I2V warning (e.g.work-zone warning).The network entities(OBU,RSU) and the communication capability (V2V,I2V), split the VANET?s architecture in 3 domains as shows in figure 1:

In-vehicle domain : consisting of an on-board unit (OBU) and one or more applications units (AU) inside a vehicle.

Ad hoc domain: composed of vehicles equipped with OBUs and RSUs forming the VANET.

Infrastructure domain: consisting of RSUs and wireless hotspots.

There are a broadly range of applications proposed for VANET, most of which come from manufactures and different project launched around the world. Raya and Hubaux (1) categorize VANET applications for example as safety-related applications and other applications (traffic optimization, electronic toll collection, Internet access..etc). Meanwhile , (2) classify safety messages into safety-related (latency is not critical) and safety-critical (latency is critical). However, Generally these fall into 2 main categories:

Safety applications: applications that are intended to reduce traffic accidents and to improve general safety. they can be further classify in safety related and safety critical.

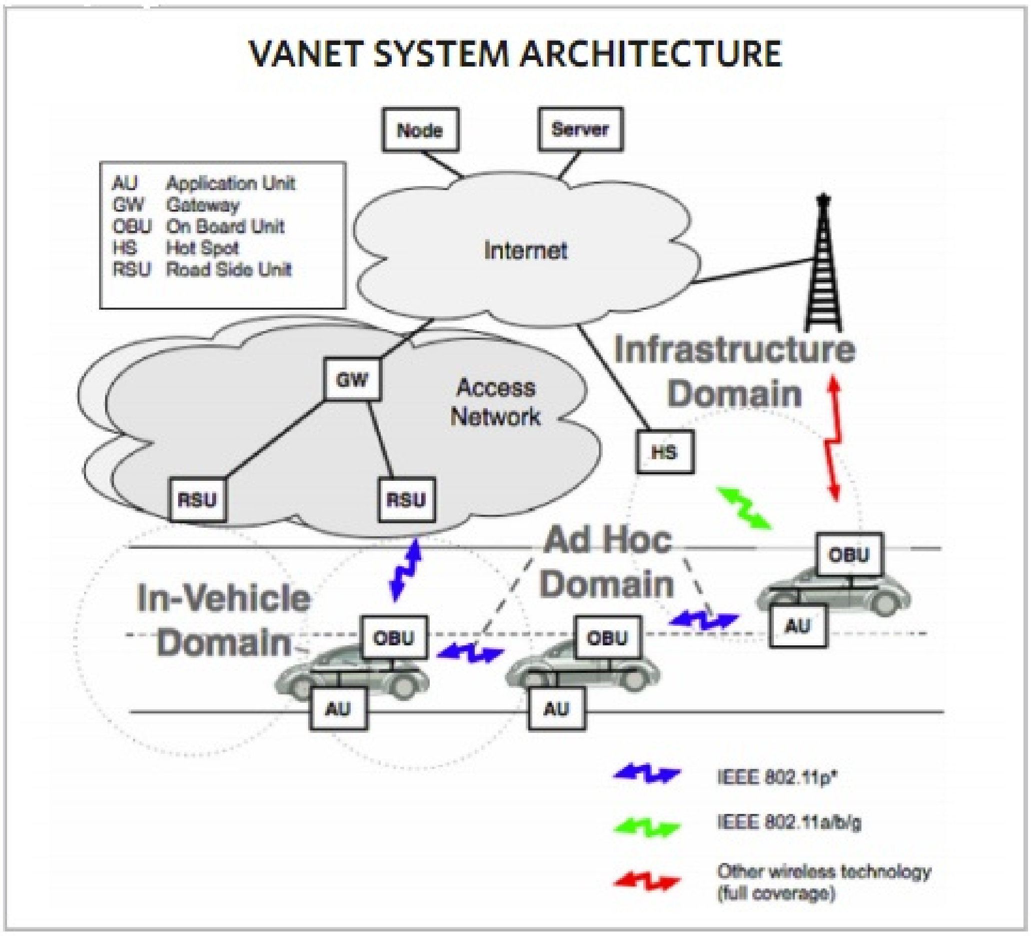


Figure 1.1: VANET?s system architecture.

Safety-related:applications that are intended to reduce traffic accidents and to improve general safety. they can be further classify in safety related and safety critical.

Safety-critical:application that have tremendous impact on safety improvement (e.g. used in hazardous situations,intersection collision warning).Such application access the communication channel with highest priority. In this case latency plays a vital role, what means that security protocol overhead and processing times should be kept at a minimum .

Internet Connectivity related: Application that increase the driving comfort; the so called ? deployment applications?. RSUs, which are directly connected to the Internet infrastructure provide infotainment experience like audio and video stream-ing.Example of such applications are parking spot locator service,wireless vehicle diagnostics,electronic toll collection.

To support Intelligent Transportation Systems (ITS) applications,a new wireless technology was designed called Dedicate Short range communication(DSRC). The DSRC is a short to medium range communication intended to support both public safety and licensed private services over roadside-to-vehicle and vehicle-to-vehicle communication channels. DSRC is meant to provide high data transfer rate and minimum latency in small communication zones (3) . Actually,different DSRC standards are in use in the US and in Europe but are not at present compatible.However recently,there have been effort by member of IEEE, ISO and ETSI to integrate these different standard into a single worldwide standard (4).

In the US

In October 1999,the U.S FCC allocated 75MHz of spectrum in the licenced ITS band of 5,9 GHz(5,85-5.925) primarily for vehicle safety service. In 2003, The American Society for Testing and Materials (ASTM) approved the ASTM-DSRC standard (published as ASTM E2213-03) which was based on the IEEE 802.11a physical layer and 802.11 MAC layer.

For safety application in VANET, the radio system need to maintain a respectable quality of service with regard to latency(transmission delay) and reliability(channel throughput and packet reception rate) in the sending, receiving and forwarding of messages (5) . However, Traditional IEEE 802.11 Media Access Control (MAC) operations suffer from significant overheads when used in vehicular scenarios. Additionally the high mobility of node result in sporadic connection, high packet errors and decreased decreased channel throughput.

To tackle the problem related to the Media Access Control and cope with the stringent time requirement of safety applications,the ASTM 2313 working group migrated to the IEEE 802.11 standard group which renamed the DSRC to IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) (6).The IEEE 802.11p standard is a modified version of 802.11a and has been adopted as the radio specification (physical and MAC layers) suitable for DSRC safety applications.The main difference to the a-variant lie in the parallel use of multiple wire free channel and the establishing of a control channels. Indeed,the DSRC spectrum is divided into 7 channels each of which is 10 MHz wide.There is a control channel (178) for network control and safety communication and two other (172,184) for safety and high power public safety applications respectively. Additional 2 aggregate channels (175,181) are included. The remaining channels are available as both safety and non safety channels. Figure 2. shows the channel allocation in the United State of America (7).

How it' s work ? The RSU advertises periodically (beacons) on its control channel the available applications of different service channels and accident warnings. All node (OBUs)

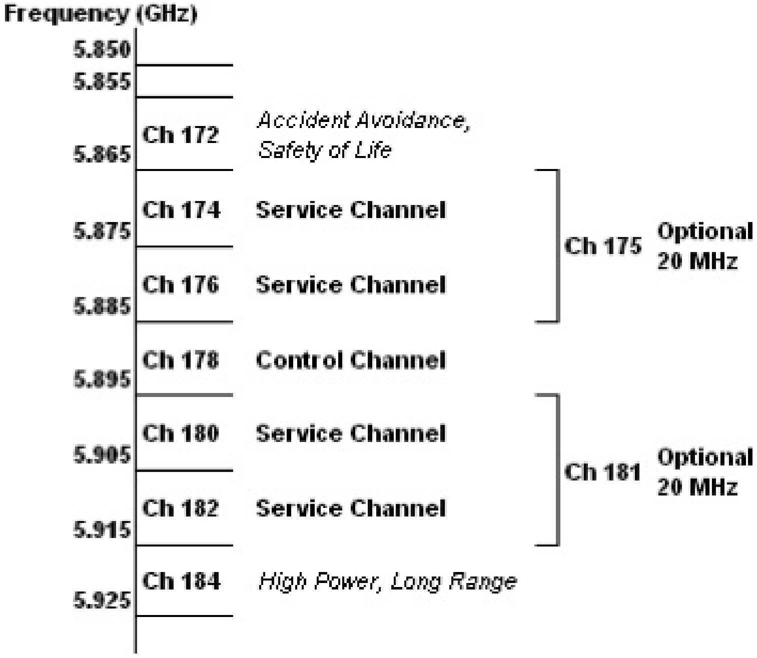


Figure 1.2: Channel allocation in the USA.

must listen on the control channel and executes firstly safety application,switch and then executes non-safety applications.

The DSRC communication stack(Figure.3)containing IEEE 802.11p and IEEE 1609.x is collectively termed as Wireless Access for the Vehicular Environment .The IEEE 1609.x represents higher communication layer for the DSRC standard.Their respective functionality are described in the IEEE 1609.x document series (8) Noteworthy here is the fact that IEEE 802.11p is limited by the scope of IEEE 802.11 which strictly works at the media access control and physical layers (9).

In Europe

The Car 2 Car Consortium (C2C-CC) is a non profit organization launched by European vehicle manufacturers and many other research organizations aiming at increasing the road traffic safety and efficiency (10).To achieve this goal,the C2CC-CC work tightly with European and international standardization organizations in particular ETSI TC ITS to create a European standard for vehicular communication.

In August 2008 the European Telecommunications Standards Institute (ETSI) has allocated 30 MHz(5.875 GHZ - 5.925 GHz) of spectrum for safety applications in the 5.9GHz band for ITS.Moreover 20 MHz have been requested as future extension for road safety and traffic efficiency (5.905 GHz - 5.925 GHz).20 MHz have been as well requested for non-safety ITS applications in the band below 30 MHz. A more detailed description on the frequency allocation can be found in the ETSI technical reports (11; 12).

Figure 5 show an overview of the Car to Car Communication Stack.The C2C-CC consider the IEEE 802.11p*[1] as the technical basis for radio communication channel .To support different type of applications, the protocol architecture propose[2] (4):

- C2CC-dedicated channels for
  - network control and critical safety application
  - road safety and traffic efficiency application
  - non-safety related C2R and C2C applications
- public channel as specified in the IEEE 802.11a/b/g within the frequency band allowed for Wireless LAN in Europe,in accordance with regional limitation

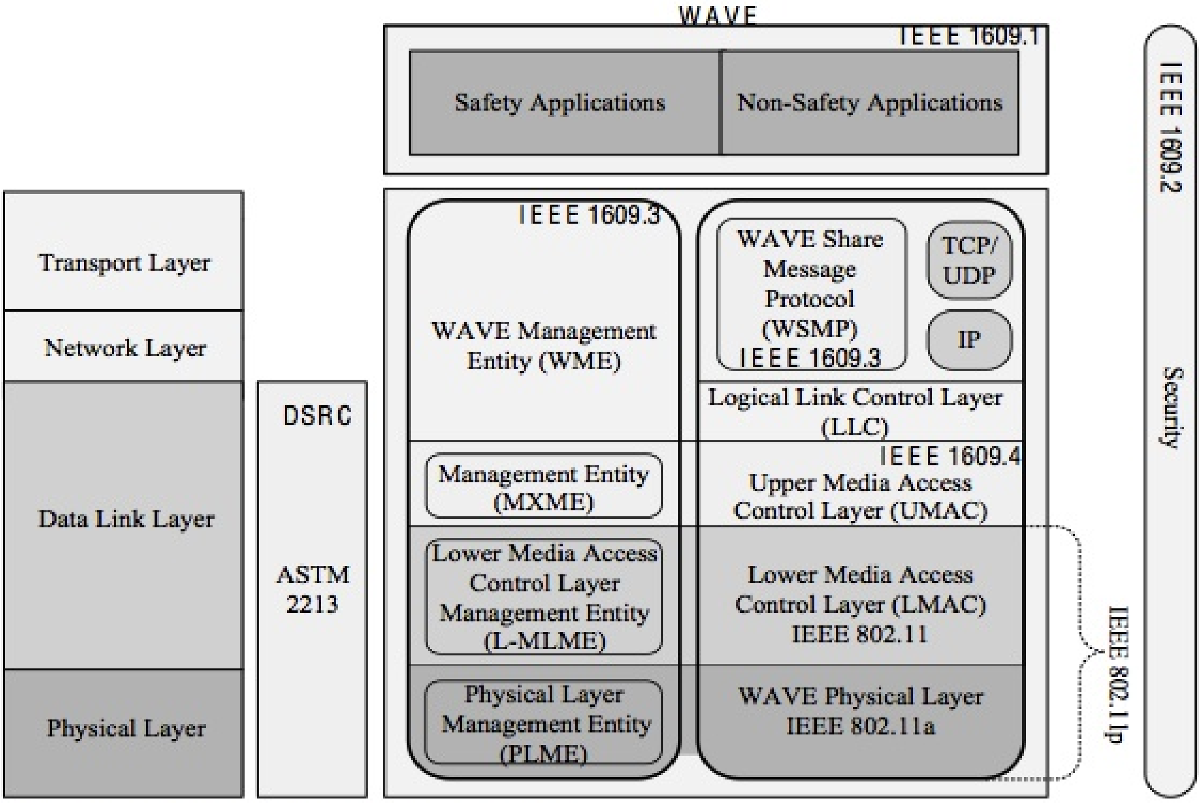
To ensure that non safety application does not block safety application,safety messages are treated with higher priority than non-safety messages.Thence, safety application can access protected radio as dedicated radio frequency as specified in IEEE 802.11p and IEEE 1609.4 MAC layer extensions as part of the IEEE 1609 standard family.

