Security in Cooperative Systems within Intelligent Transport Systems

Master of Science Thesis (Secure and Dependable Computer Systems)

LARS MÅRDBERG

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, August 2011

Security in Cooperative Systems within Intelligent Transport Systems

Lars Mårdberg
Examiner: Erland Jonsson

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0) 31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden November 2011

Security in Cooperative Systems within Intelligent Transport Systems

By:
Mohammad Amin Asadi
Lars Mårdberg

Abstract

Vehicular Communication intends to improve the safety for humans as well as the traffic efficiency on the roads. Vehicular communication requires the vehicles to communicate wirelessly, which make them vulnerable to attacks such as intentional modification and injection of bogus messages in the transmitted data stream. It also opens possibilities for adversaries to violate privacy, e.g. by performing location tracking. System characteristics including the need for real-time communication, fast changing network topology and limited resources make it extremely challenging for researchers to develop a robust and secure solution. Current proposed security solutions for the Vehicular Ad-hoc Network (VANET) are not capable of handling all the security requirements and system constraints. Thus, in this thesis we explore further possibilities to fulfill security requirements and overcome system constraints of vehicular ad-hoc networks.

Keywords

Security, Cryptography, Vehicular Ad-hoc Network, Cooperative Intelligent Transport System

Preface

This master thesis report is the result of a collaboration between two students: Lars Mårdberg from Chalmers University of Technology and Mohammad Amin Asadi from Royal Institute of Technology (KTH). Thus, there exist two versions of the report, with front pages from Chalmers and KTH respectively. The practical thesis work was carried out at Volvo Technology Co in Göteborg.

Acknowledgment

We owe many thanks to people who helped us during this research accomplishment.

Above all, we would like to thank our parents, brothers, sisters and girlfriends. This would not have been possible without their love, concern and patience.

This thesis has been carried out as a collaboration between KTH University and Chalmers University. We therefore thank our supervisors, Mrs. Iskra Popova at Royal Institute of Technology and Mr. Erland Jonsson at Chalmers University, who shed lights by advising and guiding us on critical parts of the research way.

We express our sincere appreciation to our supervisor at Volvo Technology Co., Mr. Edvin Valtersson who helped us to shape the research. We learned a lot during various discussions we had with him.

Our heartfelt gratitude to Volvo Technology Intelligent Transport System Manager, Mr. Hossein Zakizadeh, who inspired, encouraged and supported us in all parts of our thesis work life at VTEC.

We thank Mr. David Rylander and Mr. Niclas Nygren who kept us updated by providing latest publications and standardization drafts which were so valuable and helpful.

Our appreciation to Volvo Technology Co. who supported the research financially and to colleagues and friends who made a fun and friendly workplace for us.

Lastly I want to thank my dear thesis college and friend Mr. Mohammad Amin Asadi for doing a great job; sharing interesting thoughts and discussion.

Table of Contents

Acronyms

BP	Bilinear Pairing
C2C-CC	Car-to-Car Communication Consortium
CEN	European Committee for Standardization
CRL	Certificate Revocation List
CRL DZ	Certificate Revocation List using divided zones
CVIS	Cooperative Vehicle-Infrastructure Systems
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunication Standards Institute
GNSS	Global Navigation Satellite Systems
GPRS	General Packet Radio Service
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITS	Intelligent Transport System
LDM	Local Dynamic Map
LTE	Long Term Evolution
MAC	Medium Access Control
MAC	Message Authentication Code
Mbps	Mega bit per second
MITM	Man in The Middle
NTRU	Number Theorist Research. Unit
OBU	On-Board Unit
PBC	Pairing Based Cryptography
PKI	Public Key Infrastructure
RSA	Rivest, Shamir and Adleman
RSU	Road Side Unit
SeVeCom	Secure Vehicular Communication
TA	Trusted Authority
UMTS	Universal Mobile Telecommunication System
VANET	Vehicular Ad hoc Network

List of Figures

List of Tables

1 Introduction

1.1 Background

Road crashes caused more than 38000 deaths and 1.2 million injuries in 2008 in Europe. Almost 79 percent of fatalities were among vehicle passengers and the rest were among pedestrians [1]. Annual cost of accidents with deaths or severe injuries in Europe are estimated to 50 to 40.5 billion Euros respectively [2].

Cooperative Intelligent Transport System (ITS) is a technology that enables vehicles to communicate with each other and with the infrastructure to increase drivers' awareness. Vehicles frequently exchange messages in between and collaborate with road side units (stationary devices beside the roads) to provide critical and non-critical information to each other. The messages may contain vehicle's coordination, speed and acceleration data and may also possess information about special events. Cooperative ITS opens new possibilities in the areas such as traffic safety, traffic efficiency and environmental solutions (e.g. decreasing fuel consumption and CO_2 emissions).Most of the ITS features are now being standardized. The European Telecommunications Standards Institute (ETSI) in collaboration with other standardization organizations such as ISO and IEEE, is currently developing the European standard in this area (refer to 3.7).

1.2 Motivation and Purpose

Security is tied to ITS since it is critical for a system where human life is involved and safety is considered as the ultimate goal. Therefore, any unauthorized modification in life critical information must be prevented. Vehicular communication, like other wireless communication systems, is open to everyone and therefore exposed to different attacks. In addition, ITS characteristics bring new challenges such as high mobility and low bandwidth to security specialists and researchers that are different from the ones in regular networks. These characteristics open new vulnerabilities for intruders to compromise the system and exploit the resources. Numerous on-going studies are being released in this area. At the time when this document is being written, the standardization of ITS security solutions is still under development. Different reports have shown that their proposed solutions are still inefficient and do not solve all the issues ITS may encounter. Therefore this thesis is dedicated to an enhanced research on the Vehicular Ad-Hoc Networks (VANETs) from a security point of view.

1.3 Aim

The aim of this project is to investigate the different security solutions that could be utilized to secure cooperative systems within the ITS. The solutions will be evaluated to examine how well they fulfill the requirements and constraints defined in Cooperative ITS. We will also perform implementation and testing of the well evaluated solution(s). Overall, we should answer the following questions:

- What are the obstacles towards securing Vehicular Ad-hoc Networks? Which are the possibilities, bottlenecks, vulnerabilities and threats?
- What are the solutions proposed by standardization, industrial projects and academic papers within the area? How do they fulfill the security requirement and system constraints?
- Which security approaches are the most feasible or promising ones?

1.4 Limitation and Scope

The project only covers security in communication links between ITS stations and it does not consider in-vehicle security. In other words, it is assumed that the equipment and sensors (e.g. GPS Receiver) are not malfunctioning. Therefore, data generated by the sensors are assumed to be correct. The content of the messages exchanged between nodes will only be considered if needed for security purposes. Otherwise they will not be considered and the concerns would be limited only to trustfulness and correctness of the exchanged message. This thesis leaves "How to determine the compromised ITS Station?" question open since it would need further investigation in determination mechanisms. This thesis is also involved in experiment to evaluate the security solutions. The implementations are limited to the functionality needed for evaluation the predefined measures (e.g End to end delay). Therefore full security solutions are not implemented.

1.5 Intended Audience

Automotive industries active in ITS research and development, related standards working groups, ITS security researchers and people interested in both ITS and security context are considered as our intended audiences who can benefit from the content of the research.

1.6 Contribution

The thesis was funded by Volvo Technology Corporation and has been done in its premises in Göteborg, Sweden.

The workload of this thesis including, literature review, analysis, experimentation, testing and report writing has been shared equally by both of authors during the thesis accomplishment of the thesis.

1.7 Thesis Structure

This thesis is structured as follows: In chapter 2 methods, which are utilized to conduct the research, are discussed and justified. Chapter 3 presents the concept of Cooperative Intelligent Transport Systems, Vehicular Ad-hoc Networks (VANET) and also Standards and Research Groups that are active in security research within VANETs. Chapter 4 is dedicated to analyze the security approaches to VANETs based on security requirements, which are discussed and derived based on threats and attacks that the VANET is facing. Further, in chapter 5, security approaches to VANETs are analyzed considering system requirement and constraints. Chapter 6 describes the details of the Experimentations and Testing phases made. Finally, in chapter 7 the conclusion gives the answer to the research questions.

2 Methods

This chapter presents the research methods that have been used to carry out the study within material collection, analysis, experimentation and evaluation. Referring to the thesis description given by Volvo Technology Co., this research can be roughly categorized into three main sections. Within the first section, the authors try to investigate the problem area in depth and describe different concerns within the security of cooperative intelligent transport systems (including the system threats and constraints). Further, the second section focuses on analysis of different approaches to tackle the problems faced in the area. The discussion is based on the authors' knowledge and the materials reviewed and synthesized for this sake. Finally, the third section purely provides an evaluation on implemented algorithms on given prototypes and discussions which are fundamentally given according to previous sections.

2.1 Literature Review

Literature review is a depth evaluation of the related works which have been done up to the time of the research. This allows the authors to understand the problem and keep track of the latest released knowledge and ideas on the area to identify and formulate the research question(s) and the thesis path. Giving an organized summary of reviewed works would also help the readers to find out where and why the current research is started and pursued within a specific area.

The materials needed for this sake are mostly among the scientific papers, standards documentations and industrial projects publications. Digital libraries such as IEEE (accessed through KTH University digital library), standards drafts (mostly given by Volvo Technology as confidential documents) and industrial project websites are the main sources for the materials.

We tried to discuss different aspects of the vehicular ad hoc networks security by combining our knowledge with the materials reviewed and scored from mentioned sources.

The literature review in our thesis is basically composed of an overview of the system security requirements and its most challenging parts according to the threats that it is facing and system constraints and limitations that are mostly caused by its nature (such as real time communication or bandwidth limitations).

2.2 Action Research

Action research is a research method used to validate practical researches where the goal is to approach the problem area not just by studying it (in case of descriptive research) but also by expanding the knowledge leading to create changes and solve current practical problems. Action research contributes to the theory by adjusting it based on the practical outcomes of the study [68].

We firstly approached the area by investigating and describing the problem from different views. The action is made by giving an evaluation of experimented security mechanisms against security requirements and system constraints. The evaluations shed light on aspects we are looking for throughout the report such as broadcast authentication efficiency in terms of computational power, packet loss rate and end-to-end delay. The results and discussion would be our contribution to the problem area.

2.3 Empirical Research

Empirical research is based on investigation and observation of experiments to gain knowledge.

Empirical research composed of quantitative and qualitative researches. Quantitative research is utilized to prove a hypothesis by applying statistics on a large set of data that have been collected. A benefit of using quantitative research is that the results are always objective and formal and the results can be reconstructed by accomplishing the same tests. In contrary, Qualitative research tries to see full picture of the problem area and to discuss the found patterns. Qualitative research might be done in the beginning of a research, where there is not much information about the subject to find interesting research questions. These questions may later be used within quantitative research.

Through Chapter 4 and Chapter 5, different security approaches are analyzed considering vehicular Ad hoc networks security requirements and constraints. The thesis qualitative research is included in the give discussions at the end of these chapters where authors' ideas and latest knowledge on the problem area are combined to answer some of the thesis questions. By conducting qualitative research, authors concluded that a quantitative research must be made to dig more into some aspects of the problem area. Within Chapter 6, The Experiments chapter, quantitative research is applied. A large number of different tests and evaluations have been done to analyze the system behavior when security approaches are in use. Collected data are discussed to draw the latest conclusions and to answer the thesis pre-defined questions.

3 Vehicular Ad-hoc Network

The aim of this chapter is to briefly introduce the Vehicular Ad-hoc Network (VANET), its architecture, stack, communication technology and different kind of messages exchanged between ITS stations. At the end a set of safety critical applications in Cooperative ITSs are discussed.

3.1 Architecture

Vehicular ad-hoc network (VANET) is a technology that enables vehicles to communicate with each other and with infrastructure to create a mobile network. The VANET is considered to be a special type of Mobile Ad-hoc Network where vehicles are the mobile nodes. The VANET architecture consists of a backbone network including authorities and management centers, equipment installed beside the roads, namely Road Side Units, and the corresponding devices inside the vehicles, namely the On-Board Units. These components are interacting with each other as shown in Figure.1.