On top of the radio protocol layers MAC and PHY,the C2C Communication Network layer provides wireless multi-hop communication based on geographical addressing and routing. Precisely,Position Base Routing(PBR) is used to provide wireless multi-hop communication between two nodes(unicast using ?greedy forwarding?) and efficient broadcast of data packets in geographical areas(geocast). Main components of this routing protocol are beaconing and location service: Using beacons, a node periodically advertise his current status (identifier, speed,location,heading) to nearby nodes.This information is then stored in the location table of the mobile node?s OBU,which is then used to forward packet to a specific node in case of geographical unicast.Indeed, through a Location service the current position of a destination node can be determined.

A particular module in Figure 6 is the Information Connector (IC). Its main task is to efficiently coordinate the cross-layer data exchange among the different layers of the protocol

[1] IEEE 802.11p* refers to a variant of IEEE 802.11p adapted to the European conditions.

[2] Only the dedicated C2C-CC Channels are mandatory,the other are optional for the C2C-CC Radio System.


WAVE
IEEE 1609.1
Safety Applications
Non-Safety Applications
IEEE 1609.2
Security
Transport Layer
Network Layer
Data Link Layer
Physical Layer
DSRC
ASTM 2213
IEEE 1609.3
WAVE Management Entity (WME)
Management Entity (MXME)
Lower Media Access Control Layer Management Entity (L-MLME)
Physical Layer Management Entity (PLME)
WAVE Share Message Protocol (WSMP)
IEEE 1609.3
TCP/ UDP
IP
Logical Link Control Layer (LLC)
IEEE 1609.4
Upper Media Access Control Layer (UMAC)
Lower Media Access Control Layer (LMAC) IEEE 802.11
WAVE Physical Layer IEEE 802.11a
IEEE 802.11p

ASTM: American Society for Testing and Materials
DSRC: Dedicated Short Range Communication
IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

Figure 1.3: Wireless Access in Vehicular Environments (WAVE), IEEE 1609, IEEE 802.11p and the OSI Reference Model (9)

stack .

VANETs are the most promising instantiation of Mobile Ad hoc Networks. Although sharing some of MANETs' s features like short radio transmission range, self-organizing,self- management, and low bandwidth,VANETs differs from other ad hoc network as follows: *a*) Dynamically changing topology due to high mobility between nodes; *b*) No considerable power constraint; *c*) Sporadic connection caused by high speed movement; *d*) movement pattern prediction.

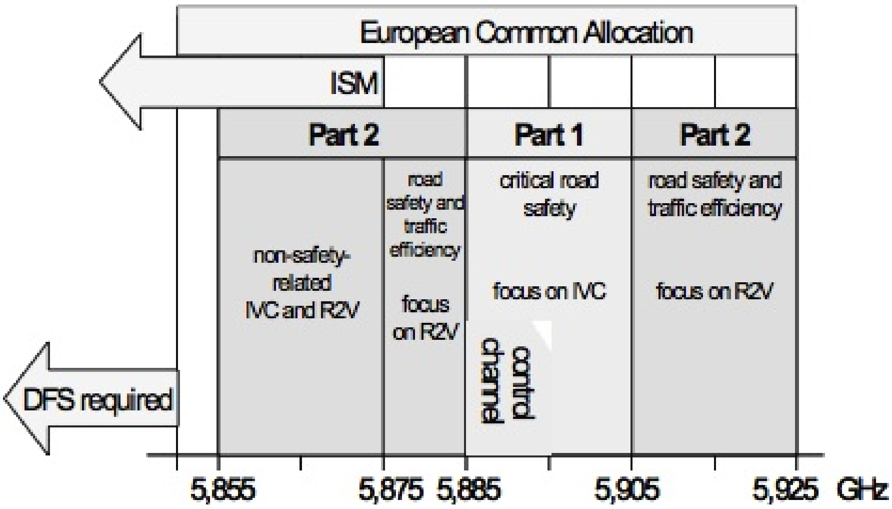


Figure 1.4: Requested frequencies in Europe (taken from ETSI TR 102 492-2)

1.3 Problem statement and contribution

1.3.1 Problem statement

The Car-to-Car Communication (C2CC) enables vehicles to exchange data autonomously among each other via a standardized radio interface without needing to rely on the existence of any infrastructure.These data collected by systems such as rain sensors, ABS and temperature gauges can provide insights on current road or weather conditions, then be relayed to others, thus ensuring more safety on the roads.

Despite its benefits, inter-vehicle communication (IVC) systems opens also opportunities for abuse when defective data have been received because data have been manipulated on the link or the source in another vehicle has generated faulty information by claiming for example a false Identity.

In this context, Public Key Infrastructure have been proposed to secure VANETs.A PKI enables drivers to securely exchange beacons through use of public/private cryptographic key pair that is obtained and shared through a trusted authority.

Although this scheme can effectively meet the mandatory security requirements like message authentication and non-repudiation,its communication and computational high cost

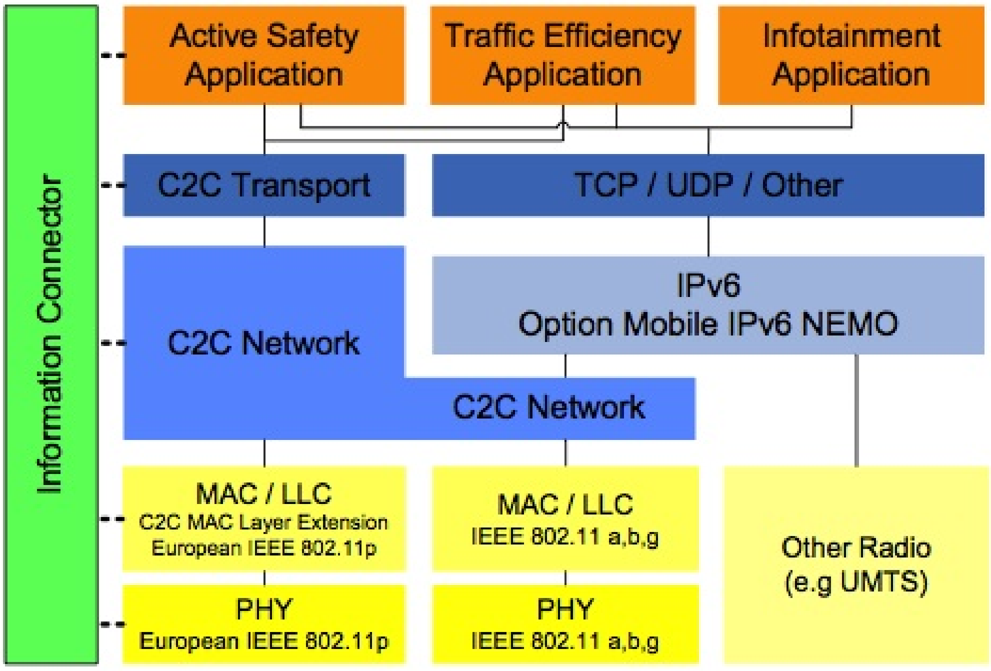


Figure 1.5: Protocol architecture of the C2C Communication System[14]

overhead does no cope well with the real time constraint of safety applications.

Authentication has to be performed before data can be validated.For example,in a real traffic situation due to the dynamic nature of VANETs and the broadcast transmission of safety message, a vehicle will receive a magnitude more packets than it sends and thus resulting in having to do more signature verification than generation.In this regard, it is imperative that the execution speed of cryptographic operations meet the real time constraint of safety applications,since computational load is in great part determined by signature verification.

In general, authentication protocol based on asymmetric cryptography are less efficient than scheme based on symmetric cryptography.To mitigate the problem related to the PKI,researchers have tried therefore to come up with lightweight solutions based on symmetric primitives or to try to find a trade off between security and authentication .

1.3.2 Contribution

All the proposed lightweight scheme however have felt to provide a completely PKI less solution in large part because symmetric cryptography is unable to provide repudiation.Moreover,the proposed scheme were intended for both form of communication namely I2V and V2V,which in our opinion felt to consider the individuals characteristics of VANETs's entities and applications.

Road Side Units for example,which are located along the road are different in nature from car driving by men as the doesn't need privacy and cannot be taking accountant for their actions like drivers.

We think that looking for a general approach based on both communication form is an objective,however finding immediate solutions for a set of applications based on their characteristics can reduce the total overhead of C2X and enhance the responsiveness of safety related applications.

We propose therefore a lightweight authentication scheme for I2V applications aiming at reducing the overall computational overhead of cars when they encounter Road Side Units.

The scheme is based on Cryptographically Generated address and one-way chain .

1.4 Outline of the Thesis

The remainder of the thesis is organized as follow.Chapter 2 provide an overview of security in VANETs and also a survey on related works .Chapter 3 present the steps that we took to come up with a lightweight solution.Chapter 4 identify the I2V applications .Chapter 5 describe and analyze our scheme.Finally, conclusion and future work are described in Chapter 6 .

2 Security in vehicular Ad Hoc Network and related work

2.1 Introduction

Nowadays,there is always some people trying to take advantage of other for profit , for gain or even simply just for fun. A malicious entity (e.g drivers or RSU) for instance may deliberately broadcast false safety message or bogus information to create confusion in the network and thus inevitably endanger the life of humans.Moreover,the periodically broadcasted heartbeat message contains user?s identities and current status. This information if not correctly protected could be used to profile drivers. therefore,it is thereby inevitable that the future deployment of VANETs will depend heavily on the degree of trust user (e.g driver) will have with any VANET?s entity or application and the capacity of the system to determine the liability of drivers while still preserving their privacy.To reach this goal,it is important not just to determine the features that make VANET secure,but also to consider potential threats on those security features in order to define efficient security mechanisms.

2.2 Security requirement

A safety application in VANET depending on its specificity should guaranty some of these following features:

Integrity or message authentication: integrity is the service that detect the alteration or destruction of information from unauthorized entities since it was created,transmitted or stored.

Authentication: Authentication is the assurance that the received message come from a trusted entity.This mean verifying that users are who the claim they are.

Non repudiation: Non repudiation is the service that prevents either sender or receiver from denying a transmission message.This requires a mutually trusted third party or PKI.

Availability: Availability is the property of a system to provide to its authorized users a timely and reliable access to its service .

Conditional privacy: Privacy is the property that keep information away from unauthorized observers. The attacker should not be able to reveal a driver?s identity or trace his trip path.However privacy is not generic and depend on the individual background or the geographical position(e.g Afghanistan and Germany). Additionally in case of accident or dispute,authorities should be able to reveal the real identities of concerned parties

2.3 Security threat

Like every network system VANET is also vulnerable to attacks. Raya et al. (13) categorizes the capacities of attackers in 3 dimensions: ?Insider vs outsider?, ?malicious vs rational?, and äctive vs passive.Adrian Perrig and Bryan Parno (14) recognizes the following class of adversaries :?greedy drivers?,?Snoops?,?prankster?,?industrial insiders? and ?malicious attacker?. These security threats are in the most part against the above presented security features. Our intention is not to be exhaustive,but to present the most basic attacks on vehicular network.