Road Side Unit (RSU): RSUs are stationary devices placed in critical locations of the road (e.g. junctions) capable of communicating with vehicles and the backbone network. RSUs are collaborating in VANET by distributing/collecting traffic and non-traffic related information to/from vehicles and by providing different features to manage the system. In other words, RSUs works as an interface between the backbone infrastructure and the vehicles. As an example, traffic management centers can utilize local RSUs to distribute information about traffic jams ahead and detouring guides to vehicles. Information about current traffic signage (e.g. speed limit and approaching to school signage), nearby point of interests (e.g. gas stations or restaurants) are also examples of what can be broadcasted by RSUs. One interesting application to RSUs is to recommend optimized speed to vehicles approaching to junctions equipped with traffic lights. This will let the driver pass the junction without stopping and smoothing the traffic which will increase efficiency (e.g. fuel consumption of heavy vehicles can be dropped drastically).

On Board Unit (OBU): In VANET, vehicles are equipped with devices called OBU, capable of communicating with RSUs and other nearby OBUs. OBU frequently broadcasts messages including information about the vehicle position, speed, direction, braking status and other related information associated to the vehicle (refer to 3.4). OBUs in collaboration with vehicle sensors can compute and generate a variety of messages upon different situations (e.g. emergency braking, traffic jams, accidents and change in weather condition). One example being, information about the position of a slippery road or ice spot sensed by ESC[1] sensors can be disseminated as an indication to other nearby nodes. Anti-lock braking system, air-bags condition, an opened door, turned on fog lights or windshield wipers can trigger OBU to broadcast related safety messages.

Trusted Authorities: VANET might have authorities as a part of the infrastructure in the backbone for different purposes. For example, management centers for monitor and controlling traffic. Enrollment Authorities for issuing canonical identities to vehicles [27] and Certificate Authorities for issuing, revoking and managing certificates for security purposes are other examples of possible backbone authorities.

[1] Electronic Stability Control

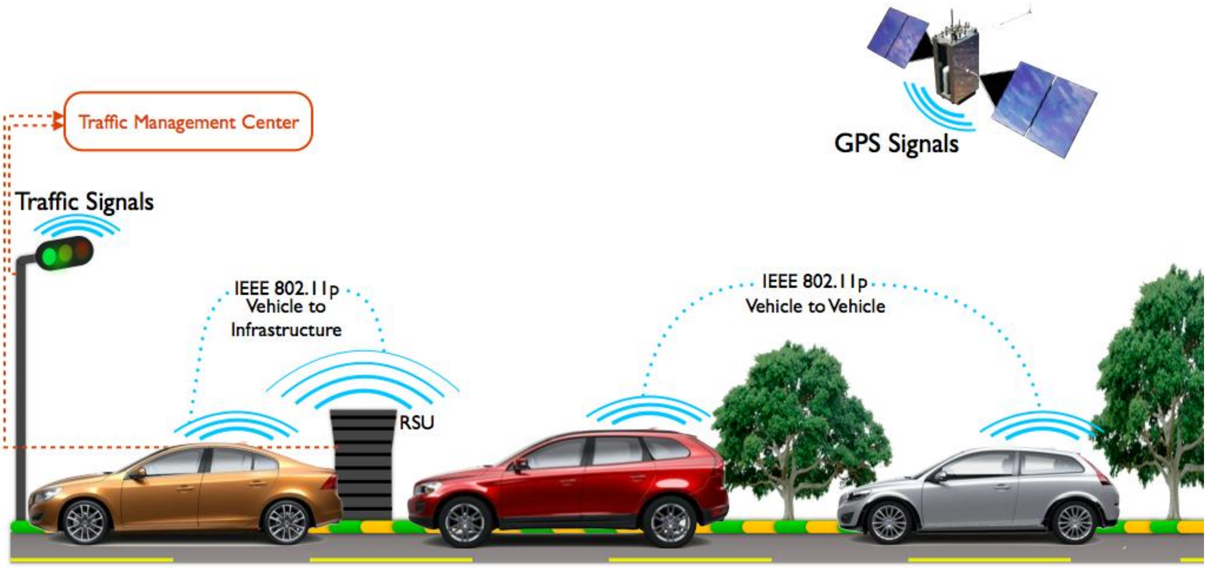


Figure 1. VANET Architecture

3.2 VANET Protocol Stack

Most probably, VANET protocol stack would follow Communication Access for Land Mobiles (CALM) architecture [3] or other similar ones. CALM is an initiative by ISO TC 204 WG16 to define wireless communication protocols for ITS [4]. It provides efficient handover, rapid connection establishments and congestion control to VANET. It supports various access technologies such as short, medium and long-range wireless communications to enable ITS stations to broadcast, unicast and multicast relative messages in between. As depicted in Figure.2, CALM stack consists of application, facilities, Networking and Transport and Access layers. Security and management layers are incorporated with all of the mentioned layers.

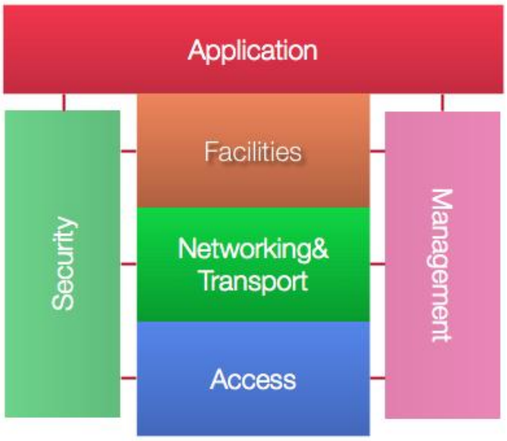


Figure 2. VANET Protocol Stack

The Facility Layer is a supporting layer for the applications which offer shared generic functions and data (e.g. refer to 3.5) to be called or fetched from the application layer. Networking and Transport Layers have equal functionality as the OSI network and transport layers with amendments to suit VANET. In other words the purpose of this layer is to provide different network (e.g. IPV6, CALM FAST and GeoNetworking protocols) and transport protocols (UDP/TCP and ITSC specific protocols etc.) [5]. The Access Layer can be compared to the two lowest layers in the OSI stack model. It is directly connected to the communication medium and is responsible for transmitting and receiving data units. The Access control layer is also responsible for other routines as sensing if the medium is occupied or not [5]. The Management Layer is responsible for supporting, controlling and managing the rest of the layers. For example the Management Layer may control the rate at which messages can be sent for the sake of congestion control in the network. It may also manage a list of surrounding nodes for routing purposes. The Security layer is responsible for handling cryptographic operations as authentication, authorization, certificate management etc. [5].

3.3 VANET Communication Technology

Due to the high mobility and speed, vehicular communication does not tolerate long establishment phases. In other words, vehicles must be able to communicate upon encountering each other. Therefore, traditional long-range communication technologies such as GPRS, UMTS, LTE and wireless local area networks (WLANs) such as IEEE 802.11 a/b/g are not efficient enough to be used for safety purposes [6]. The reason lies in the fact that all of them require authenticating and associating the parties through performing different handshakes, which cause communication latencies in the system. The former also brings extra costs to the users, which are not desirable.

In 1999, US Federal Communication Commission (FCC) allocated 75 MHZ spectrum of 5.9 GHZ frequency for Dedicated Short Range Communication (DSRC) to be used only for vehicular ad hoc networks (VANET). In 2004, IEEE 802.11 standard assigned a group, namely IEEE 802.11p WAVE (Wireless Access in Vehicular Environments), to standardize DSRC. IEEE 802.11a operates in the same frequency as DSRC[2]. Therefore, 802.11p can be achieved by conducting a number of amendments in the 802.11a MAC layer such as communication establishment processes and the PHY layer such as using 10MHz wide channels instead of 20MHz in 802.11a [7]. IEEE 802.11p enables vehicles to establish connections without the need for scanning and beaconing.

3.4 VANET Message Formats

Basically, there are two different sort of safety related messages exchanged between ITS stations which are defined by IEEE Wireless Access in Vehicular Environments (WAVE).

Cooperative Awareness Message: Cooperative Awareness Message (CAM) is a message generated by ITS stations containing specific information about their status, which are broadcasted periodically like heartbeats over the network to all nearby ITS stations in the range of a single hop. CAM includes ITS stations coordination, movement data (e.g. speed, acceleration, direction) and attributes (e.g. length and width of the vehicle). According to ETSI, a CAM message shall be generated and broadcasted every 100 to 1000 milliseconds (i.e. with 1Hz to 10Hz freq.) upon changes in vehicle’s direction (>4°), position (>5m) or speed (>1 m/s) [8].

Decentralized Environmental Notification Message: Decentralized Environmental Notification Message (DENM) is mainly generated by the events occurring on the roads for the purpose of safety to make the drivers aware of road hazardous events. DENM messages are disseminated upon detection of an event and the transmission will continue until the event disappears. An event might be reported by different ITS stations at different positions and times. In contrast with CAM, DENM is related to a specific area where the event is taking place (e.g. traffic jam ahead) rather than to a single vehicle. While CAM messages are only single hop, DENM may travel longer distances using multi hop forwarding between vehicles [9].

3.5 Local Dynamic Map (LDM)

Local Dynamic Map (LDM) is a dynamic database containing an artificial image of the real world situation into which all static (e.g. stationary vehicles or RSUs) and dynamic events (e.g. moving vehicles and other objects) are mapped. LDM is considered as an important core element within cooperative systems. The reason lies in the fact that it enables regular savings and updates of all events along with the type, position and other attributes related to the events and is therefore an effective source to all applications for retrieving desired data. Having static and dynamic information within LDM, cooperative ITS stations have the possibility to calculate, detect or guess potential hazardous events in real time. The database is updated by information received from sensors and incoming information (CAM an DENM messages) sent by the infrastructure or other vehicles in the network. LDM can either provide automatic push notification when certain conditions are met or provide information upon queries from applications [10].

3.6 VANET Applications

In VANET, applications are software designed to assist the system in generating relative indications to drivers. Naturally, applications define how to use data received from other nodes. They are also designed to generate appropriate messages derived from sensors data and other sources. Applications can be classified in various

[2] Indeed 802.11a operates in 5GHz frequency

ways. Several literatures proposed applications in different fashions [60][11][17]. For example, ETSI's basic set of applications are Road Safety Applications, Traffic Control Applications, Local and Internet services Applications, which are chosen based on the results of conducted surveys among ETSI's stakeholders [11].
In this section, we limited ourselves to investigate safety critical applications since they possess the highest priorities among the others in the system. It should be noted that we follow the VSC-A (refer to VANET Standardizations & Industrial Projects) list of safety applications which are more tangible for the sake of our thesis.

Emergency Electronic Brake Light (EEBL): Whenever a vehicle does an intense brake, The EEBL application is triggered to generate broadcast messages to the surrounding vehicles. In recipient sides, a warning will be shown to driver depending of the relevance of the event.

Forward Collision Warning (FCW): The FCW application is triggered to warn the driver about rear-end collisions (collisions with vehicles in the same lane or direction).

Intersection Movement Assist (IMA): Intersections are critical points causing most of the accidents in roads. The IMA application is intended to warn drivers about the safety status of an approaching intersection assisting them to avoiding collisions.

Blind Spot Warning and Lane Change Warning (BSW and LCW): When a driver decides to change current lanes on the road, the lane might already or soon be taken by another vehicle with the same direction in the driver's blind spot. In this case, BSW and LCW application warns the driver about the potential risk.

Do Not Pass Warning (DNPW): A driver might use another lane to pass a slow moving vehicle ahead. This has high risk when the lane is being used by vehicles from the opposite side. DNPW are designed to warn the driver not to pass the slow vehicle when collision probability is high.

Control Loss Warning (CLW): In certain situations, a driver might loose control of the vehicle. In these cases, the CLW application broadcasts a control loss event message to surrounding vehicles. Receiving vehicles may then determine the relevance of the occurred event before informing the driver.