Threat on the integrity or the message authentication

Masquerading: The attacker assumes a false identity and can use it to impersonate a Road Side Unit or an emergency vehicle for example.

Replay Attack: The attacker re-injects in the networks already received message at another point of time in order to take advantage of the situation,which prevailed before.For receiver the message look valid,but it?s actually obsolete.

bogus message attack: The attacker inject purposely fake message into the network to disrupt the traffic circulation or simply to quench a selfish behavior (e.g., to divert the traffic from a given road and thus free it for themselves (13)).

Threat on the availability

Denial of Service Attack: The adversary prevents the user from having access to offered network service or resources. To achieve this, it could for instance jam the communication channel or send flood messages in order to overwhelm the node resource such that it can?t perform another task.

Black Hole Attack: In this attack a Node ,which is used to further propagate a message toward a destination constantly drop out from the network or drop the message preventing the sender to reach its destination. In fact the malicious node can claim to have the shortest path toward a destination causing thus all message to pass through him.

Threat on the privacy

Big Brother attack: In this attack,the adversary disclose the ID of other vehicle in order to track their location. An adversary for instance could blackmail a user based on the gained location information;the user might have been in a place he want to keep secret .

2.4 Related work

2.4.1 On VANETs Security mechanism

Safety applications use broadcasted beaconing to enhance traffic circulation or to prevent user from potentials dangers. Only through analyze of reliable data can a safety application make accurate decision. There have been extensive research's on how to implement VANETs security requirements,which have to be understand as building blocks when apply to safety applications. However,the industry have commonly agree on one point:In VANETs, driver encounter entities they never meet before and accountability of action is mandatory,Therefore referring to the state of art in cryptography,asymmetric cryptography is the best choice,since its quite impossible task for its counterpart symmetric cryptographic to provide non repudiation and authenticate strangers .

In this order of thing ,Raja and Hubaux propose in (13) the use of a Public key Infrastructure (PKI) and digital signature to guaranty message authentication and non repudiation. In this scheme each vehicle V or referred as On Board Unit is assign a public /private key pair noted . Before sending a message (M), a vehicle sign it with its corresponding private key SK and include the CA's (Certificate Authority) certificate C,which bind the vehicle's public key to the identity of the driver as follows:

$$V \rightarrow * : M,\ [M|T]_{sk}, C \tag{2.1}$$

Upon receipt of the message, the receiver extract the message M and verify the public key of the sender using the certificate and the Certificate Revocation List (CRL) which list excluded certificate from the network. Finally it verify V's signature using its certified public key

Likewise,to address the security issue in VANETs,the IEEE 1609.2 trial-use standard (15)for Wireless Access in Vehicular environment has been developed.This standard defines several mechanisms to protect message against attacks like spoofing,eavesdropping to name a few in a WAVE environment.

This standard also identify the use of a PKI for message authentication and recommend the utilisation of Elliptic Curve Cryptography (ECC) as public key cryptography standard. Broadcast messages (e.g., safety vehicle warnings, vehicle safety messages) are defined as only being signed and, in general, not encrypted and as such, asymmetric techniques are again defined to be ideal (16).

Safety message are intended to be of public usage and will not contain secret message. However, the periodically heartbeat message,which contain identifiers and location information could be subject of attack related to privacy.The IEEE 1609.2 standard recognize the importance of this requirement but does not define a mechanism to provide anonymity.

To address privacy issue Raya et al. in (17) suggested to use temporary pseudonym to achieve anonymity. In their scheme vehicle are preloaded with a bunch of short lived anonymous key pairs together with their corresponding public key certificates. According to (17),an anonymous key pair is a public/private key pair that is authenticated by the CA and which doesn't allow a third party to gain information about the vehicle real identify without a special authorisation. Each public/private key are utilised for a short period of time to assure anonymity. A variation of this scheme can be found in (18; 19).The first make use of group signature to overcome the large key storage and management required in (17) . The latter is a hydride scheme that couples the traditional PKI based scheme with the group signature based scheme aiming at mitigate the high computational overhead observed in (18).

2.4.2 On lightweight security protocol

Secure message format involves the uses of signature and certificate. Although the proposed security mechanisms meet the mandatory security requirement like authentication and non repudiation,they introduce a significant amount an overhead due to the computational high cost caused by the use of public key cryptography and the enormous cost of maintaining an up to date certificate infrastructure in which it sometimes may be impossible for a node to establish timely communication with a CA (Certificate Authority) or a CRL (20). For instance,in case of misbehavior or key expiration, the anonymous credentials belonging to a vehicle [1] must be revoked and put in the CRL.The drawback of this scheme is that the CRL may grow quickly in case of multiple misbehavior vehicles so that it might take more time to check the validity of a certificate and consequently of a safety message.

Any delay overhead introduced by an authentication is not tolerable considering the real-time reaction required for safety application.Consequently,there have been tentative in the research to alleviate the drawbacks related to the use of a PKI as a basis for authentication.

Any delay overhead introduced by an authentication is not tolerable considering the real-time reaction required for safety application.Consequently,there have been tentative in the

research to alleviate the drawbacks related to the use of a PKI as a basis for authentication .

In this term F.kargl et al. in (21) proposed in their scheme 3 strategies to reduce this overhead:

Caching: if communication partner have previously exchanged their certificate, they could cache already verified certificates and thus subsequent beacons can be verified without cryptographic operations.

Omitting signature generation: generally all beacons are not safety related and therefore,depending on the situation,one can based on a periodic schedule selectively activate signature.

Omitting signature verification: the idea behind it is to let the OBU on the receiver side controls its computational load (i.e.,decide which signature to verify or not).

This scheme balance well security and efficiency.Another recent work paper promises to eliminate channel overhead and eliminate the use of (22).However the 2 schemes still maintain the existence of a public key infrastructure as basis for message authentication.

Road Side Unit as well are used in a number of scheme to provide lower overhead. In (22; 23), the authors used as building block RSA and MAC as encryption means to provide message security and uses RSU to validate the message integrity.However, the vehicle in their scheme are unable to authenticate across communication range because the session keys used at different RSU ; additionally when moving from A RSU to another,the new RSU must obtain the vehicle?s certificate for authentication thus making the scheme inefficient in a global way .The work in (24)intend to alleviate these 2 problems .

The above schemes are the closest related to our scheme.Although taking advantage of the efficiency of symmetric cryptography,they still depend on certificates issue by the CA and consequently of the PKI.

3 Methods

Obviously,message authentication is the security features that take a toll on a total message size(signatures,certificate) when considering actual solutions based on PKI. Taking a different route inevitably comes to regard infrastructure less protocols and protocols based on symmetric buildings blocks as an alternative to provide authentication.Additionally, key exchange protocols has to be considered since symmetric credentials need to be exchanged between parties before communication.
We have considered severals protocols based on a bright perspective about the issues the solves in cryptography and then we have apply them in the context of VANETs aiming to get some insights.

3.1 Preliminaries

3.1.1 One way hash chain

One way hash chain is a cryptographic primitive that use a one-way hash function $H(x)$ to generate a sequence of random value from a selected seed h_n that serve as authentication keys. The important properties are:

1. $H(m)$ can take a string of any length as input and produce a message digest of a fixed-length output,which is defined as: H : $0, 1^* \rightarrow 0, 1^\phi$,where ϕ is the length of the output of the hash function .

2. Given m, it is easy to compute $x = H(m)$, but hard for a given x to compute m such that $m = H^{-1}(x)$, this concept is related to that of *one way function*.

3. Given m , it is computational infeasible to find $m' \neq m$ such that $H(m') = H(m)$.This property is sometime referred to as *weak collision resistance*.

4. It is hard to find any two pair $mandm'(m \neq m')$such that $H(m') = H(m)$.Such a pair is called *a cryptographic hash collision*, a property which is sometime referred to as *strong collision resistance*.

Figure 3.1 shows the application of the hash function $H(x)$ on h_n . To generate a chain of length $n - 1$,the first element of the chain h_n is randomly picked and then the chain is generated by successively applying a one-way function(denoted as H in figure 3.1). In utilization and revelation of these chain element ,we use the reverse direction of the chain generation starting from h_1. Each chain element h_i is the commitment of the subsequent element in the chain, for example h_1 is the commitment of h_2,h_3,...,h_n . Any element of the chain h_j can be verified from $h_i(1 \leq i < j \leq n)$ to be an element of the chain by applying H successively $j - i$ times, that is ,$h_j = H_{j-i}(h_i)$ .The owner can create he chain all at once and stored it , or starting from h_n compute on demand the other element of the chain in this oder $h_n - 1, h_3, \ldots, h_2, h_1$.

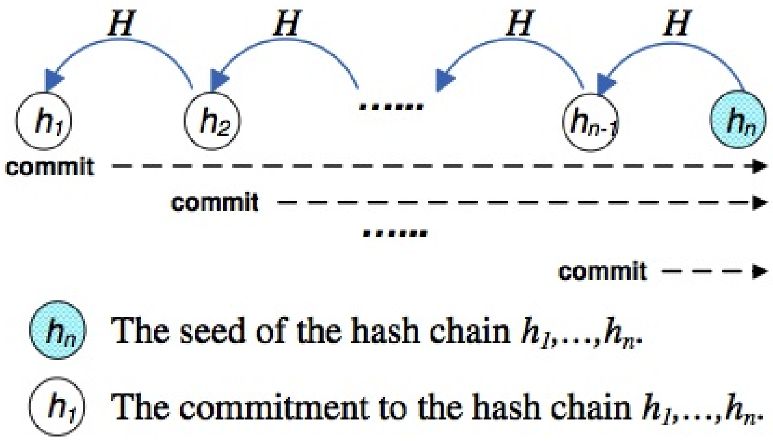

H
H
H
H
h1
h2
......
hn-1
hn
commit
commit
......
commit
hn The seed of the hash chain h1,...,hn.
h1 The commitment to the hash chain h1,...,hn.

Figure 3.1: One-way hash chain(25)

3.1.2 Message Authentication Code (MAC)

A MAC is a cryptographic primitive used to provide message authentication . Precisely, a cryptographic checksum that is generated based on a message M of variable length using a secret key K as follow: $MAC = C(K, M)$.

Before starting a communication the parties in presence must agree on a shared secret key K as in the case of symmetric encryption .

A cryptographic hash function is used by the sender to produce a MAC. The MAC is then send to the message receivers along with the message M . At receipt of the message, the receiver computes a MAC on the received message M with the same key K and hash function as was used by the sender . If the two value match, then the message is valid and the receiver can be assured of the origin and the integrity of the message.Figure 3.2

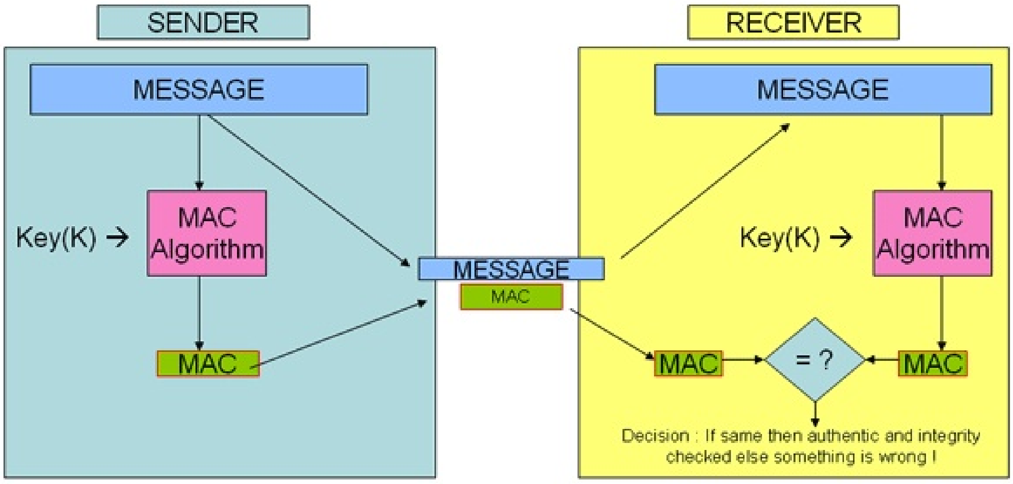


Figure 3.2: Illustration of the MAC(26)

illustrates the protocol.

HMAC is a special algorithm, which combines a cryptographic hash function and a secret key to generate a MAC.

3.2 Reviews of considered protocols

3.2.1 Lamport's password

Lamport was the first to propose the use of one way hash chains as a password protection in an insecure communication channel (27).

In this protocol, after an authenticated initial password exchange between the client and the server, the server store n and the n-fold hash of the password:
$[n, h^n(pwd)]$.

For each authentication,the user logs in the server ,which trigger it to respond with a prompt n. The user machine calculates then $x = h^n - 1(pwd)$ and send this to the server.

The server computes $h(x)$. If the value obtained after the hash function match the one it has stored before, then the login is successful. The server update its values $[n = n - 1, x]$.When n reach 1,the password need to be reset.

Although widely used for authentication in ad hoc network,lamport's hash chain does not provide however entity authentication. 1 gives an algorithm description of the scheme.

Algorithm 1 Lamport's password algorithmus

```
At startup,the servers stores:$n, userID, y = h^n(pwd)$
foreach authentication do
    user log in with his userID.
    server reply with a prompt n
    user then computes and send $x = h^n - 1(pwd)$
    server calculates $k = h(x)$
    if (k==y)
    then $y = x$;n=n-1;accept;
    else reject;
    end if
    When n reach 1,the user need to reset the password(pwd)i.e back to 1.
end for
```

3.2.2 TESLA-broadcast authentication

Tesla(Timed Efficient Stream Loss-tolerant Authentication) (28) is an efficient broadcast authentication protocol,who achieves asymmetric properties through loose time synchronization and using essentially purely symmetric cryptographic functions like MAC .
The main idea is that after time synchronization between communication partners , the sender generate a one way hash chain keys know only to itself and then reveals theses values in the opposites order .

Precisely , the sender divide the time into uniform intervals of durationT_{int} (i.e.,time interval 0 will start at time T_0,Time interval 1 at time $T_1 = T_0 + T_{int}$) and assign to each interval one key k_i of the one way chain. Before sending a message m_i at the current time interval t_i,the sender computes the packets with his correspondent key k_i and send it to the receivers .

The receivers buffers the received packet without being able to authenticate it . After a specific time ,which we call the key disclosure delay ,the sender disclose k_i and the receivers is able to authenticate the packet or the packets he has buffered following the principle of commitment of the one way hash chain .This implies that, in oder for the receivers to proceed a successfully authentication and be able to resist to collusion , the receiver must obtain from the sender the following elements through an authenticate channel :

1. Time interval schedule: interval duration T_{int}, start time T_i and index of interval i, length of one-way key chain.
2. Key disclosure delay d (number of intervals).
3. A key commitment to the key chain k_i (i$< j - d$ where j is the current interval index).

A required property of Tesla stipulates that the receiver does not need to know the exact δ(i.e.,the exact difference between the sender and the receiver's time) but only an upper bound on it, Δ,which is referred to as the maximum time synchronization error [8]. figure 3.3 describes the Time Synchronization :

At the beginning of the protocol,the receiver store his local time t_R and request a time synchronization containing a randomly chosen nonce(1),at this moment the sender's clock is t_1.Upon receiving the synchronization request,the sender S stores his local time t_S and replies with a signed packet (2)[1]containing t_S and the nonce it previously received.
To validate the packet the receiver R verifies his digital signature and check if the received nonce is the same as its own. If the verifications are successful,then the receiver stores t_R and t_S and calculates the upper bound on the sender's clock at local time t as

[1] At setup,we assume,the sender posses a public/private key pair (SK,VK) and that the receiver,through a mechanism is able to gain the authentication keys VK.

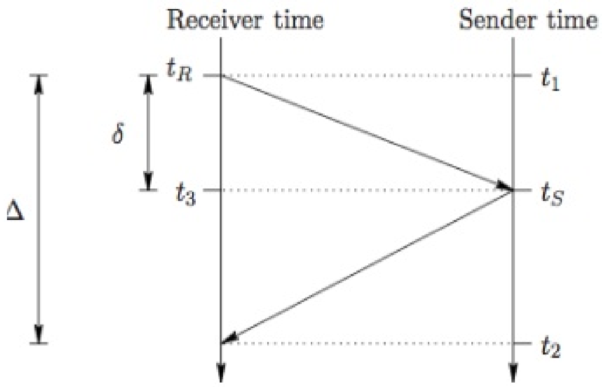


Figure 3.3: Time synchronization between the sender and the receiver(28)

Algorithm 2 Tesla brodcast authentication (28)

```
1: Initially,A signs $S := [k_0]_{sk}$ and broadcast S.Each verifier verifies S.
2: for message $m_i$ in time interval $t_i$, $i = 1$ to n do
3:     A computes $M_i := MAC(m_i, k_i)$ and broadcasts $M_i, m_i$.
4:     Each receiver checks wether he received $M_i, m_i$ in time interval $t_i$ and buffer it.
5: end for
6: for message $m_i$ in time interval $t_{i+1}$, $i = 1$ to n do
7:     A broadcats $k_i$
8:     Each receiver checks wether $M_i =?MAC(m_i, k_i)$.
9: end for
```

$t_s \leq t - t_R + t_S$.
After this,the real synchronization error is δ as shows in figure 3.3. However since the receiver doesn't know the real propagation delay,it muss assumes that the time synchronization error is Δ or (the full round-trip time(RTT)).The authentication algorithm is described in Algorithm 2

$R \to S : Nonce(1)$
$S \to R : \{t_S, Nonce\}_{sk}(2)$

3.2.3 Zero Common Knowledge(ZCK)

ZCK (29) is a very lightweight security protocol not intending at inferring involved entities identities, but aiming at recognizing foreign communication partner whenever the meet for the first time.

In most case to establish a trust relationship,entities often relies on a logical and commonly agreed trust authority, however it happen that the nodes involved belong to complete different administrative domains or they are unable to reach the authorities. Hence ,in both case they cannot easily establish a trust relationship .

Taking into account those facts and the claim that without a previous knowledge of the involved parties (knowledge generally held in a PKI or by trusted third party) , the best one can do is to recognize.Consequently Zero common-knowledge authentication define his secure objective as follow: 1. A recognizes B, if is able to identify again the authority that runs B or; 2. B authenticate to A ,if B is able to convince A that both had some relation in the past .

Algoritm 3 (29)describes ZCK in a general manner:here the entity B after generating randomly a secret key x,send his public key $f(x)$ to A.Then A and B perform a challenge-response protocol.

Algorithm 3

```
1: B generates x S at random
2: B sends $f(x)$to A
Repeat Step 3 to 5 for each authentication process
3: A sends random r to B
4: B sends authenticated $(r)_x$ to A
5: A checks if $((r)_x)_{f(x)} = r$
   If yes A accepts,otherwise rejects
```

To prevent an entity to inject his public-key to a service he did not offer, the public-key is associated with the service. As a result we have a slightly improved version Algorithm4 .Step 3 and 4 of Algorithm 3 are replaced by the step 3 and 4 of Algorithm 4 (29).

Algorithm 4

```
Repeat Step 3 to 4 for each message to authenticate
3: B sends $(m)_x$ to A
4: A checks if $((m)_x)_{f(x)} = m$
   If yes A accepts,otherwise rejects
```

From this general description of the ZCK two instantiations arise:

- ZCK based on traditional signature schemes like MAC and public key cryptography:

Here authentication is done by the proof of knowledge of the secret key in a challenge and response manner.

- ZCK based on symmetric cypher:Here the protocol requires a secret channel to exchange the shared secret a priori.

However,the high computation of public key cryptographic and the permanent key exchange due to changing topology in a pervasive environment overstrain the capacity of weak devices. As a result , a lightweight solution seems to be more appropriate.

ZCK key-chain scheme only requires the use of one way hash chain, which is more efficient than any public-key schemes. Let consider f a function that maps the identity ID to a bit string,r_{ID}, be t-bit random strings, and θ be an operator on bit strings.In a section involving A and B,x_0^A is A private's key and x_0^B is B private's key. From their respective global keys (x_A^G, x_B^G),identities (ID_A, ID_B),and random value (r_A, r_B) one can derive the value of their corresponding private keys $x_0^A = x_A^G \theta f(ID_B) \theta r_A$ and $x_0^B = x_B^G \theta f(ID_A) \theta r_B$.These private keys are actually anchors from a one way chain,which after n applications of an one way function h give respectively $x_{n_A}^A$ and x$_{n_B}^B$,which are called the public key of A and B.The protocol work as follows (29):

Algorithm 5

```
1:A sends her public key $x^A_{n_A} toB$, who stores $(x^A_{n_A}, r_B, n_B, 1)$
2:B sends her public key $x^B_{n_B} toA$, who stores $(x^B_{n_B}, r_A, n_A, 1)$
Repeat Step 3 to 9 for each authentication process
3:Assume A stores $(x^B_i, r_A, j, u)$ and B stores $(x^A_j, r_B, i, v)$
4: (+) A sends authenticated messages $(m)_{x^A_{j-u-1}}$to B
5: (+) B sends authenticated messages $(m)_{x^B_{i-v}}$ to A
6: A open her key by sending $x_{j-1}$ to B
7: B checks if $h(x^A_{j-1}) = x^A_j$
8: For $k = 1tok' \leftarrow max\{u, v\}$ repeat Steps 8.1 to 8.5
   8.1: B opens his key by sending $x^B_{i-k}$ to A
   8.2: A checks if $h(x^B_{i-k}) = x_{i-k-1}$ to B
   8.3: A open her key by sending $x^A_{j-k-1}$ to B
   8.4: B checks if $h(x^A_{j-k-1}) = x^A_{j-k}$
   8.5: If any check fails,or the loop is interrupted ,A and B stop execution.
   Then A stores $(x^B_i, r_A, j, max\{u, k+1\})$ and B stores $(x^A_j, r_B, i, max\{v, k, +1\})$.
9: A and B stores the new values $(x^B_{i-k'}, r_A, j - k' - 1, 1)$
and $(x^A_{j-k'-1}, r_B, i - K', 1)$
```

3.2.4 Cryptographically Generated Address

A CGA is an IPv6[2] address for which the interface identifier (i.e., the least-significant 64 bits of the 128-bit IPv6 address) is generated by computing a cryptographic one way hash function of a public key and auxiliary parameter (30).
The message are signed by the corresponding private key of the address owner .To authenticate the message,the receiver muss know the public key, the source address and the values of the auxiliary parameters of the sender .This mechanism does not require the existence of a PKI .
In the following we will describe the CGA format /parameter ,then we describe the step needed for generating and verifying CGA.

CGA format

When talking about address ,we refer to IPv6 address in which the leftmost 64 bits of the 128-bit address form the subnet prefix and the rightmost 64 bits of the address form the interface identifier (30). The CGA has a security parameter (Sec) ,which determines its strength against brute-force attacks . It occupies the three leftmost bits(i.e.,bit 0-2) of the interface identifier. Other notable bits of the Interface identifiers are the 6th bit úb́it and the 7th bit or ǵb́it.

CGA parameters and Hash values

Every CGA address is associated with a public key and auxiliary parameters data structure. The public key muss be formatted as a DER-encoded ASN.1 data structure of the type SubjectPublicKeyInfo, defined in the Internet X.509 certificate profile (31).The following three unsigned integer are the auxiliary parameters:

- A 128-bit modifier : Implement hash extension and enhance privacy by adding randomness to the address.
- The 64-bit subnet prefix of the CGA address.
- an 8-bit collision count (value must be 0,1,2) : This parameter is incremented each time a duplicate address detection was detected upon the generated CGA address

The hash value Hash1 and Hash2 are computed with the SHA-1 hash algorithms from the concatenation of these above parameters . The SHA-1 hash algorithms produces a 160 bit hash value from which the 64-bit Hash1 is obtained by taking the leftmost 64-bit of the 160-bit SHA-1 hash value . The 112-bit Hash2 is obtained by the same process except that the

[2] In Ipv6 address,the leftmost 64 bits of the 128-bit address form the subnet prefix and the rightmost 64 bits of the address form the interface identifier.

subnet prefix and the collision count are set to zero.This being ,to define a CGA as an IPv6 address, the following condition must be satisfied:

- A 128-bit modifier : Implement hash extension and enhance privacy by adding randomness to the address.
- The first Hash1 value equals the interface identifier of the address (Sec bits, 'u' and 'g' are ignored in the comparison).
- The 16*Sec leftmost bit of Hash2 are zero.