3.7 VANET Standardizations and Industrial Projects

A lot of industrial and academic projects were or are being done within the context of vehicular ad hoc networks each trying to shed lights on a dark side of the challenge. Their collaboration and coordination towards a robust system will then inject to the standardization to be agreed and used worldwide. We bring the most well-known and honored ones including standards, collaboration platforms and specialized projects here.

eSaftey Forum: eSaftey forum is a platform aiming to accelerate and promote eSaftey systems and to support all involving road safety players from industries to public sectors in international level (Europe, US, Japan). It basically monitors the involved parties' achievements and disseminates results to all stakeholders [12]. eSaftey Forums s vision is to achieve safe, smart, clean and accident free traffic [13].

COMeSaftey: COMeSaftey as a subgroup of eSafety forum is a platform assigned to support and to accelerate vehicle to vehicle and vehicle to infrastructure communications deployment by both exchanging information and presenting the results [14]. Coordination, harmonization and consolidation of emerged projects to prepare standardization process in worldwide level are the primary goals of COMeSafety [15]. The Intelligent Transport System communication architecture and framework are mostly defined by coordinating and motivating different European projects such as CVIS, SafeSpot, COOPERS, PreDrive and SeVeCOM. Collaborating closely with standardization organization such as ETSI, IEEE, ISO and CEN leads the results to be standardized and adopted.

Car-to-Car Communication Consortium (C2C-CC): C2C-CC is an organization supported by European automobile manufacturers composed of different working groups as R&D units. It contributes to the release of an open European standard by developing, adopting and harmonizing the specifications of Cooperative Intelligent Transport System. C2C-CC Security working group (WG) analyzes technical and non-technical security requirements of secure and privacy preserving Car2X communication [16].

Secure Vehicular Communication (SeVeCom): SeVeCom is a European project aiming primarily to address security requirements of vehicular ad hoc networks and to develop and deploy a security architecture to improve immunity against threats and vulnerabilities of the system. Most of the other projects and organizations refer to

SeVeCom's results or similar whenever security is discussed. In this thesis SeVeCom project results are studied and evaluated.

European Telecommunications Standards Institute (ETSI): ETSI is a European standard in telecommunication context. ETSI TC ITS is intelligent transport system body of ETSI standard aiming to standardize architecture, protocols and applications of different parts of cooperative intelligent transport system. ETSI in collaboration with IEEE, CEN and ISO is forcing different standards to be adopted before July 2012. There are various working groups in ETSI TC ITS. WG5 is assigned for the context of Security. At the time of writing this thesis two security documents are released by ETSI; Security Services and Architecture (ETSI TS 102 731) and Threat, Vulnerability and Risk Analysis (ETSI TR 102 893). There is a third document in progress(ETSI TS 102 867) to map specifications of IEEE 1609.2 in more details, which is currently in draft version.

Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA): IEEE standards adopt a broad range of globally standards in different industries. One of the most notable IEEE groups is IEEE 802.11, which is dedicated to wireless local area networks. As mentioned before, IEEE 802.11p is specialized for Vehicular Communication to be used on DSRC band. IEEE assigned a group (IEEE 1609.2) to define security specification of vehicular ad hoc networks (e.g. secure message format and methods).

International Organization for Standardization (ISO): ISO standard assigned TC 204 to be responsible for overall aspects of Intelligent Transport Systems. TC 204 Working Group (WG) 16, which is namely called CALM (Communication Access for Land Mobiles), is specialized to define wide area communications and protocols for ITS. A sub group WG 16.7 is assigned for the context of security.

Vehicle Safety Communication - Application (VSC-A): VSC-A is a project assigned to develop and test dedicated short range communication application for V2V communication safety systems conducted by Vehicle Safety Communications 2 Consortium (VSC2) including Ford, Honda, Mercedes-Benz and Toyota R&D sections in North America [17].

It should be mentioned that ETSI, IEEE and ISO are standards collaborated to build their bodies for security issues within ITS. Organizations such as COMeSafety and Car-to-Car Communication Consortiums do the efforts to harmonize them as much as possible. Generally, there would not be any significant difference between them at least from a security point of view.
We left other projects (e.g. CVIS, SafeSpot and PreDrive) and standards (e.g. CEN) unexplained since we are mostly focusing on security parts of them which are mostly similar and in some cases are not discussed at all.

4 Analysis of Security Approaches over VANET Security Requirements

Initially in this chapter, different threats and attacks against VANETs are introduced. Security Requirements needed to protect a VANET against them are discussed in 4.2. Within section 4.3, different approaches to secure VANET are discussed and analyzed against the security requirements. It starts with a brief introduction to cryptography to make contents more tangible for the readers.

4.1 Security Threats

Denial of Service Attack: Denial of Service attack is an effort to make the resources of a system unavailable or inaccessible. Jamming is considered as one of the DoS attacks in VANET, where the attacker intentionally transmits radio waves at the same frequency that is used in communication channels between ITS stations. Interferences in the communication channel may make the ITS stations unable to exchange data in between. Resource exhausting is another sort of DoS attacks where the attacker overloads the system by exhausting the resources, causing both latency and drop of messages.

Spoofing Attack: An attack is considered as spoofing when an adversary tries to impersonate or masquerade someone or something. In VANET, an attacker may masquerade as an emergency vehicle to take the advantage of its privileges. (e.g. system will warn the drivers to keep right upon approaching an emergency vehicle).

Traffic Analysis Attack: Traffic Analysis is the process of intercepting messages to deduce desired information or interpret a pattern in data traffic. Although it could be utilized as a tool for gathering information and statistics (e.g. how often vehicles get connected to a specific RSU), it can turn into a potential attack tool for an eavesdropper. An adversary could intercept the data exchanged over the air to analyze nodes behavior, disclose sensitive information, trace the sender and receiver of the messages, violate privacy and anonymity, locate the nodes' positions, infer trip patterns etc. [18].

Man in the Middle (MITM) Attack: MITM can be considered as active eavesdropping where the attacker can get access to traffic exchange between nodes without being visible and by making them believe that they are privately connected. This has effects mostly on session-based communications in VANET (e.g. an e-commerce session between vehicle and RSU to pay for a service).

Modification[3] Attack: Modification includes transmitting falsified or modified messages to the system. In vehicular ad hoc networks, an attacker can send bogus messages to ITS stations nearby to fool them into a situation that is not real (e.g. an forged emergency break message may confuse receivers to do unexpected maneuvers causing major impact on both traffic safety and efficiency).

Sensors Tampering: Sensor tampering is manipulating sensors of a vehicle to produce false data (e.g. tampering speed sensor).

GNSS Attack: Global Navigation Satellite System is vulnerable to denial of service attacks since the signal can be interfered by jamming transmitted from a device with the same frequency as satellite transmitters. Another potential vulnerability to GNSS is signal spoofing in which a signal is transmitted fooling GNSS receivers to calculate a wrong location. When it comes to vehicular ad hoc networks, GNSS attack may cause pernicious effects (e.g. fooling the vehicle in locating itself and other stations).The attacker can also exploit temporary loss of GNSS signals (e.g. being in a tunnel) to inject fake data to vehicles [19][20].

Privacy Violation: Privacy is violated when an attacker successfully recognizes the user by associating the messages sent by the ITS station with a unique identity belonging to the vehicle which is not desired by the VANET users and must be prevented.

Location Tracking and Linking Attack: Location Tracking enables the attacker to track the user in real-time or conclude later where the user has been visiting. An adversary may also link a number of messages to a single source by analyzing the traffic exchanged by the same vehicle. The attacker may link the vehicle to areas or routes that may reveal personal data about the victim, or routes taken may be linked to real identity or other ids.

[3] known also as Alteration Attack

As an example, the victim might visit its home or job. (The victim might also visit other places, and databases may store information about the victims habits.)

Sybil Attack: Sybil attack is based on the fact that an attacker can imitate multiple nodes. In other words, a single malicious node acts as multiple nodes by creating a large number of identities. The Sybil attack is suitable for VANET. An attacker acting as hundred of vehicles, may cause other vehicles to do not-necessary maneuvers [21], [22].

Replay Attack: The effort in Replay Attack is to take advantage of using old messages to cause confusion within the network. It could be conducted by maliciously retransmitting old messages.

Wormhole Attack: A Wormhole attack is conducted against routing protocols. The attacker first creates a communication channel (tunnel) between two nodes to exchange data. Then, the data is sent through the tunnel and at the other side, another node will retransmit it to others. In other words, the wormhole attack can be considered as a replay attack conducted at different locations [23], [24].

Black Hole Attack: Multi-hop communication enables vehicular ad hoc networks to route the messages to distances not reachable by normal broadcast communication. The nodes in vehicular network can act like routers in regular computer networks. In Black Hole attacks the malicious node first convinces other nodes that it has the shortest path to destination then start to drop the packets received to prevent the messages from further dissemination to the rest of the nodes causing a form of DoS attack. A gray hole attack is a variant of black hole attack in which the attacker initially acts normal then becomes malicious making attack detection harder [25], [57].

Silent Attack: During the Silent Attack the vehicle does not transmit any data for a period of time to make other nodes believe that it does not exist.

Repudiation Threat: Repudiation is the undue denial of an action that has been performed by a user. In vehicular ad hoc networks, repudiation causes different problems concerning law enforcement and system management (accountability). A security solution needs to offer a mechanism to confront repudiating.

4.2 Security Requirements

In order to prevent a malicious node from threatening the VANET through discussed attacks, a number of security requirements must be held by the system, which is discussed below.

Authentication: Authentication is the process of confirming or determining if an identity of a user is what he/she/it claims to be. It can be accomplished through confirming what a user knows (e.g. password), what a user has (e.g. ID card or Token), what a user is or does (e.g. biometrics or user’s signature) and where user is (e.g. being at a place at a certain time). Authentication is one of the critical requirements to apply security in vehicular ad hoc networks. Authentication verifies that the messages are received from a trusted source and not an adversary or malicious node (refer to Spoofing and MITM attacks).

Message Integrity: Integrity is the process of detecting any modification, corruption or loss of data. Integrity does not prevent a message from being altered it rather makes alterations detectable. Wireless networks are transmitting in the air, therefore open for intentional (refer to Modification attack) or unintentional (e.g. interferences or disturbances) alterations. Hence a mechanism must be provided to vehicular ad hoc networks to preserve messages integrity.

Message Confidentiality: Confidentiality is a goal in information security context aiming at preventing disclosure of secrets or other critical information to unauthorized parties (refer to Traffic Analysis Attack). Information shall only be exposed to trusted and authorized participants. Road safety messages are public to all vehicles and therefore do not need confidentiality, only messages containing sensitive information must be protected against eavesdroppers (e.g. credit card number in a transactions).

Availability: Information, resources or assets must be accessible at any time needed. Availability aims to have system available when needed. Availability is one of the biggest challenges in vehicular ad hoc networks. For example, denial of service attacks or jamming prevents the assets from being accessed and causes the whole or a part of the system to become unavailable. Cryptography algorithms/protocols should also be carefully chosen and used otherwise they may turn into bottlenecks in ITS system especially where bandwidth is low and computationally limited devices are in use which may hinder scalability of the system by overloading the bandwidth or processor load.

Non-Repudiation: Non-repudiation is a security requirement to prevent a user from denying a certain action that has been performed by him/her (refer to repudiation threat). In vehicular ad hoc networks, sender shall provide an assurance so he/she cannot later deny transmitting/receiving the message. Non-repudiation is desired for trusted authorities especially for law enforcement purposes (e.g. recognizing guilty driver in a traffic accident).

Privacy Preservation: Privacy is the right of preventing personal data from being disclosed to strangers. VANET should care about privacy-preserving solutions to have public acceptance. VANET Users should be aware of the related information the system disseminated in behalf of them. Since collecting vehicle and driver's information from communications overheads is possible in wireless networks, privacy must be preserved in order to protect a driver's identity, location and other related information from adversaries (who might seek financial benefits or other misuses). We contrasted three different privacy concerns which must be preserved within VANET.

- **Identity Privacy:** Information broadcasted from vehicles may contain data which can be linked to the real identity of the owner, this is against privacy. It is therefore necessary to prevent the system from using such information.