A simplified CGA generation and encapsulation steps

the generation of CGA is also shown in Figure 3.4

- A private /public key pair is generated for a node.
- Interface ID is calculated as an public key fingerprint (Hash1 generation).
- InterfaceID and subnet prefix are concatenated to form and 128-bit Ipv6
- CGA parameter is formed : IPv6 address public key and auxiliary parameters
- After then the sender computes the signature of subnet prefix ,the public key and the data encrypted with his private key.
- Sender include the subnet prefix,the public key, and the signature in a CGA parameter within the packet
- Sender add data and sends the packet

A simplified CGA verification and decapsulation

- The verifier know the sender source CGA address .
- The verifier gets the sender public key from CGA parameter .
- The verifier checks the binding between the source address and the public key
- After then the digital signature of the packet is verified.

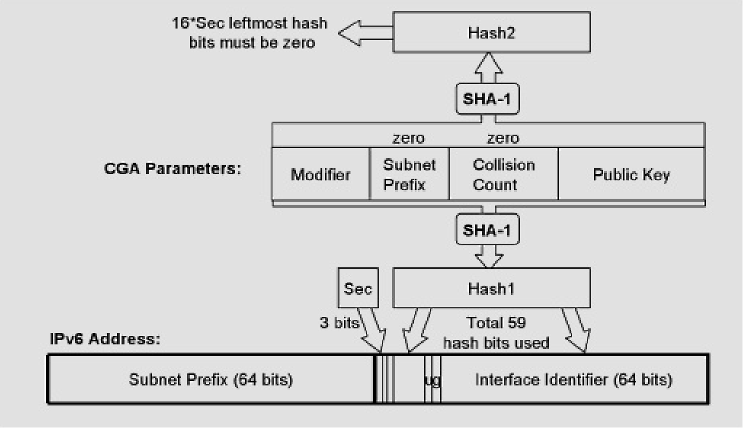


Figure 3.4: Detailed Data Flows in Address Generation of Cryptographically Generated Addresses (32)

3.2.5 Diffie Hellmann key agreement (DH)

DH is a key agreement protocol used by two parties to agree on a shared secret over an insecure medium. It was developed by Diffie and Hellmann in 1976 (33) in a paper called " New Direction in Cryptographic " The protocol work with two public system parameters p and g .Parameter p is a prime number and g (commonly know as the generator) is an integer less than p with the following property:
for every number n between 1 and p-1 inclusive, there is a power k of g such that $n = g^k modp$. Let suppose,Alice and Bob want to agree on a shared secret key using the DH.They will proceed as follow:

1. Alice generates a random private value $a \in N$
2. Bob generates a random private value $b \in N$
3. Alice and Bob derive their respectively public values from parameter p,g,a and b: $x^a = g^a modp; x^b = g^b modp$
4. They exchange their public values
5. Alice computes $g^{ab} = g^a x^b$, Bob computes $g^{ba} = g^b x^a$

6. $g^{ab} = g^{ba}$ and therefore Alice and Bob have their shared secret key.

The security of DH lies on the discrete logarithm problem.It is indeed computationally infeasible to calculate the shared secret key $k = g^{ab} mod p$ given the two public values when the prime p is sufficiently large.

3.3 Dolev-Yao- threat Model(DY)

To counterpart attacks on cryptographic protocol , it is essential to find systematic process , which could not just validate the security of cryptographic protocols , but at the same time predict possible attacks on these protocols. Danny Dolev and Andrew C. Yao (34) are the first to formally analyze crypto-protocols or 'ping-pong' protocols. In this thread model a malicious entity or node has the followings properties:

Eavesdropping :It can hear and filter any any message passing through the network.

Spoofing: It can send messages by impersonating any other member of the network.

Membership: It is a legitimate member of the network and thus can send and receive any message.

Limitation: Only the constraint of the used cryptographic methods limit its actions

Figure 3.5: A Simplistic Visual representation of the Dolev -Yao Model (35)

In the next section,we apply the Dolev-Yao model to detect vulnerabilities from the above presented protocols in the context of VANETs.

3.4 Flaws and benefices from the above presented protocols

3.4.1 Lamport Password

Flaws

No mutual authentication

Although this scheme is largely used, it doesn't solve the problem of identity authentication.The communication partner still have to find a way to prove their identity. Otherwise it is impossible for the client for example to know with certitude who is at the other end of the line.

Password Reset:

After n reach 1,the user must choose a new password and send it to the server

Small N-attack

Here the adversary impersonates the server . When the client tries to authenticate , the man in the middle (the attacker) queries with a small $n' < n$. After the man in the middle get the reply from the client he can then impersonates the client when n is decremented to n' .

Benefices

Secure against eavesdropping and replay Attacks

The scheme use a sequence chains of hash values and each chain values is just used once. In order to authenticate the user, the server muss know the sequence .

3.4.2 Cryptographic Generated Address (CGA)

Flaws

No Legitimation

Since the CGA are not certified any attacker can create a new CGA from any subnet prefix and its own or anyone else 's public-key .Thus making it hard to know wether the message is legitimate or not.

Prevent spoofing

The public key of the address is bound cryptographically to his CGA address. It uses the corresponding private key to asserts its ownership of the address and to sign message send from his node.

Benefices:

No Infrastructure

A node only need to have a public/private key pair and auxiliary parameter in order to generate a CGA. Messages can be protected by attaching the public key and auxiliary parameters and by signing the message with the corresponding private key [10].The only protection lies in the fact that an attacker cannot impersonate an address by signing message that appear to come from the owner of this address.

3.4.3 Diffie-Hellman Key exchange

Flaws

Man in the Middle Attack know as bucket-brigade

The D-H itself does not provide authentication of communication partners .Let's say Alice and Bob want to establish a shared secret key using the DH. Eve is a malicious entity ,which has the properties like described in the DY. To realize his attack, Eve open two section (i.e.;he intercept and substitute the message from Alice to Bob ,also the message from Bob to Alice with his own message).At the End,Eve has two keys (k_A, k_B) and can impersonate both Alice and Bob.Figure 3.6 schematize this attack.

Benefices:

No eavesdropping

The scheme is safe against passive eavesdropping,as the information transmitted in plain text is not sufficient to construct the key.

3.4.4 Timed Efficient Stream Loss-tolerant Authentication(Tesla)

Flaws

Impracticability

In highly dynamic networks such as VANETs,the mechanism by which a key is authenticated: clock synchronization ,delay estimation ,may become impractical

Benefices:

Low computational and data overhead

The scheme make use of symmetric cryptographic primitive like one-way hash chain and message authentication code(MAC),which requires less computation time than asymmetric cryptographic .

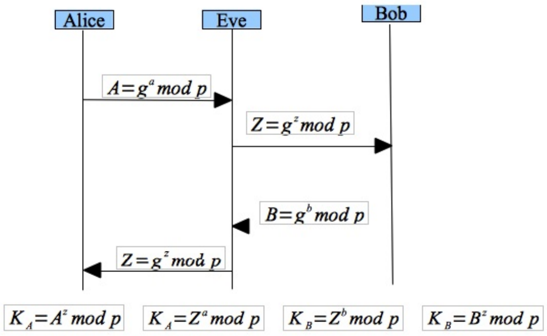


Fig.4 Man in the Middle Attack

Figure 3.6: Man In The Middle Attack

3.4.5 Zero Common knowledge

Flaws

based on recognition of entity

VANETs is a highly dynamic Network with vehicle driving in a random way (i.e., not following a specific route each time) over multiple authorities and domains . In our view , to make an assumption , that vehicle will retain information about every vehicle or RSU they encounter in oder to recognize them the next time the meet is not just unrealistic , but quite impossible since doing so will require a large amount of storage,which the vehicle doesn't have ; and in the case they do have : how much storage or number of vehicle will suffice?

The handshakes(Mutual recognition)

From the Initial key exchange , Just for the authentication of one entity there are alone about 5 exchanges. If we consider for example vehicles driving across a road and then an RSU standing along this road,which can detect vehicles coming from a reasonable near distance and make contact with them in order to warn or advertise them

.We consider that a mutual recognition exchanges just for one communication pairs is extremely high considering that the vehicle are driving at a reasonable speed .This might cause that some vehicles reach out of the range of the RSU before it can even contact them.

Benefices:

the man in the middle attack is of no effect

A reliable relay channel for the first recognition process is a requirement in a formal model [11]. Although this provide message integrity ,it doesn't infer entity identity . However this might be irrelevant also, because if an entity is interested at a service, and we suppose that the man in the middle was at the first recognition process between him and another entity (the real service provider) , it doesn't really matter for the service requester ,wether it is the man in the middle or the real service provider, if the attacker provide the required service with the same quality.

4 Identifying I2V applications

In VANET, vehicle sent at short interval of time status message,such as speed and position referred to as beacons.These message are evaluated by other vehicles and RSU,which are installed along the road .Through their position and the collected data, RSUs can make accurate decision about the state of the road and prevent unpleasant situation. Usually an accident on the road causes traffic jam and affect indirectly other vehicle. For example, an accident might occur at some kilometer away ; RSU having received information about an accident will prevent other vehicles who can choose to continue along the same road or to change. Previous and ongoing projects like row (36), FLEETNET (37) and the C2C-CC have brought up a broad variety of envisioned applications.

4.1 Application Description

The followings description are based on the I2C application identified in SEVECOM (38) .

4.1.1 Assist driver with signage

Traffic signal violation: Traffic signal violation warning uses infrastructure-to-vehicle communication to warn the driver to stop at the legally prescribed location if the traffic signal indicates a stop and it is predicted that the driver will be in violation.

The in-vehicle system will use information communicated from infrastructure located at traffic signals to determine if a warning should be given to the driver. The communicated information would include traffic signal status and timing, traffic signal stopping location or distance information, and directionality. The type of road surface and weather conditions near the traffic signal may also be communicated as this could be used to estimate braking distance.

Stop sign violation warning: Stop sign violation warning uses infrastructure-to-vehicle communication to warn the driver if the distance to the legally prescribed stopping location and the speed of the vehicle indicate that a relatively high level of braking is required for a complete stop.The in-vehicle application will use information communicated from the infrastructure to provide the warning. The communicated information would include stopping location or distance information, and directionality. The type of road surface and weather conditions near the stopping location may also be communicated as this could be used to better estimate braking distance. As an alternative to DSRC, digital maps and GPS could be used.

4.1.2 Assist driver at intersection

Intersection collision warning: Warn vehicles at an intersection, when a collision would be probable, e.g. warn driver if he is going to accelerate from stop although another vehicle is approaching.Infrastructure sensors and/or DSRC communications can be used to detect all vehicles, their position, velocity, acceleration, and turning status while approaching an intersection. Weather status and the road shape/surface type can be variables for calculating the likelihood of a collision. The in-vehicle unit determines when a collision is imminent and issues a warning to the driver.

Pedestrian crossing information: This application provides an alert to vehicles if there is danger of a collision with a pedestrian that is on a designated crossing.

4.1.3 Assist driver on special road conditions

Work zone warning: Work zone warning delivers warning and additional information on a work zone to cars. Data could include speed limit, lane closures/changes etc.Information on work zone may also be relevant to vehicles further away from the scene.

Curve-speed warning(rollover warning): Curve speed warning aids the driver in approaching curves at appropriate speeds. This application will use information communicated from roadside beacons located ahead of approaching curves. The communicated information from roadside beacons would include curve location, curve speed limits, curvature, and bank and road surface condition. The in-vehicle system would determine, using other on- board vehicle information, such as speed and acceleration whether the driver needs to be alerted.

Infrastructure-based road condition warning: This infrastructure-based application will detect marginal road conditions using infrastructure systems and sensors (e.g. fog-detectors, temperature sensors, etc.), and transmit a road condition warning to approaching vehicles using geocast . Information is forwarded by other vehicles.Road condition information can be used by vehicle safety applications in the receiving vehicle. For example, an application can be designed to work in the vehicle to calculate maximum speed recommendations based on road conditions and upcoming road features (e.g. curve, bank, intersection, or stop sign) and notify the driver appropriately.

4.1.4 Assist driver in dangerous traffic situation

Wrong way driver warning: Cars heading in the wrong direction in one-way streets or on highways will receive a warning. Other vehicles driving in the correct direction will also be alerted of the upcoming vehicle. The wrong-way car will be detected by its position beacons or by infrastructure.

Rail collision warning: Railroad collision avoidance aids in preventing collisions between vehicles and trains on intersecting paths. Drivers of cars get informed about upcoming trains, which is of importance especially at crossings without gates.
This application will use information communicated from roadside beacons located near railroad crossings. The communicated information from roadside beacons would include data about approaching trains such as position, heading, and velocity.