Location Privacy: Location privacy refers to the ability of a user to protect his/her position from non-authorized parties. Location privacy security requirement limits Location Tracking in VANET.

- **Unlinkability:** Information in different messages, transmitted between the ITS stations should not be linkable to each other since an attacker more easily may track the vehicle. Message content should not give the opportunity to adversaries to relate the message to a specific vehicle (e.g. including vehicle attributes like length, brand or color) [26]. A Security solution should be able to support unlink-ability requirement to prevent attacks such as linking attacks.

Privacy must be provided in a conditional way. Conditional privacy means that users must be protected from unlawful tracing but at the same time a trusted party should be able to either trace a vehicle to bring proof for jurisdictional purposes, in case of a crime or revoke misbehaving users from further disturbing the system.
Perfect privacy is not desired since functionality in applications may get affected. (e.g. Emergency break requires the correct position of the vehicle). And if there is no possibility to distinguish between nodes, routing cannot be achieved, and possible sibyl attacks may be generated. Therefore privacy should be considered from both a human and a system functionality perspective.

Data Freshness: Received data may be retransmitted again for malicious purposes (refer to Reply and Wormhole Attacks). Therefore a security solution should provide information about freshness of the messages.

Revocation: An attacker, tampered software/hardware or a faulty device may lead the system to broadcast bogus messages causing sever harms to other vehicles' safety. Therefore such nodes must be recognized and revoked from the system as fast as possible to prevent them from functioning in the system or informing others about their revocation status. Other purposes such as Legal consideration (e.g. stolen vehicles or running after an accident) and administrative considerations (e.g. payment refusal) make revocation a critical security requirement for VANET.

Secure Hardware: Unauthorized accesses to security credentials and other data must be prevented at each ITS station. This is achieved by utilizing tamper proof devices, which can persist against physical and logical attacks. These devices should be capable of performing cryptographic operations and storing secret keys and logged data. All sensors, communication facilities and human machine interfaces must also function correctly and in a secure way.

4.3 Security Approaches to VANET

A security approach to VANET is a set of different security mechanisms which provide needed security requirements together to protect VANET against the threats and attack its facing. A security solution must be designed in such a way that both security requirements and system constraints can be addressed at the same time. Following this chapter, Different categories of VANET security approaches including Asymmetric, Hybrid (of Asymmetric and Symmetric) and ID-Based Cryptography as well as the Verify-on-Demand concept are

introduced respectively. Finally an analysis section is dedicated to discuss all of their characteristics in against discussed Security Requirements.
Before going through introducing different security approaches, initially a brief introduction to computer security and a few security terms is given.

4.3.1 A Brief Introduction to Cryptography

Cryptography is the science of protecting data which is being transmitted between two or several information systems against interception, modification and other threats. In computer security, the data is protected not by hiding the data but by changing it into a form (cipher text) that only recipient(s) or the parties who possess a special knowledge (mostly called key) can make it the same form of the data the sender sent (clear text) while assuring that the data is most probably unreadable to other unauthorized parties. In cryptography science, the process of creating a cipher text from a clear text is so-called *encryption* and the backward process is so-called *decryption*. Cryptography can be further discussed into two fields of *Symmetric Key* and *Asymmetric Key (Public Key) Cryptography*. At the end, the concept of ID-Based Cryptography, which is assumed as a new form of Public Key Cryptography is discussed as well.

Symmetric Key Cryptography: Symmetric Cryptography uses the same key in encryption and decryption processes so it is mandatory for sender(s) and recipient(s) to decide on a shared key before communicating. Sharing a key is considered as a tricky process in symmetric key cryptography and can be problematic since the key also must be protected against disclosure to adversaries in transition to parties.
Symmetric key cryptography does not provide authentication of the senders or recipients standalone except having third trusted authorities in between which manages the shared keys and identities in such a way that parties can authenticate and know each other (e.g. Kerberos Authentication systems).
Authentication based on symmetric key cryptography can be utilized in small or at most medium size systems (such as computer network in an organization) in other words it is not considered as a scalable system (problem of key management). It also suffers from having a large number of handshakes between parties and authorities for each communication. In contrary, symmetric key cryptography benefits from being fast in security processes it does within encryption and decryption. In other words, the computational power and the time needed to do the processes are lower than other type of cryptography (asymmetric key cryptography). 3DES, AES, RC4 are three well-known algorithms used in symmetric key cryptography.

Public Key (Asymmetric) Cryptography: Compared to symmetric cryptography, asymmetric key cryptography provides each member with a key pair instead of one single key. These keys are called, Public key and Private key. Public key is known to all in the network and everyone are able to access it. The private key is kept secret for each member and only accessible by him/herself. The key pair are bound to each other and does the process of encryption and decryption inversely where one key is used for encryption the other one can be used for decryption i.e. If one can download the public key of another member and use it to encrypt a text, no one except the second member, who posses the private key, would be able to decrypt the cipher text. It should be mentioned that it is mathematically (nearly) impossible to derive a member's private key having his/her public key.
Since invention of asymmetric cryptography, several algorithms with different characteristics are introduced to fulfill the idea behind it. Asymmetric cryptography algorithms typically exploit hardness of mathematical problems or assumptions (e.g. Factoring of Large Integers problem, Discrete Logarithm problem and Diffie-Hellman assumptions) to be secure enough against cryptanalysis.
Public key cryptography solves the problem of key sharing since parties are able to obtain each other’s public keys by downloading from a depository or can be appended to the cipher text by the sender without the fear of disclosure. Another advantage over symmetric key cryptography is to have authentication possibilities standalone [refer to Appendix Digital Signatures].
The public key needs to be bounded to an identity; otherwise a malicious user may fool others by giving a wrong public key, so a trusted authority must approve the public key and its bounded identity. After approving one’s identity, the trusted authority will give a document including his/her identity and public key and etc. called Certificate[4] which is signed by the authority's private key [refer to Appendix A].There exists also another certificate type called Implicit certificates, which is introduced in Appendix C.
Asymmetric key cryptography solves a lot of hassles in key establishment of a secure system. Comparing to symmetric key cryptography, asymmetric cryptography is computationally intensive. A system composed of CA, certificates and signatures is known as Public Key Infrastructure (PKI). Besides, confidentially and authenticity of sender/receiver, PKI can bring a new possibility to defeat repudiation threat meaning that if a member uses his/her private key to sign a message, he/she could not be able to repudiate it later.

[4] Explicit Certificate

Certificate authority is also responsible for revoking misbehaving members meaning that a certificate being violated can be declared as invalid. This is accomplished typically by disabling misbehaving users' certificates then distributing a list of revoked ones called Certificate Revocation Lists to all members.

4.3.2 Public Key Cryptography Approach to Secure VANET

Asymmetric cryptography utilizing PKI is probably the most promising type to be used in vehicular ad hoc networks. Since it provides **Authentication**, **Confidentially** (if needed), **Integrity** and **Non-Repudiation** standalone, which are achieved through utilizing digital signatures created by cryptographic algorithms. Public key cryptography provides most of the security requirements standalone but privacy preservation and revocation security requirements need a wider look.

Public Key Cryptography vs. Privacy: Privacy security requirements need the system to consider identity, location privacy and also unlinkability. These features should be performed in a conditional way so that trusted and legal authorities can still recognize or track the vehicle.
To achieve identity privacy, the real identity of the owner can be replaced by a pseudo identity. We will call it Pseudo-ID. Having an immutable pseudo-ID may help an adversary to link it to positions in order to trace or track the owner, which is against the location privacy and unlink-ability feature. A solution to this is proposed by Raya et al [26] where to have many pseudonym-certificates stored within the OBUs, to be used upon time passed or distance traveled by a vehicle. The number of pseudonyms may vary and different numbers have been proposed. Car-to-Car communication consortium proposed to store 1500 short-lived certificates for one year, each possessing one pseudo-ID (so called pseudo-certificate). Assuming a vehicle would be used 4 times a day then it will consume one pseudo-certificate for each ride. Raya et al. [26] proposed to store 48000 certificates in each OBU to be switched more frequently.

Public Key Cryptography vs. Revocation: The Scale of the system, high mobility of nodes, vehicles inaccessibility most of the time, low deployment of infrastructure in early stages, size of information to be distributed and added operation to each verification process make revocation a big challenge for VANET security specialists. Revocation mechanisms that verify the sender against a trusted party after the message are been received are not suitable since this would invalidate the real time constraints. Various solutions are proposed in different literatures, which are generally discussed in this section.

• **Certificate Revocation List (CRL):** A CRL contains a list of revoked vehicles IDs and a signature from the authority which issued the revocation list. This list must be disseminated among all ITS stations.

• **Certificate Revocation List using Geographical Divided Zones(CRLDZ):** To limit the CRL distribution and size, several proposals as [76][77] have been made to divide VANET into geographical zones. Whenever a vehicle leaves a zone its previously valid certificates becomes invalid (if the vehicle has a TPD the certificates can even be removed from the vehicle) and the vehicle has to apply for new certificates for the new zone.

• **Short-Lived Certificate:** A short-lived certificate is a certificate which possesses an expiration time. Therefore it is valid for a certain period of time. Short-lived certificates can eliminate the need for distributing CRLs. If a certificate gets compromised, it will be automatically revoked or disabled after a certain period of time.

• **Adversary Certificate or Remove Notification:** Samara et al. [33] proposed a solution in which, an adversary certificate will be injected to the revoked vehicle. Signing the outgoing message with this certificate will result in rejection at the recipient sides. Raya et al. in [34] proposed a similar solution in which a tamper proof device on the OBU will delete all credentials of the vehicle upon receiving the revocation message from the infrastructure.

4.3.3 Hybrid Approaches to Secure VANET

Infrastructure Aided Symmetric Solutions (IASS)
Wu et al. in [61] and Zhang et al. in [41] proposed a similar solution in which a RSU is involved in process of inter-vehicle communications verification. Based on the range of communication, each RSU comprise a zone for itself. When a vehicle enters the zone of a RSU, a symmetric key and an ID will be established between the OBU and the RSU through the Diffie-Hellman key establishment secured with signature scheme [42] the key may also have been pre-established from a previous establishment [61]. This key will then be used by vehicle to create message authentication codes [refer to Appendix A Hash Function] of each outgoing message. Vehicle's ID, message content, time stamp and MAC of them, all appended together and broadcasted to other nodes in the

system. Since a receiving nodes do not possess the symmetric key, which is used to create the MAC, are therefore not be able to verify the message. Instead they will create a hash of message and discard the MAC and then will wait for next message, which will be broadcasted by RSU after a certain time window. RSU has a database of all IDs and symmetric keys assigned to them. The RSU will receive the message sent by vehicles so it can calculate MAC of incoming messages and compare it to the MAC appended to message. If they are identical then the message is authenticated. RSU will then create hash of the authenticated message and append it to several other authenticated messages until a certain time has elapsed. It then signs the whole hash chain and broadcast it to the zone. Recipients will then verify the authenticity of pre-received and cached messages by comparing them with the ones sent by RSU.

IASS vs. Authentication: As mentioned, messages broadcasted by RSU contain a digital signature to be used for RSU authentication and the message content will be used to authenticate the message received from surrounding vehicles. The Mac in the message authenticates the vehicle to the RSU.

IASS vs. Integrity: Both MAC and Signature provides Integrity to the messages.

IASS vs. Privacy: Privacy is preserved using k-anonymity [58] concept. The idea with k-anonymity is to assign all of the vehicles in the RSU zone with the same ID in which, RSU can distinguish them but the other nodes cannot. This is possible since RSU knows all used keys, and may test them exhaustively to find the sender.

IASS vs. Revocation: Revocation requirement is also provided to IASS by distributing the CRLs up to the level of RSUs. RSUs will not assign Keys and IDs to revoked vehicles. Vehicles may also be revoked instantly, since all traffic must pass thought an RSU.

IASS vs. Non-Repudiation: Since RSU possess a table of vehicles assigned IDs and symmetric keys, it would be used as a proof against repudiation threats for each message sent by the vehicle.

Time Efficient Stream Loss-tolerant Authentication (TESLA)

TESLA is an authentication protocol that benefits from symmetric cryptography's high computation speed and tiny generated overhead. TESLA requires the nodes to be timely synchronized (e.g. they may sync with a GPS clock). TESLA utilizes a one-way hash function [refer to Appendix A] in corporate with synced time feature. Initially, sender side chooses a random value and creates a one-way hash chain, which is calculated by repeated hashing the returned value of previous hash function. The bottom of the chain (the anchor) can be calculated from all of the other chains in the hash chain but the opposite way is impossible. The sender also chooses a start time and an interval time. Each determined interval time corresponds to one of the hash values in the chain. Start and interval time as well as the anchor value of the hash chain are then signed [refer to Appendix A] and included in the first broadcast messages to the other nodes. Each of the values in the chain is then used as a key to create a MAC of each outgoing message in that particular interval. Note that the key has not been released by sender yet so the recipient side is not able to verify the message until the key get disclosed in later intervals. When the sender reveals the hash value corresponding with that particular time interval, the receivers can verify the key by calculating the hash of it and comparing it with the hash chain end value received before [43]. The key can never be used for signing messages, since all vehicles knows that the interval for that key has passed. This is why the nodes needs to be timely synchronized.

There exist two options for key release. In one approach the key is released after a fix period of time and the approach, called TESLA Piggyback, the key is released in the next message.

TESLA is vulnerable to DoS attacks where an adversary may flood a node by sending multiple messages to a node. TESLA++ is an updated version of TESLA. First, the MAC of message is sent and in the next interval the message and the key are broadcasted [44].

VANET Authentication using Signatures and TESLA++ (VAST)[5] is a protocol which combines asymmetric cryptography (refer to next section) and TESLA++. Sender signs the message with its private key to create a digital signature. A MAC is then generated of the Message concatenated with the signature and the secret key for that interval and broadcasted to other vehicles. On receiving side, the node verifies the key using one-way hash function and comparing with a hash value in the chain. If the node has not previously authenticated a key in the chain, the node uses the public key of the sender to authenticate the message.

TESLA/TESLA++/VAST vs. Authentication and Integrity: Authentication is achieved by first authenticating the delayed released key using the hash function. The Message is then authenticated by calculating and

[5] or TADS (TESLA Authentication and Digital Signatures)

comparing the MAC of received messages. In case of VAST, one might authenticate the sender through the appended signature to the message.

TESLA/TESLA++/VAST vs. Non Repudiation: Apparently non-repudiation is only achievable through VAST since it includes a digital signature of each message so application needing non-repudiation may verify the digital signature. It might be argued that VAST only provides non-repudiation if the digital signature is verified, verify the MAC do not verify that digital signature is correct. All other alternatives lack in providing this requirement.

TESLA/TESLA++/VAST vs. Privacy & Revocation list: Since Tesla is based on PKI, it utilizes the same principles for privacy and revocation as in PKI.

4.3.4 ID-Based Cryptography Approach to Secure VANET

Identity based cryptography is a form of asymmetric key cryptography in which public keys of the users could be either their identity, social security number, street address, telephone number or any other string which represents a unique identity of the user and cannot be denied later. The correlated secret key is issued by a trusted authority and will be given to the user in a secure form (e.g. on a smart card or a trusted platform module) [62]. ID-based cryptography scheme was firstly introduced by Adi Shamir in 1984. The proposal was to simplify certificate management in email systems [36]. In other words, it allows users to verify digital signatures using identity or email address of the signer.

The scheme proposed by Shamir remained unsolvable until 2001 when D. Boneh and M. Franklin proposed a secure and efficient solution to the context. The solution, called Bilinear Pairing(BP), bases on the modified Weil or Tate pairing [36] constructed on the Elliptic Curves. Security of BP scheme is based on the Diffie-Hellman assumptions in which the Decisional Diffie-Hellman problem (DDH) is easy but the Computational Diffie-Hellman problem (CDH) is difficult to solve. Theoretical of Bilinear Pairing scheme is introduced in appendix B.

Since advent of Bilinear Pairing, a number of novel schemes such as BLS Signature Scheme [63], Signcryption [64], Blind and Threshold Signatures have been proposed.

The need for distributing the public keys as in traditional public key cryptography can be discarded through utilizing pairing based schemes [35]. Further, sending a certificate along with messages increases the size of the data to be sent which may lead to limit bandwidth when number of messages arises which seems convenient to be used in VANET.

A few of BP schemes adopted to be used in Vehicular Ad-hoc Network such as [35][37][39][40] have their own advantages and disadvantages.

Researchers has proposed schemes such as Aggregated or Multiple Signatures and Batch Verification, in which, a number of signatures coming from one node or different signatures from multiple nodes can be verified at once. In other words, instead of using pairing operation for verification of each signature, it can be used to verify *n* signatures at once. If batch verification returns false, it means that there are one or more false signatures existing in the batch. These false signatures can be discarded by utilizing divide and conquer algorithm and redoing the batch verification for each divisions [65]. Another advantage of BP is its possibility for privacy. BP schemes [74][40] offers both the possibility of self generating pseudo-IDs or anonymous signatures. In these schemes there is no need for certificates.

BP-Based Schemes vs. Authentication, Integrity and Non-Repudiation: These three requirements are fulfilled through appending a signature generated on the content of the message.

BP-Based Schemes vs. Privacy: Privacy security requirement in BP based schemes is provided efficiently wherein most of them a pseudonym is generated for each outgoing message [35], [39]. Zhang et al. [35] used mathematical operations within ID-based cryptography (such as point multiplication) to generate pseudo-IDs out of real identity for each out-going message. These pseudo-IDs will involve both authentication and verification phases. A trusted authority possessing the secret key can calculate real-identity of the vehicle back from pseudo-IDs. Therefore, it provides all privacy preservation requirements.

BP-Based Schemes vs. Revocation: In schemes based on protecting privacy by using anonymous signatures or self generating IDs, only revocation lists are possible. Revocation is one of the concerns faced in BP-based schemes where checking the revocation status of each incoming signed message (for example in revocation list) involves heavy mathematical operations.

4.3.5 The Concept of Verify on Demand

Safety application should warn the driver whenever a threat is recognized. Only a few of receiving messages contain information that affects the driver's safety [45]. For example, a moving vehicle may not need to process the messages broadcasted from other vehicles behind except in special cases such as approaching emergency vehicles from behind or notification of an overtaking vehicle. Incoming messages may also carry repetitive information about an event. These redundant messages can be discarded before being verified.

In contrast with verify-then-process approach, which only considers the messages that have been verified successfully, verify-on-demand (VoD) processes the context of the message first, then it decides on whether data is needed to be verified or not i.e. the messages are verified only if they are assessed as safety critical, relevant or useful. This is possible through processing the incoming messages and assigning a safety level to each of them. Based on the given levels made, the category that the message is belong to and the processing power available, it will be decided to verify an incoming message or not [45].

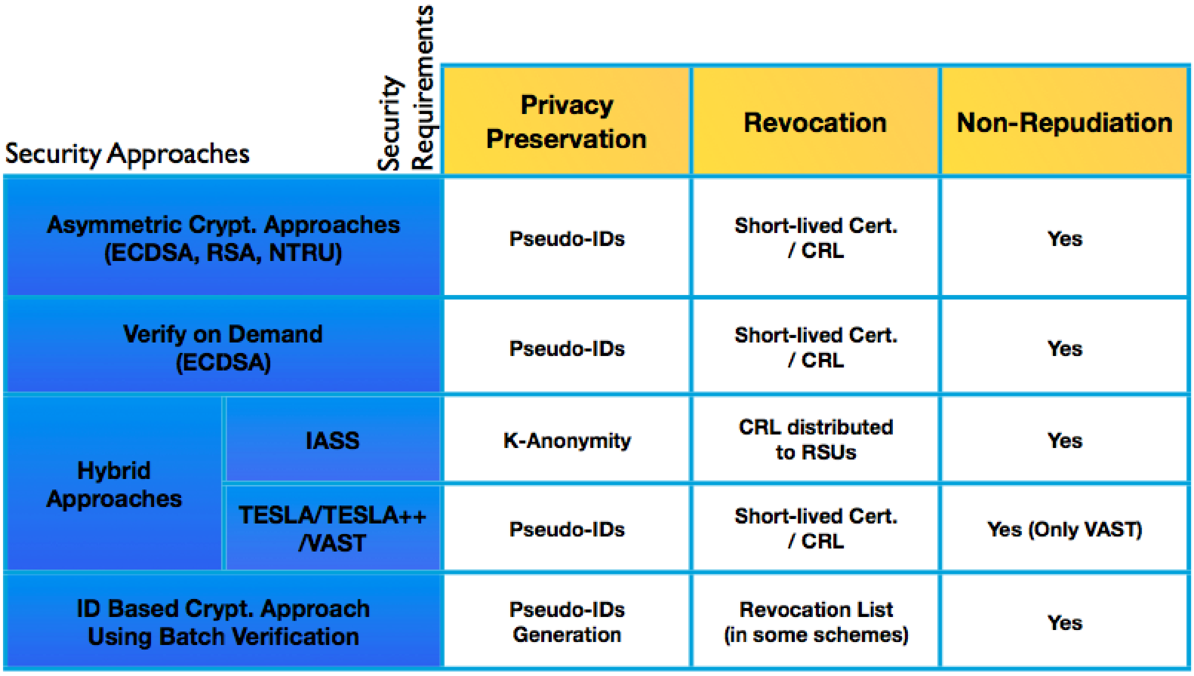
4.4 Other Considerations

Time Stamp and Sequence Number: Data-freshness is one of the security requirements mentioned. Time information in each incoming message could help the receiver to reject expired or old messages. Normally, Timestamps and Sequence Numbers are recommended to protect a system against attacks such as Replay Attack. A timestamp denotes the time at which the message is processed and broadcasted from a node. It is inserted in the message structure and signed digitally to be protected against any alteration. Sequence Number can also be utilized in VANET but it is basically useful in case of a unicast communication or streaming.

Logging: In case of an accident or a probable miss-use or malfunctioning of device, a security alternative shall provide relevant information and evidences to be used by police or other trusted authorities. Non-Repudiation and Revocation security requirements and a mechanism to log incoming and outgoing messages along with a tamper-resistant security module to protect the secret keys are essential for this sake. Caching or logging the messages shall be done for a certain period of time. This period shall be selected effectively in such a way that it considers both governmental policies and hardware capacity limitations.

4.5 Summary

Table.1 shows the comparison of different discussed approaches against security requirements. The table does not show confidentially, integrity and data freshness security requirements since these are fulfilled by all solutions. The first goal of these approaches is Authentication security requirement, which is therefore provided. Regarding authentication, various experiments including delays in authentication generation (signing) and verification are done in the experiments chapter.



Security Approaches	Security Requirements	Privacy Preservation	Revocation	Non-Repudiation
Asymmetric Crypt. Approaches (ECDSA, RSA, NTRU)		Pseudo-IDs	Short-lived Cert. / CRL	Yes
Verify on Demand (ECDSA)		Pseudo-IDs	Short-lived Cert. / CRL	Yes
Hybrid Approaches	IASS	K-Anonymity	CRL distributed to RSUs	Yes
	TESLA/TESLA++ /VAST	Pseudo-IDs	Short-lived Cert. / CRL	Yes (Only VAST)
ID Based Crypt. Approach Using Batch Verification		Pseudo-IDs Generation	Revocation List (in some schemes)	Yes

Table 1. Security Approaches comparison considering security requirements

5 Analysis of Security Approaches over VANET Constraints

VANET is facing constraints and limitations, which are mostly originating from its nature such as high mobility and semi-random network topology changes. Hardware designed for VANET also bring more limitations to the system such as wireless link bandwidth or OBU's computational power. A security mechanism must not only provide VANET security requirements, but must also be able to overcome VANET system constraints to be robust and scalable.

In the following sections, VANET system constraints will be discussed and then used to evaluate and analyze proposed security approaches to VANET.