4.1.5 Applications characteristics

Properties that describe characteristics aspects of the applications are used to distinguish different kinds of applications (38).

Influence on Safety: There exist different level of influence on road safety .We distinguish between safety related /safety critical and internet connectivity related applications .

Driver Involvement: When a vehicle receive a message from a RSU ,this may be treated automatically by the OBU or may demand the driver's awareness ,attention or even reaction . Such a message could have a direct repercussion on the safety of the vehicle and therefore they muss be trustable . The following numerical value shows the degree of involvement.

- 0 = no driver involvement
- 1 = driver awareness
- 2 = driver attention required
- 3 = driver reaction necessary

Forwarding: Message can be send without a response or with a response . In this case we speak respectively of one-way and two-way . Message delivered by RSUs are of public safety nature and in that way always one way. A concern about the authenticity of the message is a challenge.

Dissemination of message: To reach nodes or specific location in their area applications make use of single-hop,multi-hop or relevancy-based (nodes forward message to the other nodes) communications. For this purpose routing is utilized ,however since routing involves multiple nodes there is a higher risk of fraud.

Single-Hop: Here messages are directly sent to the destination, which is within the communication range of the sender. Normally for single-hop communication, a range of at least 150 m is assumed for normal road conditions (38).

Single-Hop: Multi-hop communication is used when the destination is beyond the wireless range of the sender. In this case messages from sender are forwarded to destination by intermediate nodes. A position-based routing scheme is used to realize multi-hop.

Relevancy-based: i. Message are transported passively,using a content and situation based relevancy calculation.With this transport mechanism,messages can be spread in an area even with very low network connectivity (38).

Addressing: This refer to who receive the message when it is send

Unicast: A unique node (RSU ,vehicle) receive a packet

Single-Hop: In this case message are send to all node within the wireless range of the sender.It uses either single-hop (Beaconing) or limited multi-hop (restricted flooding) based on TTL(time to live).

Geo cast: Here node who receive packet check their position to decide wether they are intended to process the packet. In the case of single-hop there is no relaying and only nodes in the defined location receive packet. In the case of multi-hop the receiving node flood the packet within the region if it is in the target region or forward the packet to the target region, if outside the region and then flood.

Latency: To react efficiently, applications need to receive informations within a certain delay: For safety-critical applications, latency ≤ 100 ms ; For safety-related latency $> 100ms$ and latency $\leq 1000ms$ (38).

4.2 Security requirements

The British Standards Institution (39) defines information security as the protection of information assets from a wide range of threats . This mean that according to the specificity of application maintaining authentication , integrity, privacy, confidentiality, availability . As a matter of fact there is no one size fit it all solution. In this sense every application has its own set of security requirements. Infrastructure installed along the road(RSU) transmit information of public nature and doesn't need either privacy or confidentiality .These properties are given later in Table

authentication: ensure that the sender of a message is correctly identified.

- Property authentication: allows to verify the properties of a sender(vehicle,RSU)

- Location authentication: allows to verify the acclaimed position of sender

Integrity: assures that the transported information are not altered between sender and receiver.

Availability :assures the availability of the communication system .

4.3 I2C safety application list

From the list of applications compiled by SEVECOM (38),the application characteristics and the security requirement we can derive our table.

Abreviations:

C=safety-critical application ; R= safety-related application
O=one way ; Y=Relevancy based ; G= geocast
B=Broadcast U=Unicast ; M=multi-Hop ; S=single-hop

IS=Influence on safety; DI =Driver involvement ;
FW = Forwarding ; DE=Dissemination of message;
AD=Addressing ,LT= latency ; PN=Property authentication; LN= Location authentication
IT= Integrity; AV= Availability

Applications	IS	DI	FW	DE	AD	LT	PN	LN	IT	AV
Assist driver with signage										
Traffic signal violation warning	C/R	3	O	S	G	1,0	2	2	2	1
Stop sign violation warning	C/R	3	O	S	G	1,0	2	2	2	1
Assist driver at intersection										
Intersection collision warning	C/R	3	O	S	G	0,5	1	2	2	1
Pedestrian crossing information	C	2	O	S	G	1,0	1	1	2	1
Assist driver on special road conditions										
Work zone warning	R	2	O	M	G	0,5	2	2	2	1
Curve-speed warning (rollover warning)	R	2	O	S	G	1,0	2	2	2	1
Infrastructure-based road (condition warning)	R	2	O	M/Y	G	5,0	2	2	2	1
Assist driver in dangerous (traffic situation)										
Wrong way driver warning	C/R	3	O	M/R	G	1,0	2	2	2	2
Rail collision warning	C/R	2	O	S/Y	B	1,0	2	2	2	2

Table 4.1: I2C safety critical/related applications

5 A CGA based message authentication scheme for I2C Applications

5.1 Network model and assumptions

5.1.1 Network model

In a general manner our network model is hierarchically composed of two layers :
The upper layer consist of the Road Side Units (RSUs), a Trust Authority (TA) and a Transport Control Center.The RSUs are connected to the Traffic Control Center . The Transport Layer Security protocol can assure for example the secure communication between RSU and the Traffic Control Center .
The lower layer consist of RSUs and OBUs . By means of short range wireless communication based on IEEE 802.11p* radio technology,the RSUs communicate with each other and with OBUs and can also provide to the latter access to the internet(Gateways).

5.1.2 Assumptions

According to our network model we assume:

1. A state is divided in zone under the control of the Traffic Control Center
2. There are 3 kinds of RSUs
   - Bootstrap RSUs:they are responsible for exchanging keys with vehicle(OBU)entering a zone.They continually broadcast their public key.
   - Slave RSUs:they warn vehicle about road condition or other informations related to the traffic optimization.
   - Public RSUs:they serve as a gateway to the internet .
3. A zone is composed of a Bootstrap RSU and a Slave RSU who are all securely connected to the Traffic Control Center.
4. OBU of mobile vehicles are able to obtain trough a TCC the public key of all the Bootstrap RSUs of a state.Updates of these keys can be made through Public RSUs .They preload these key before they engage in the road.

5. For prevention and detection of tampering,each vehicle and RSU are equipped with storage area named as Tamper Proof Devices (TPD).

5.2 CGA extension Field

According to (30) the CGA extension Field Format is an optional variable-length field of the CGA parameter Data Structure , which are not used in the current specification .We intend to use this field in our scheme .When broadcasting safety message, Slave RSUs use this field to store the subsequent symmetric key of the hash chain used by the OBU to check the authenticity of a message.

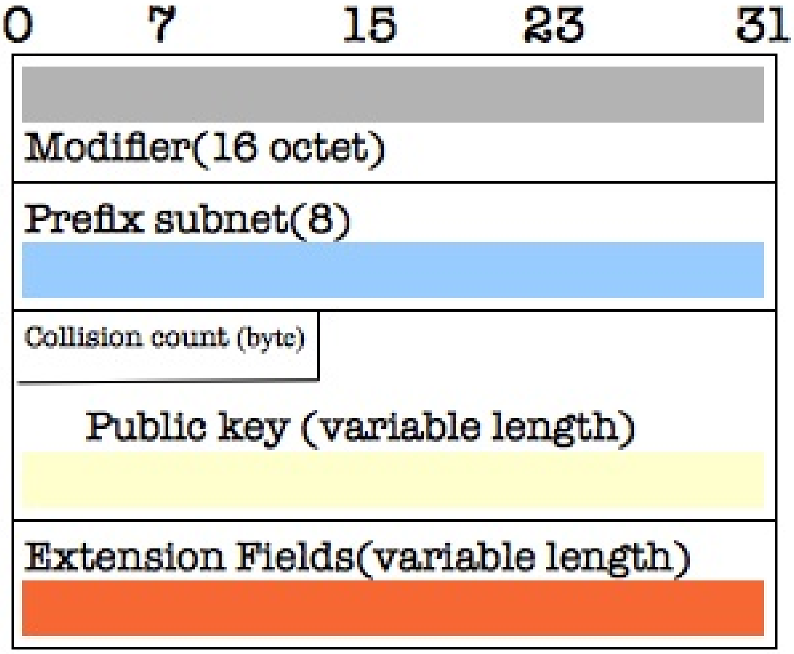


Figure 5.1: CGA’s parameter Data Structure

5.3 Security objectives

The proposed scheme aims to achieve the followings security objectives:

Message integrity and data origin authentication:

All safety message should be delivered unaltered in the delivery and the source of message should be authenticated to counterpart an impersonation attack.

Lightweight security: The security primitive should be efficiently selected in such a way that ensues small communication overhead and an acceptable processing latency .

Prevention against RSU Replication: It can happen that an adversary relocate a RSU or with a wireless device try to impersonate a RSU to launch attack such as message replay. Therefore there should be mechanism to countermeasure such a attack.

5.4 A CGA based message authentication scheme for I2V applications

In this section, we present a CGA based message authentication for I2V application called CAGE .This scheme take advantage of the benefices related to the use of the one-way hash chain and the Cryptographically Generated Address (CGA)namely the principles of commitment and the proof of ownership.

Briefly, a bootstrap RSU located at the entrance of a zone advertises his public key. The OBU of a mobile vehicle approaching the zone recognizes his public key and initiates a challenge response protocol.At the end of this protocol, the OBU of the mobile vehicle receives a combination of one item of a chain sequence,an integer value and the hash value of a slave RSU's public key.This combination are then later used by the vehicle to validate broadcasted safety message coming from the corresponding Slave RSU when driving inside zone.

The proposed scheme can be divided in 4 principal steps:
system setup , recognition and key assignment , verification ,timeout and system update.
The detailed implementation of the scheme are presented in the following subsections. For ease of presentation the notations throughout this paper are listed in Table 5.1.

5.4.1 System Setup-Phase A

At startup ,the TCC apply n iterations of H on different seed in oder to create different chain sequence of key values regrouped respectively in subsets[1].Meanwhile, it generates as well a bunch of public/private keys ,which will be later used by different slave RSUs. Each zone is mapped to a different seed,which is used as a starting point for all subsequently operations in the zone. The bunch of public/private key pairs are interchangeability and randomly

[1] We call in our scheme each of these subset D

Notation	description
$\{\ldots\}$	A subset
$\|\|$	A message concatenation
N	Nonce
D	Set of sequence of one way chain value
B	Bootstrap RSU
S	Slave RSU
x_n	A Seed
V_i	The OBU of the vehicle
$< V_s/S_s >$	public/private key of a Slave RSU

Table 5.1: Table of Notation

assign to zone.Each public/private keys pairs are only valid in the zone for a delimited time. Afterward,TCC sends these different subsets and public/private key pairs to the different zone of the states.

Precisely, taking the case of a specific zone, the TCC securely issue a concatenation of a subset D, its length n and a hash value of a randomly picked public key[2] to the bootstrap RSU (1); Simultaneously it also issue a concatenation of the last element W of the subset D and the public/private key pair to the slave RSU(2). The RSUs acknowledge the reception with their identification number (3). Let consider for instance a zone A,where X_n is the randomly chosen seed and W the result of n iteration of H on X_n.The obtained chain sequence is regrouped in the subset D,$D = \{X_n, X_{n-1}, X_{n-2}, \ldots W\}$. If $< V_s/S_s >$ is the randomly picked public/private key ,then we can interpret this process as described in algorithms 6 as follows:

Algorithm 6 System setup

```
1: $TCC \rightarrow B : D||n||H(V_s)$ (1)
2: $TCC \rightarrow S : W|| < V_s|S_s >$(2)
3: $S \rightarrow TCC : MYID$(3)
4: $B \rightarrow TCC : MYID$(3)
```

[2] Only the public key not the the public/private key pair is send to the bootstrap RSU

5.4.2 recognition and key assignment-Phase B

At the entrance of a zone , a bootstrap RSU advertises his public key . An OBU of a mobile vehicle approaching within its transmission range receives the public key . The OBU then check if the public key is valid by looking up the preloaded keys inside its Tamper Proof Devices storage . When the operation is successful the OBU initiates a challenge response protocol to authenticate the bootstrap RSU .For this,V_i ,generates a pseudo random number N (Nonce) and sent it encrypted with the verified public key V_B.