5.1 VANET System Constraints, Limitations and Characteristics

Timing Constraints: Since vehicular ad hoc network is a real time system that handles safety related applications, time constraints must be carefully taken into account. Otherwise, some parts of the system may turn into bottlenecks or emerge as points of failure. It is obvious that safety related warnings must be announced in a period of time enough for the driver to be able to react in time. Several non-human factors plays a role in deriving end-to-end timing requirements of VANET applications such as average and maximum driving speed, wireless link transmission delay between two or N nodes, average time of heavy operations such as security operations in each node and etc. Different active ITS research teams and standards specified a maximum end-to-end delay for different applications and use cases. For example, ETSI [8] and SeVeCOM [29] recommended 100 and 500 milliseconds respectively.

Bandwidth Limitations: IEEE 802.11p could support transmission rate between 3 and 27 Mbps, which is performed on a bandwidth of 10 MHz [30]. Wireless link can emerged as a bottle neck in communication between ITS stations especially when the number of nodes increases. The reason lies in the fact that when generated data traffic exceeds the available bandwidth, the network performance degrades due to inter-system interference [14]. This further produces congestion in the medium access, which leads to increase the packet loss rate, transmission or end-to-end delays.

IEEE 802.11p uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to prevent congestion and collisions by enforcing random back-offs when the channel found to be busy by a transmitting node. Performance of CSMA/CA in congested scenarios is not yet proven to be robust and argued in different literatures [31] [32].

It is critical to use a security mechanism which is highly efficient in terms of generating security overheads and bandwidth usage.

Computational Power and Storage Limitations: Devices installed in OBUs or RSUs are limited in terms of computational power and storage. Adding extra hardware will increase the cost of their implementation and production. Security mechanism operations must be computationally feasible even having a lot of nodes sending and receiving messages. Onboard storage should also be utilized efficiently. Size of security credentials, revocation methods, logging and caching policies affect the amount of storage needed in the ITS stations.

Routing Feature: For some applications data needs to be forwarded to vehicle not in the range of one-hop. Especially data related to a specific area as data included within DENM messages need to be routed to all vehicles within the area. It is important that the proposed security solutions are able to handle routing efficiently.

VANET Topology Change: Since VANET is a mobile network with roaming nodes vehicles it constantly gets new neighbors. Some vehicles follows the same route and are therefore neighbors for a long time, whereas others are driving in the opposite direction and are neighbors for only a few seconds. This is also one of the reasons why it is not suitable for establishing connections between vehicles.(e.g utilizing symmetric communication channels).

VANET Deployment: It takes time for VANET to be completely deployed. For example the number of RSUs in early stages might be limited. Therefore, proposed security mechanisms must be independent of infrastructure as much as possible to be widely available. It is also not desired/possible to use other wireless technologies since they may cause extra cost and effort to the system.

Unbounded Network Size: Mentioned in [75], the size of VANET could be arbitrary large, and may involve anything from one city to a country or even the whole world. A solution in VANET should therefore not be affected by its size and scale.

5.2 Public Key Cryptography Approaches Analysis

Asymmetric algorithms can be compared by their performance, signature and key sizes. The former would be left out to be tested in next chapter. We will test them on VANET prototype to derive more accurate and real values. Signature and key sizes of selected algorithms will be tested in figure.5 in the next chapter.

CRL vs. Unbounded Network Size and Storage Capacity: Revocation lists tend to be large. According to Wolfram-Alpha statistics, there are 53.2 million vehicles in use in Germany [67]. Even if one percent of the total number of vehicles in Germany get revoked (assuming that each vehicle possesses one certificate), the CRL list would contain 532000 revoked certificates. It can be argued that 1 percent is considered large, but it is important for a system to be able to handle extreme values, otherwise the system may fail during system usage, with consequences. Also to consider the size of a country is not large, if the network is unbounded it may have the size of the whole world. Assuming that CRL contains pseudo IDs of size 8 byte for each certificate then the size of CRL would be approximately 4.06 megabyte which must be distributed to all nodes nation wide. This is the case when only one pseudonym is present. Consider the case when all pseudonym certificates from a vehicle are needed to be revoked. In Car-to-Car consortium a vehicle contained around 1500 certificates to be used within a vehicle, this will give a list with a size of around 6,1 Gigabytes of revocation data. It may be concluded that pure revocation lists does not scale well with VANET.

CRL vs. Bandwidth Constraint: As mentioned in the section before the size of revocation lists tends to be large. Considering the case using one ID, 4,06 megabyte, this amount would take approximately 10 second to be sent through a 3mbps channel. During this period no other vehicles are able to transmit in the medium. The case of 1500 certificates would take around 4.2 Hours to be transmitted in the wireless medium.
Further, this list should be updated regularly. This might be a great burden on the infrastructure. Even having different compressing functions, would assumingly not be able to shrink the list enough.

CRL vs. VANET Deployment: Vehicles basically download the CRL through RSUs which means that VANET must be deployed enough for the vehicles to download the latest CRL everywhere. As mentioned before long-range communications such as GPRS, UMTS and LTE are not desirable to distribute revocation lists. Involvement of telecommunication industries increases the costs and efforts to manage the system.
Further, inaccessibility (in not covered areas) and delivery latency are of the other drawbacks to them. Approaches have been taken to more efficiently distribute the CRL. Papadimitratos et al. [49] suggested dividing CRL into several pieces then distributing them separately when the vehicles come available. Laberteaux et al. [50] went further and suggested to use car-to-car communication to share and distribute CRL between nodes when RSUs are not available which both make the CRL distribution faster. The results in [50] even shows better results than if VANET where fully deployed of RSUs. Still this solution did not consider the size of the revocation lists since this solution might suffer from large unavailability in bandwidth resources. This might be a safety risk in the system. Not considering the size, this solution actually works for VANET Deployment.

CRL DZ vs. Unbounded Network Size: Compared to regular revocation lists, the scale of VANET does not affect the CRL DZ in the same amount as pure CRLs since the number of vehicles are bound to the size of the zone.

CRL DZ vs. VANET Deployment: Each road exiting from one zone to another zone needs at least one RSU for the vehicle to receive a new valid certificate. When the size of the zone shrinks the more RSUs are needed which makes it highly dependent of the infrastructure.

CRL DZ vs. Limited Bandwidth: A smaller zone gives a smaller revocation list which needs to be distributed within VANET.

CRL DZ vs. Storage Capacity: CRL only need storage capacity to the extent of the number of revoked vehicles within the zone.

Short lived Certificates vs. Routing Feature: Changing pseudonyms may affect the performance of some protocols who are mostly relying on geographical routing, which is based on neighbor awareness. These protocols may also need constant MAC addresses of each node for their purpose which is against privacy preservation. Changing either Pseudonyms or MAC addresses may either mislead a vehicle about the existence of an extra node or lead messages to be lost since there is no receiver available any more [47][46]. To continue within this area an analysis of risk and cost is needed to decide on the number of pseudonyms to be used.

Short-lived Certificate vs. VANET Deployment: Regarding Short-lived certificates, existence of a vulnerable period between the time that a certificate must be revoked and the time that the certificate expires is the disadvantage of this solution. Another drawback to short-lived certificates is that, they allow a malfunctioning OBU or sensor to keep generating bogus messages until the last one short-lived certificate get expired which is against safety in VANET. Therefore, to minimize this vulnerable period, the vehicle should update short-lived certificates more frequently, this makes it more dependent on the infrastructure.

Short-lived Certificate vs. Storage Capacity: Short-lived Certificate also requires each vehicle to save a number of short-lived certificates in OBU or to update them regularly. Short-lived certificate is recommended by IEEE 1609.2 and C2C-CC (at least in their latest drafts). Current discussions on this solution are mostly about the number of pre-saved short-lived certificates, certificate consumption frequency and updating mechanisms, which are mostly affected by privacy preservation strategies. Apparently, less expiration period requires more certificates to be saved for example in one year inside each OBU. This period should be selected in such a way that it can mitigate the misuse of a compromised certificate and at the same time it considers updating costs and efforts as well as OBU storage.

Short-lived Certificates vs. Computational Power: Imagine that each vehicle has a data structure for storing previously verified certificates so the same certificate does not need to be verified twice. The more often the certificates are changed, the more certificate verification is needed.

Adversary Certificate or Remove Notification vs. VANET Deployment: Would need the revoked vehicle to get available and connected to infrastructure. Otherwise, the malicious or malfunctioning node can continue to put the system in risk. A vehicle may refuse to get adversary certificate or remove notification in different ways (jamming RSU signals, hiding, etc.).
Short-lived certificate seems to be a better option since it does not have the problem of scaling as the CRL has. But this is true only if the vehicle could update the stored certificates frequently enough for both privacy and revocation purposes.

5.3 Hybrid Approaches Analysis

From a computational point of view, Symmetric Solutions outperforms pure asymmetric approaches discussed earlier since mechanisms including MAC and one-way hash functions are both much faster than operations performed in asymmetric solutions. On the contrary, they require a nearly fully adopted VANET's infrastructure.

IASS vs. VANET Deployment: IASS require a nearly fully adopted VANET, since the IASS are highly dependent of RSUs. This makes the solution not suitable for establishing.

IASS vs. Bandwidth Limitations: A large number of messages in the air may cause congestions and collisions, this may be the case if key establishment have to be proceeded at every RSU. If the key is pre-established, only the broadcast message from RSU is added. It also should be mentioned that if the RSUs accumulated message gets lost in the air then no vehicle in the zone would be able to verify the cached messages.

IASS vs. Timing Constraints: IASS adds an extra delay since messages need to be accumulated before RSU broadcast the message. One problem that may appear is if a vehicle leaves a zone before RSU broadcasts, then the vehicle will not be able to receive the message.

IASS vs. Computational Power: Symmetric keys are used for signing messages, and only one digital signature is signed by the RSU. This lowers the computational burden on vehicles.

IASS vs. Storage Capacity: Since a vehicle needs neither to store multiple certificates for privacy purposes nor to store large revocation lists, IASS lowers the burden on storage capacity on vehicles. On the other hand, RSUs need to be able to store lists of vehicle keys and revocation statuses.

IASS vs. Routing Feature: This is possible if the RSUs have overlapping zones and vehicles within this overlapping zone have the possibility to receive messages from both RSUs.

IASS vs. Topology Change: IASS is mostly affected by incoming and outgoing vehicles within the zone when it comes to topology change. Also mentioned within Timing constraint, vehicles leaving the zone may not be able to receive the latest sent messages.

TESLA/TESLA++/VAST vs. Bandwidth Limitations: Regarding key releasing strategy, TESLA Piggyback burden the bandwidth least, since less messages are exchanged in the air, but on the contrary suffers from larger verification delays. If a fixed time key releasing is set to a small interval, the verification delay would be smaller but this solution suffers from more congestion in transmission [44]. VAST increases the signature size on each message since the message carries both kinds of signatures (a MAC and a digital signature).

TESLA/TESLA++/VAST vs. Timing Constraints: Generally, TESLA protocols despite their efficiency in saving computational power suffer from the delay they cause to verify a message (up to 100ms [51]) which are undesirable for delay-intolerant VANET system. It’s possible to shrink the delay, but in cost of bandwidth when more messages need to be exchanged.

TESLA/TESLA++/VAST vs. Routing Feature: The verification of a MAC is dependent of the anchor; this makes TESLA and TELSA++ inefficient for routing purposes. Since both the anchor and the message need to be routed, this is problematic in fast topology changes, since the anchor is only broadcasted once. On the other hand, using VAST, one can verify the message signed by the digital signature where the anchor is not present.

TESLA/TESLA++/VAST vs. Topology Change: When the hash chain is calculated and broadcasted to other nodes for a few time in intervals, it means that the set of receivers should not be changed during the usage of hash chain. A new receiver cannot verify the message until next hash chain generation, which is an unacceptable requirement for VANET. VAST works better in these cases.

5.4 Pairing Based Scheme analysis

Pseudonym Generation, Anonymous Signatures vs. Computational Power: Most of these schemes are involving several mathematical operations such as pairing, point multiplications and hash to point. Pairing operation is computationally intensive among them. This makes pairing schemes comparably slow in verification of signatures, which is undesirable for VANET. As mentioned before only revocation lists are possible in these schemes, these also requires heavy weight operations which are comparable to verifying a signature which needs to be performed for each revoked vehicle in the list. This makes revocation a burden in those schemes.

Pseudonym Generation, Anonymous Signatures vs. Storage Capacity: A benefit from having anonymous signatures or pseudonym generation within the vehicle is that storage capacity is much smaller compared to solutions where multiple certificates needs to be stored. Revocation lists on the other hand takes considerably more storage capacity.

Pseudonym Generation, Anonymous Signatures vs. Routing: For routing to be stable it is important for the nodes to distinguish between other nodes. The MAC address needs to be constant for a period of time; this makes it possible to link between different messages when they contain the MAC-address. In anonymous signatures it is therefore still possible to link between messages.
Instead, problems may arise when new MAC addresses need to be set. Compared to having a number of short lived certificates, the MAC address may be a part of the ID. Having the vehicle self generating MAC addresses may lead to collisions when the generated MAC-Addresses are the same.

Pseudonym Generation, Anonymous Signatures vs. Bandwidth Limitations: The messages sent do not need to contain a Certificate but on the other hand the keys and signatures need to be larger for these schemes.

5.5 Verify on Demand Concept Analysis

Verify on Demand relieves computational load on the ITS stations since the number of verification decreases dramatically. This means that it would be possible to communicate with more nodes without any drop caused by computational power. This would also allow the VANET to use processor power for other purposes in the future. A drawback to VoD is that it compels to have a cross layer stack, which is complex and costly to design. Another drawback to VoD can be the implicit effects on Local Dynamic Map or other databases, it may be hard to know if data that seems to be non-safety may have implicit effects on other safety data in the future.

5.6 Bandwidth Throughput

Chart.1 shows a comparison of various solutions to handle VANET scalability issue having Bandwidth as a limitation. The chart values are theoretically calculated to see how the size of security overheads and different sizes of application layered data (100/200 bytes), affects the number of vehicles capable to be handled in the system having 3Mbps bandwidth, the security bit parameters is set to 112 for each solution respectively. The number of vehicles that an approach can handle reduces by increasing the message overheads. It should be mentioned that in creating this chart, only size of security and application overheads are considered and all other factors (e.g. network transport protocols) are neglected. Comparing to ECDSA, ECDSA (IC) is calculated having Implicit Certificate [refer to Appendix C] instead of an Explicit one. This makes it smaller in size of security overhead and therefore it shows an small increase in the number of vehicles. For TESLA/TESLA++ solutions, the hash chain is considered to be 3 units long. This seems to be a reasonable length, making approaching vehicles able to join the communication. For IASS, the accumulated messages are released every 50 ms to not increase the delay considerably.

An estimation of 120 vehicles (as estimated in [26]) in a radius of 300meter (communication range) can be considered in a traffic congestion scenario (e.g. a 6 lane high way. 3 lanes for each direction and 30meter space between vehicles). This assumption is shown by a red line in the chart below showing that RSA and NTRU fail in handling congestion scenarios. Other factors in the system may also make other solution fail as well which are not presented in this chart and kept to be discussed later.

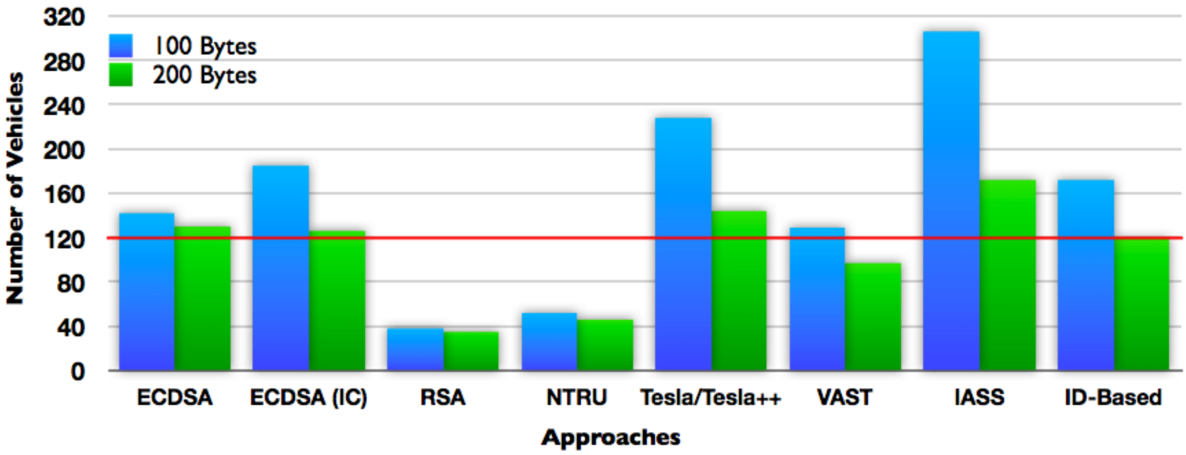
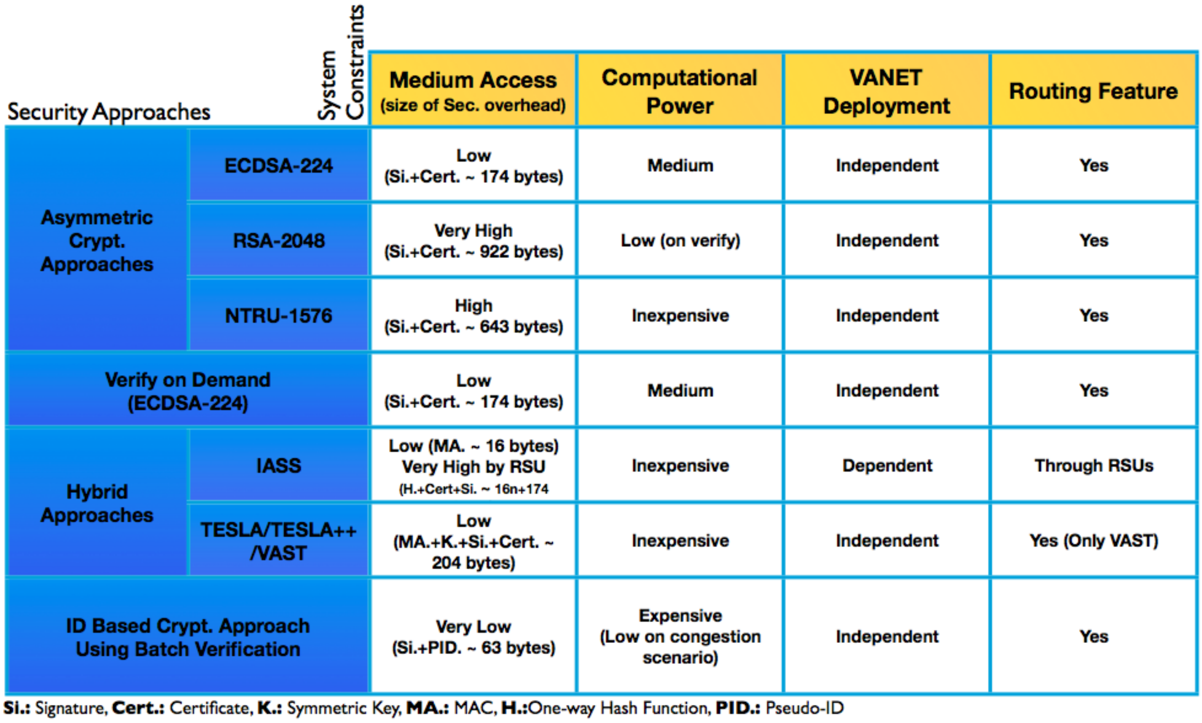


Figure 3.Security Approaches comparison considering bandwidth

5.7 Summary

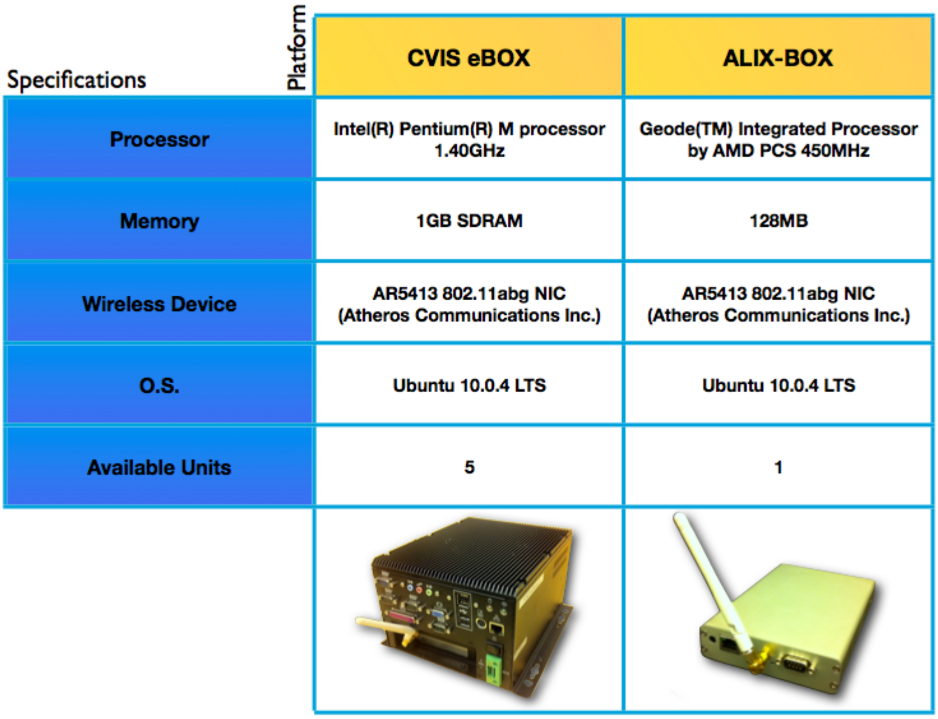
Table.2 shows the comparison of different discussed approaches against system constraints. Timing Constraint is affected by processing time of security operation and End-to-End delay is left out to be tested in the Experiments chapter. Storage limitation constraint is also neglected since it is basically affected by logging policies and privacy considerations (e.g. number of pseudonym short-lived certificates).A routing feature is basically possible where Digital Signatures are involved. In case of IASS, RSU can forward or route a message to next RSUs to be disseminated there as well. A batch verification feature in ID-based cryptography lowers the computational load of processors in congestion scenarios compared to a one-by-one verification.



Security Approaches	System Constraints	Medium Access (size of Sec. overhead)	Computational Power	VANET Deployment	Routing Feature
Asymmetric Crypt. Approaches	ECDSA-224	Low (Si.+Cert. ~ 174 bytes)	Medium	Independent	Yes
	RSA-2048	Very High (Si.+Cert. ~ 922 bytes)	Low (on verify)	Independent	Yes
	NTRU-1576	High (Si.+Cert. ~ 643 bytes)	Inexpensive	Independent	Yes
Verify on Demand (ECDSA-224)		Low (Si.+Cert. ~ 174 bytes)	Medium	Independent	Yes
Hybrid Approaches	IASS	Low (MA. ~ 16 bytes) Very High by RSU (H.+Cert+Si. ~ 16n+174	Inexpensive	Dependent	Through RSUs
	TESLA/TESLA++ /VAST	Low (MA.+K.+Si.+Cert. ~ 204 bytes)	Inexpensive	Independent	Yes (Only VAST)
ID Based Crypt. Approach Using Batch Verification		Very Low (Si.+PID. ~ 63 bytes)	Expensive (Low on congestion scenario)	Independent	Yes

Si.: Signature, **Cert.:** Certificate, **K.:** Symmetric Key, **MA.:** MAC, **H.:**One-way Hash Function, **PID.:** Pseudo-ID

Table 2. Security Approaches comparison based on System Constraints



Platform Specifications	CVIS eBOX	ALIX-BOX
Processor	Intel(R) Pentium(R) M processor 1.40GHz	Geode(TM) Integrated Processor by AMD PCS 450MHz
Memory	1GB SDRAM	128MB
Wireless Device	AR5413 802.11abg NIC (Atheros Communications Inc.)	AR5413 802.11abg NIC (Atheros Communications Inc.)
O.S.	Ubuntu 10.0.4 LTS	Ubuntu 10.0.4 LTS
Available Units	5	1

Table 3. Prototypes Specifications

6 Experiments

6.1 Selected Algorithms

Among different PKI algorithms, ECDSA, NTRU and a Bilinear Pairing Scheme are selected to be discussed in this chapter. ECDSA is recommended by ITS active sections such as IEEE 1609.2 standard, SeVeCOM project and Car-to-Car Communication Consortium. The reason lies in the fact that it produces a relatively small signature, public key and hence certificate size, which directly affects the bandwidth usage of each node while communicating in VANET. NTRU on the other hand, is not as computationally heavy as ECDSA, and is therefore a very popular algorithm to use within embedded systems and low computational devices. On the contrary NTRU has larger keys and signature sizes.