At receipt of the message , the bootstrap RSU decrypt the packet and stores the nonce N in its Queue[3]. Next, it fetch the first key chain value of the subset D in the order of the chain generation. Thereafter sends it in the clear together with the previously received nonce N, a timestamp t_B and an integer value I ;I represents the number of iteration H necessary to obtain the key able to verify the MAC of a safety message broadcasted later by the slave RSU in the zone. After passing the bootstrap RSU, the vehicle enter the zone. Algorithm 7 shows this process as follows:

Algorithm 7 Recognition and key assignment

```
B $\rightarrow^*$ $V_i$ : $V_B$% public key advertising
**for**($i = 0; i < TTD.length; i++$)
    **if**(TTD[i] =? V$_B$)
        $then$
        V$_B$ is valid
        $V_i \rightarrow B$ :{N}$_{V_B}$
    **end if**
end for
B $\rightarrow$V$_i$ : $X_i||I||N||t_B$.
(N is valid)? $V_i$ stores $X_i||I||N||t_B$:**reject**
```

5.4.3 Timeout and System Update-Phase C

when the Bootstrap RSU finish assigning the first element of its subset D in the **phase B**, it sends a message to the TCC saying it want a new subset and continue processing other requests. At receipt of this request, the TCC generates another chain sequence D' starting where it left the last time(this mean starting with the seed W) and pick randomly another public key which it computes the hash value. Finally it sends to the corresponding bootstrap RSU the packet $D'||n||H(V'_B)$and to the slave RSU the new pair public /private key and the

[3] A sort of FIFO (first In ,First Out)

last element of the chain sequence D' namely the packet $< V'_S|S'_S > ||W'$.

The RSUs receives and stores the packet . When it is about to assign its last element,it informs the TCC ,which directly instruct the Slave RSU to start broadcasting safety message with the newly received packet .

Since traffic density are not uniform in all zone, an assigned subset can stay for a long time in the Bootstrap RSU without any request from a vehicle . This could give time for a malicious entity to mount an attack to an upcoming vehicle knowing $X_i||I||V_S$.Therefore we introduce a Timeout.

The timeout in our context is the time during which a request must take place after an item has been assigned if there is no another request pending in the queue. Beyond this time the current subset is no longer valid and the bootstrapRSU must instruct the TCC about it. This instruction is similar to the one it issue when it is about to assign the last item of its subset(i.e my current data are now invalid ,send me another concatenation).

We assume that the T timeout [4] is a function of the number of items g assigned to a subset . Depending on the traffic density and the implemented application, g and T will vary. If we consider for instance that the queue in the bootstrap RSU is full and $T_i$is the time necessary for a bootstrap RSU to assign an item to a vehicle ,then the time for processing all the request in the queue would be what we consider our timeout namely with $T = gT_i$ representing itself the decryption time T_d of the request added to the time Q_i necessary to pop an item from the subset and to assemble the corresponding packet.

5.4.4 Verification-Phase D

After passing the entrance zone, the vehicle V_i ventures inside the zone,where a slave RSU broadcast safety information in case of hazard events. Concretely, the slave RSU first computes the MAC C of the safety message M with its key commitment W :$C = HMAC(W, M)$. This MAC is stored in the extension field of the CGA parameter [5].Thereafter before broadcasting the packet P, it generates a CGA address,sign the safety message M with his private key and append to it the timestamp T_S . In fact, the packet is composed of the CGA address,the CGA parameter,the signature, the payload and the timestamp as shows in figure 5.2.

[4] We consider Ti, Td, Qi as constant

[5] when the Slave RSU send the safety message,the MAC is stored in the extension field of the CGA parameters.

V_i receives the broadcast message when within the range of the slave RSU. After receiving the message ,$V_i$uses the previously stored pair value obtained during the phase B to match the key W of the slave RSU and subsequently verify the MAC stored in the CGA extension field i.e verify the message authenticity (Integrity and source authentication) of the safety message. Additionally V_i make a hash of the CGA parameter data structure's public key and compare it with the hash it received during thephase B .When these two operations are successful then the vehicle V_i is sure it shares a *common knowledge* with the RSUs and therefore can go on to prove the ownership of the claimed CGA address i.e verify the CGA address . Before validating completely the safety message it check if the difference of the timestamp is less than a *threshold)* τ*. Algorithm 8 illustrates this process:*

Algorithm 8 Verification-Phase D

```
$V_i's$ IMPUT
**imput 1:** let consider that a vehicle $V_i$ received at Phase B $X_j||I||H(V_S)||t_B$
**imput 2:** $V_i$ receives Packet P from slave RSU in Phase D;
    1:$W' = H^I(X_j))$;
    2: compare C and C',C'=HMAC(W',M);
    3: make a hash of the CGA parameter' public key and compare it with the hash obtained during phase B
    **if**(2. and 3. are true)
        **then if**(CGA address is true)
            **then if**
                the safety message M is taking into account
            **end if**$((T_S - T_B) < \tau)$
        **else reject;**
        **end if**
    **else reject**
    **end if**
```

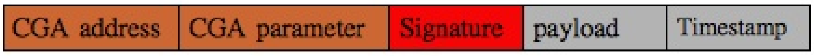


Figure 5.2: Composition of slave RSUs packets

5.5 Analyze of the scheme

5.5.1 Lightness and efficiency of the scheme

A secure message 5.3format within the DSR/WAVE (15) are defined in the current IEEE Trial-Use standard concerning the security in VANET and the choice of the crypto system.It is specified that to assure the integrity of a safety message, OBU and RSUs should sign message with their private key before these message are send . In this secure message format we notes that a 125 byte certificate and a 56 bytes ECDSA signature are attached to the 53 bytes payload of each safety messages .

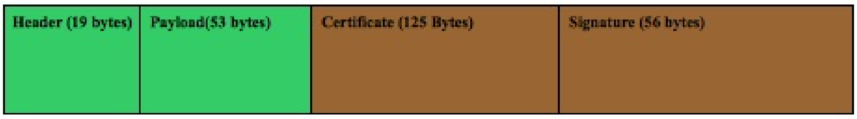


Figure 5.3: A simplified version of secure message format in VANET

However, the heavy overhead (certificate and signature) and the computational burden associated with the use of a Public Keys Infrastructure are not scalable with the traffic density . In VANET, a vehicle must frequently verify status message called beacons,which are send within the time interval of 100-300 ms from other vehicles (3) . A vehicle at receipt of the beacons must not only check the signature but also the certificate. Since verification of public key are not very fast this result into a burning computation for the vehicle . If we consider for instance 50-200 vehicles within the transmission coverage of a vehicle ,this would mean according to the beacon generation that the vehicle would have to verify around 200-2000 beacons per second . Added to this,the verification of safety message coming from Road Side Unit and the vehicle is not any more able to respond correctly to the stringent time requirement of safety applications .

Therefore, we suggest in our protocol to reduce this computational burden as well as the authentication tag size (signature and verification) by using small public/private key size in the Phase A,D.We take also advantage of the speed of the MAC ,which is several order of magnitude faster than generating or verifying a digital signature.Indeed,with respect of the NIST key size recommendation we use a typical MAC algorithm namely a HMAC-SHA1 algorithm.

The choice of the crypto system and the key size are decisive in the evaluation of a protocol or a secure system.To verify and sign message , the IEEE 1609.2 standard for secure VANET communication proposes the use of the Elliptic Curve Digital Signature Algorithm

(ECDSA). In fact, a comparable level of security afforded by an RSA based crypto system with large bit can be achieved with small bits using ECDSA(see Figure 5.5). Based on this comparable security and storage advantage vehicle are preloaded in our scheme with 163-bit ECDSA public keys before they engage in the VANETs .These public keys belong to the bootstrap RSUs of different zone and serve as recognition at zone entrance.

It is assumed that the decryption time is faster than the encryption time with ECDSA keys. Therefore we don't think that the scalability of our scheme is a problem.We argue that after a request(nonce n in the Queue) is processed,it is deleted making thus a place free for another vehicle's request. Moreover we point out that the shortness of the communication at phase B and the transmission range make it easy for the bootstrap RSU to process a load of request. In fact, if we consider the transmission range of a RSU ,which is up to 1000 m, a vehicle driving at 20 m/s for instance would still be inside the range after 10 s.

Hence, even if the Queue is full and giving the fact that a request is handle in millisecond ,all vehicle's request can be processed at time before leaving the bootstrap RSU transmission range.

Another point is,the public keys and the one-way chain sequence are generated by the TCC and not by the RSUs,which limit the computation burden at one place.

As shows in figure 5.3, a secure overhead of 181 bytes (certificate +signature) is mandated for safety message. For security Our scheme use :

- *The CGA header (16 bytes) .*
- *The CGA's parameter data structure (65 bytes),which contain 20 byte output of the HMAC stored in the extension field .*
- *A signature (21 byte).*
- *A timestamp of 1 byte to counterpart replay attack.*

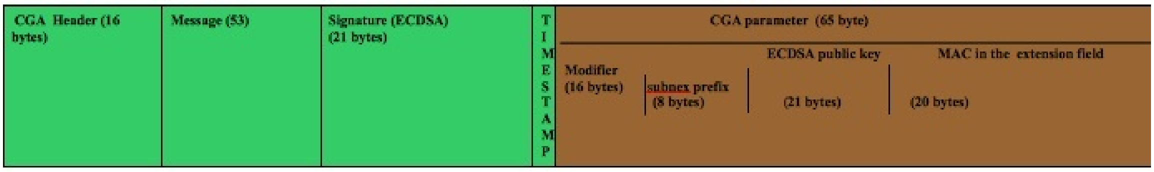


Figure 5.4: Message format in our scheme.

Figure 5.3 compared to Figure 5.4 shows more than a 55 % reduction of the overall security overhead and hence in the computation necessary to determine the authenticity of safety message broadcasted by Slave RSUs in our scheme.

5.5.2 Security analysis

The security of our scheme lies under :

The self certification of CGA address:

C.G.A aims at preventing stealing and spoofing of existing Internet address.The cryptographically bounding between the public key and the address enable the address owner to prove ownership through signing with its private key.

An attacker through able to create a new CGA from any subnet prefix and its own (or anyone else's) public key cannot take a CGA created by a node and send signed messages that appear to come from the owner of that address,thus preventing impersonation.

Indeed,to be able to attack our scheme(impersonation),the attacker must find a second pre-image (i.e generate another public/private key that can actually impersonate the node) of the 59 bit interface identifier which is a brute force attack of $O(2^{59+16*sec})$ *hash* [6] *computations. In fact ,for security purpose for the future,the extension hash2 has been introduced,in large party to prevent that as the computer become faster the CGA technology become obsolete.To achieve the effective extension of the hash length, the input to the second hash function, Hash2,is modified (by changing the modifier value) until the leftmost* $16 * Sec$ *bits of the hash value are zero. This increase the cost of CGA generation by a factor of* $O(2^{16*sec})$*,but also the total cost of the brute force attack from* $O(2^{59})$ *to* $O(2^{59+16*sec})$ *(30).*

$Sec > 1$ *is for high security, however,for efficiency in the CGA generation and giving the short duration time and the dynamic changing of CGA address in our scheme, we set the sec to zero.Therefore, the attacker has to find a second pre-image for the 59 bit digest,which require a brute force attack of* $O(2^{59})$ *hash computations.*

Figure5.6 provide the CPU time and investment required by a brute-force search to find a second-preimage for a 64-bit hash function (41).Looking at this table,even for a 59 bit,the short time validity of an CGA address within a zone will not suffice for an attacker to find an appropriate public/private key pair given the fact that CGA address change frequently in our scheme and there is a Timeout T in case of slow or no traffic at all.

The shared common knowledge between RSUs and the vehicle:

The problem with CGA address is that they are not certified.In principle ,anyone is able to create a new CGA from any subnet prefix and its own (or anyone else's) public key

[6] since in the comparison for the validity of the CGA address between the hash1 and the interface identifier,the security bit sec(3 bit) and the universal IPv6 bits ?u? and ?g? are left out then we have 59 bit.

.To overcome this weakness,the Traffic Control Center send a MAC value of the slave RSU?s public key to the Bootstrap RSU(Phase A),who after having being authenticated by a vehicle entering the zone (Phase B) pass it to the correspondent vehicle. Therefore at this stage, the vehicle share a common knowledge with the slave RSU.This knowledge will then be useful to check the legitimacy of the sender(the slave RSU) and subsequently of the .

In fact,since the MAC is transmitted through Internet secure communication,it is quite impossible for an attacker to know in advance which public key will be send to the Bootstrap RSU or even to launch a Man in the Middle Attack for instance to send instead the MAC of its public key.

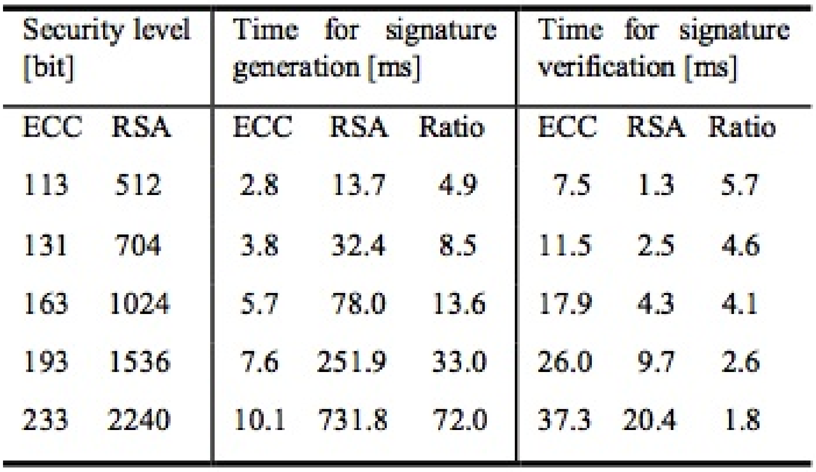
The only way for an attacker to be successfully is to take control of the traffic center.This is however quite impossible given the security at such center.

An Integer value:

Each Vehicle that pass through a bootstrap RSU get after authentication an individual integer value I,which is different from what other vehicle get.This integer value denotes the number of iterations necessary to find the key W used by the slave RSU to verified the safety message.This features re enforce the trust from vehicle toward the slave RSU,since the key W required to verified the MAC in the phase D is a commitment of a one way chain sequence ,which they vehicle get through hash iterations.

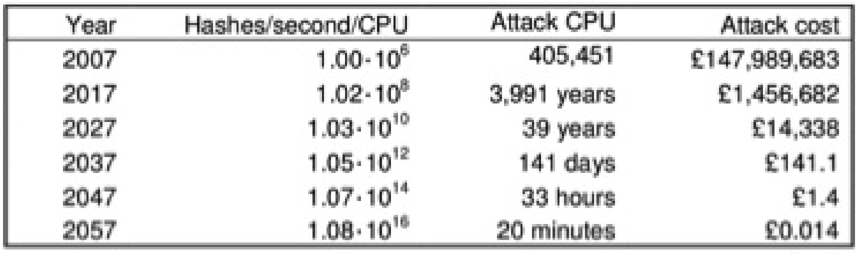
Timestamp:

To prevent replay attack,message are invalid beyond a threshold value.



Security level [bit]		Time for signature generation [ms]			Time for signature verification [ms]		
ECC	RSA	ECC	RSA	Ratio	ECC	RSA	Ratio
113	512	2.8	13.7	4.9	7.5	1.3	5.7
131	704	3.8	32.4	8.5	11.5	2.5	4.6
163	1024	5.7	78.0	13.6	17.9	4.3	4.1
193	1536	7.6	251.9	33.0	26.0	9.7	2.6
233	2240	10.1	731.8	72.0	37.3	20.4	1.8

Figure 5.5: EXECUTION TIME FOR SIGNATURE OPERATIONS WITH DIFFERENT SIGNATURE SCHEMES ON A SHARP ZAURUS SL-5500G (40).



Year	Hashes/second/CPU	Attack CPU	Attack cost
2007	$1.00 \cdot 10^{6}$	405,451	£147,989,683
2017	$1.02 \cdot 10^{8}$	3,991 years	£1,456,682
2027	$1.03 \cdot 10^{10}$	39 years	£14,338
2037	$1.05 \cdot 10^{12}$	141 days	£141.1
2047	$1.07 \cdot 10^{14}$	33 hours	£1.4
2057	$1.08 \cdot 10^{16}$	20 minutes	£0.014

Figure 5.6: Median Cost of a Second Preimage Attack Against 64-bit Hash (41).

6 Conclusion and future work

Beaconing are the cornerstone of VANETs.The security of these broadcasted heartbeat message are vital for the acceptance of the car to x technology, since safety applications rely on information provided like velocity, direction and position to warn driver or to detect potential dangerous situations.

The DSRC/WAVE standard identify the use of PKI to support message authentication and recommend the utilization of Elliptic Curve Cryptography (ECC) as public key cryptography standard.However, these security mechanisms come with heavy overhead that affect the overall performance of VANETs and thus of safety applications.

On the other end symmetric security primitive like one-way chain are less computational demanding,nevertheless introduces complexity in key maintenance and exerts difficulty in authentication for multicast or broadcast communications (42).

The recent research works have opted of using lightweight cryptographic constructions for broadcast authentication,therefore hybrid scheme have been proposed.However, although presenting respectable results ,they have in one form or another rely on a public key infrastructure.Trust bootstrapping is an example.

In our scheme, we have gone another direction by stating that the better approach to provide a lightweight solution without relying on any infrastructure is to consider find first lightweight solution for small set of applications based on their characteristics and go from there for a more general approach .We believe,by considering small sets of applications based on their characteristics the overall authentication overhead of VANETs can be reduced.

Therefore,we have proposed a lightweight authentication scheme for I2V applications.The scheme rely on self certificating address called Cryptographically Generated Address and one-way chain to provide broadcast authentication.The scheme use common knowledge between RSUs (Bootstrap RSUs and Slave RSUs) and vehicles to establish trust instead of relaying on a Certificate Authority.

The analysis of the scheme shows a significant reduction in the overall security overhead compared to the IEEE P1609.2 (43) standard. Additionally, the scheme prevent Attacks like *impersonation, Man in The Middle and replay of messages.*

Due to lack of an appropriate VANETs's simulator in our department, we couldn't go further in simulating a real traffic situation and compare results in term of performance between our scheme and a PKI supported scheme like defined in the IEEE P1609.2 (43)in presence of Road Side Units.Therefore this could be subject of further work.

Bibliography

[1] *M. Raya and J. Hubaux, "Securing vehicular ad hoc networks,"* Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.*

[2] *G. Doe, "Vanets security requirements final version . technical report, secure vehicle communication (sevecom)."* `http://www.sevecom.org/Pages/ProjectDocuments.html`*, Sept. 2006.*

[3] *Learnstrong.* `http://www.leearmstrong.com`*, 2011.*

[4] *I. E. T. I. WORKSHOP, ed.,* Global Co-operation*, (Sophia, Antipolis), Feb 2009.*

[5] *X. Ma, X. Chen, and H. Refai, "Performance and reliability of dsrc vehicular safety communication: a formal analysis,"* EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 3, 2009.*

[6] *I. P802.11p/D3.0, "Draft amendment for wireless access in vehicular environment (wave)," tech. rep., Juli 2007.*

[7] *Y. Qian and N. Moayeri, "Design of secure and application-oriented vanets," in* Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pp. 2794–2799, IEEE, 2008.*

[8] *I. D. P1609.0/D01, "Ieee trial-use standards for wireless environments access in vehicular (wave)," tech. rep., February 2007.*

[9] *E. T. I. Workshop, ed.,* A.Global Standardization of Network and Transport Protocols for ITS with 5 GHz Radio Technologies*, (Sophia Antipolis, France), February 2009.*

[10] *C2CCC.* `http://www.car-to-car.org/`*, 2011.*

[11] *E. T. S. Institute, "Radio spectrum matters (erm); intelligent transport systems (its); part 1: Technical characteristics for pan-european harmonized communications equipment operating in the 5 ghz frequency range and intended for critical road-safety applications," system reference document, 2005.*

[12] *E. T. S. Institute, "Electromagnetic compatibility and radio spectrum matters (erm); intelligent transport systems (its); part 2: Technical characteristics for pan-european harmonized communications equipment operating in the 5 ghz frequency range intended for*

road safety and traffic management, and for non-safety related its applications;," draft system reference document, ETSI TR 102 492 - 2 V1.1.1, 2006.

[13] M. Raya and J. pierre Hubaux, "The security of vanets," in Mobile Computing and Networking*, pp. 93–94, 2005.*

[14] B. Parno and A. Perrig, "Challenges in securing vehicular networks," 2005.

[15] IEEE Standard 1609.2, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments- Security Services for Applications and Management Messages*. July 2006.*

[16] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," Security and Communication Networks*, 2010.*

[17] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, SASN '05, (New York, NY, USA), pp. 11–21, ACM, 2005.*

[18] X. Lin, X. Sun, and P.-H. Ho, "Gsis: A secure and privacy preserving protocol for vehicular communications," in Vehicular Technology Conference*.*

[19] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, VANET '07, (New York, NY, USA), pp. 19–28, ACM, 2007.*

[20] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, Q2SWinet '05, (New York, NY, USA), pp. 79–87, ACM, 2005.*

[21] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in Proceedings of the third ACM conference on Wireless network security*, WiSec '10, (New York, NY, USA), pp. 111–116, ACM, 2010.*

[22] G. Samara, S. Ramadas, and W. A. H. Al-Salihy, "Design of simple and efficient revocation list distribution in urban areas for vanet's," CoRR*, vol. abs/1006.5113, 2010.*

[23] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "An efficient message authentication scheme for vehicular communications," IEEE Transactions on Vehicular Technology*, vol. 57, pp. 3357–3368, 2008.*

[24] *W. Hsin-Te, W.-S. Li, S. Tung-Shih, and W.-S. Hsiehz, "A novel rsu-based message authentication scheme for vanet,"* Systems and Networks Communication, International Conference on*, vol. 0, pp. 111–116, 2010.*

[25] *X. Lin,* Secure and privacy-preserving vehicular communications*. PhD thesis, University of Waterloo, 2008.*

[26] *"Mac." http://en.wikipedia.org/wiki/Message*$_a uthentication_c ode$.

[27] *Lamport, "Password authentication with insecure communication,"* Communications of the ACM*, pp. 770–772, November 1981.*

[28] *A. Perrig, R. Canetti, J. Tygar, and D. Song, "The tesla broadcast authentication protocol,"* RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.*

[29] *A. Weimerskirch and D. Westhoff, "Zero common-knowledge authentication for pervasive network," in* Selected Areas in Cryptography*, pp. 73–87, Springer, 2004.*

[30] *T. Aura, "Cryptographically generated addresses (cga)." http://www.ietf.org/rfc/rfc3972.txt, March 2005.*

[31] *R. Housley, "Internet x. 509 public key infrastructure certificate and certification revocation list (crl) profile,"* RFC 3280*, 2002.*

[32] *T. Aura,* Cryptographically Generated Addresses(CGA)*. No. 6th, Bristol, UK: 6th Information Security Conference(ISC'03), October 2003.*

[33] *W. Diffie and M. Hellman, "New directions in cryptography,"* IEEE Transactions on Information Theory 22*, pp. 644–654, 1976.*

[34] *IEEE Transactions on Information Theory,* On the Security of Public Key Protocols*, 1983.*

[35] *"http://en.wikipedia.org/wiki/Dolev-Yao-model".*

[36] *"Now - network on wheels project.." http://www.network-on-wheels.de, 2005.*

[37] *W. Enkelmann, "Fleetnet-applications for inter-vehicle communication," in* Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*, pp. 162–167, IEEE, 2003.*

[38] *S. Project, "Security architecture and mechanisms for v2v/v2i (deliverable 2.1). technical report," tech. rep., SEVECOM, 2007.*

[39] *British Standards Institution,* Information Security Management - Part 1: Code of Practice for Information Security*, (London), 1999.*

[40] *D. Westhoff, B. Lamparter, C. Paar, and A. Weimerskirch, "On digital signatures in ad hoc networks,"* European transactions on telecommunications*, vol. 16, no. 5, pp. 411–425, 2005.*

[41] *J. W. Bos, O. Özen, and J.-P. Hubaux, "Analysis and optimization of cryptographically generated addresses," in* Proceedings of the 12th International Conference on Information Security*, (Berlin, Heidelberg), Springer-Verlag, 2009.*

[42] *B. Lu and U. Pooch, "A lightweight authentication protocol for mobile ad hoc networks," 2005.*

[43] *"Its standardsprogram,." http://www.standards.its.dot.gov/StdsSummary.asp.*

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit im Sinne der Prüfungsordnung nach §24(5) ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, June 15, 2011	
Ort, Datum	*Unterschrift*