Unfortunately, NTRUSign library is licensed by *Security Innovation* [52]. Therefor it was decided to test RSA instead of NTRUSign, which has larger key, signature, signing time but perform verification nearly as fast as NTRUSign which made it interesting for us to be tested as a counterpart to ECDSA.

Due to existence of pairing and point multiplication operations in each verification process, bilinear pairing is not a fast scheme comparing to ECDSA and RSA unless utilizing Batch Verification. Due to lack of time, we skipped batch verification but we were still interested in BP, since it offers other possibilities for securing VANET.

6.2 Test Platforms

To be more realistic, the implemented schemes was tested on specific hardware, which are equipped with wireless cards capable of simulating 802.11p. Table.3 summarizes their specification.

CVIS eBOX platform introduced in CVIS projects founded by the European Commission was used to implement and test a variety of ITS applications across different European projects. Therefore it is considered a widely accepted and well tested platform which makes it considerable for this thesis. To best of our knowledge, although wide range of projects have been done on eBOX, no project involving VANET security considerations has been tested on it.

ALIX-BOX, a small cheap and Unix-based platform is selected since it resembles the future in-vehicle computing system.

6.3 Selected Security Libraries

OpenSSL [69] and Crypto++ [70] are used to implement ECDSA and RSA, which are both Open-Source and written in C/C++. The purpose of using two different libraries was to test their performance and to eliminate their effect on the final results as much as possible. PBC [71] (Pairing Based Cryptography) library is selected to implement Bilinear Pairing solution, which is an Open-Source from Stanford University.

6.4 Choice of Security Parameters

The different algorithms contains several parameters, these affects both speed and the security level achieved, its therefore necessary to have correct parameters to the algorithm to achieve correct results. 112 bits of security was used, since this is specified in the IEEE standard 1609.2[77].

Based on what Standards for Efficient Cryptography Group (SECG) [59] and National Institute for Standards and Technology (NIST) [72] has specified for Elliptic Curve Cryptography, ECC 224 would have the equivalent strength of a 112bits symmetric cipher which is sufficient to be used until year 2030. SECG recommends using secp224r1 [59] as Elliptic Curve Cryptography domain. Similarly, RSA 2048 provides equivalent security level of 112bits. NIST strongly recommend to choose the size of exponents (e) not smaller than 65537. PSS is also selected as RSA padding scheme. Pairing based cryptography uses two subgroups to have equivalent strength to 112 bits of security, the group bits was set to 224 bits and 2048 bits respectively.

6.5 Test Plans

Our test plans can be categorized into two groups; Algorithm Performance test and System Performance Test, as shown in figure.3.The former is limited to test the ability of the algorithms in Signing and Verifying random data. The purpose is to see which algorithms do the security operations the fastest. The latter is assigned to test the ability of security schemes when different nodes are communicating with each other. Hence, we got access to COSMO project source code given by Volvo Technology Co., which therefore can fulfill our requirement for second test plan. The purpose is to test how much the security schemes and number of nodes involved in communications can affect the End-to-End Delay, CPU Load and Packet Loss Rate.

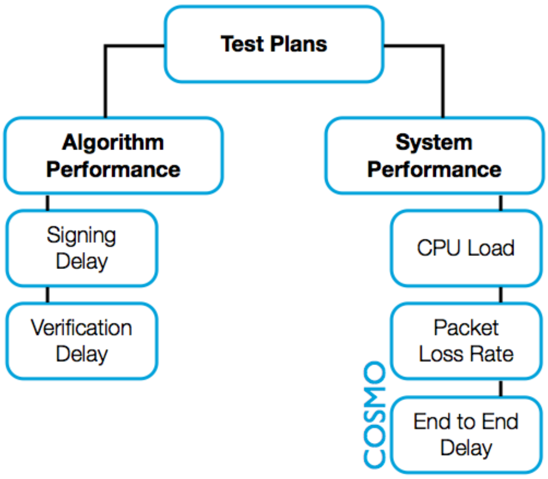
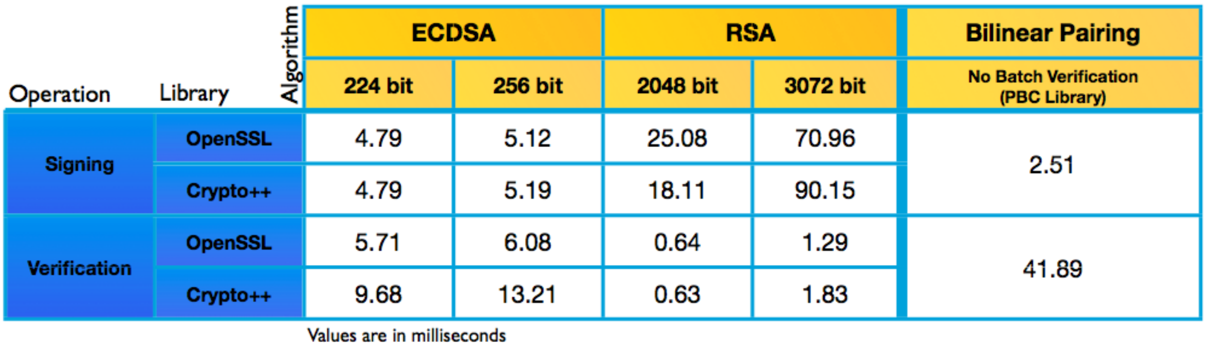


Figure 4.Test Plans

Algorithm Performance Tests

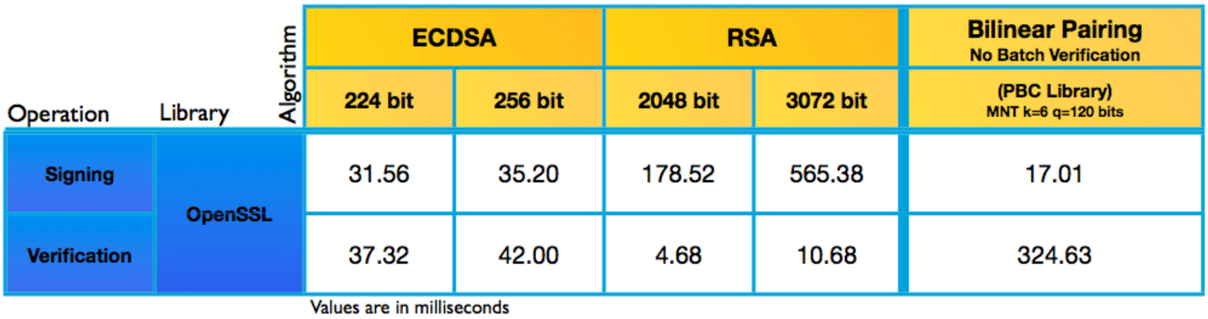
Measuring signing and verification delays of specified security algorithms is the only purpose of this test. The results are presented for both boxes with different libraries in Table.4 and Table.5 respectively. There are different ways to measure the time taken by a specific function in source code. Some of them have high resolution and accuracy, such as hardware-based solutions, but with the cost of difficulties. We chose, the clock function from C library, it gives an accuracy of 15 milliseconds. To increase the accuracy of the values even more, the time was measured while the function was executed within a loop of 1000 cycles. This will make the accuracy high enough.



	Algorithm	ECDSA		RSA		Bilinear Pairing
Operation	Library	224 bit	256 bit	2048 bit	3072 bit	No Batch Verification (PBC Library)
Signing	OpenSSL	4.79	5.12	25.08	70.96	2.51
	Crypto++	4.79	5.19	18.11	90.15	
Verification	OpenSSL	5.71	6.08	0.64	1.29	41.89
	Crypto++	9.68	13.21	0.63	1.83	

Values are in milliseconds

Table.4 CVIS eBOX Performance Test



	Algorithm	ECDSA		RSA		Bilinear Pairing No Batch Verification
Operation	Library	224 bit	256 bit	2048 bit	3072 bit	(PBC Library) MNT k=6 q=120 bits
Signing	OpenSSL	31.56	35.20	178.52	565.38	17.01
Verification		37.32	42.00	4.68	10.68	324.63

Values are in milliseconds

Table.5 ALIX BOX Performance Test

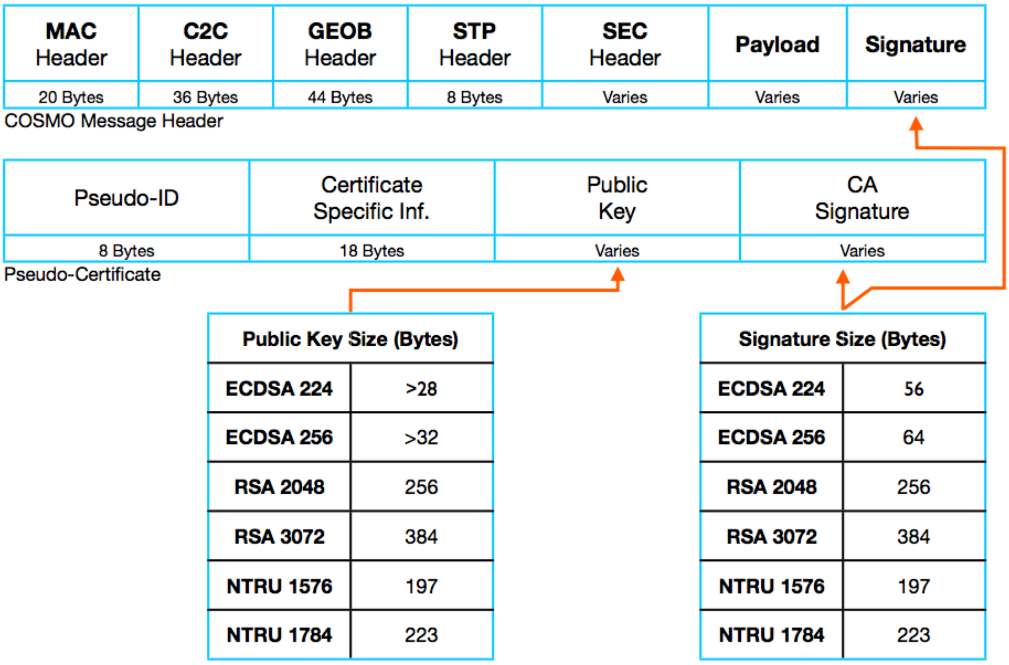
System Performance Test

System performance test intends to test a fully implemented system. Therefore, we got access to the COSMO project given by Volvo Technology. Indeed, COSMO provides us with the communication architecture needed. It sends/receives messages by communicating with both network and facility layers while giving the possibility to configure the message sending frequency and the communication device in use.

Security layer was be added to COSMO project. The functionalities of security layer are generally composed of generating required security related parameters (e.g. curves and keys), to sign and verify the outgoing and incoming messages. The security layer was implemented based on the pre-designed test plans.

Figure.5 shows a certificate including owners pseudo-ID, Public Key, CA signature and an extra field for certificate specific information (such as expiry time if short-lived certificates are in use) is utilized which is identical to C2C-CC certificate structure.

Different algorithms provide different sizes of public key and signature. Therefore the certificate size, message signature and eventually security overhead of each corresponding message between ITS stations would be affected by chosen algorithm. Figure.5 depicts the structure of certificate structure we used in our implementation. It also provides different algorithms' public key and signature sizes. COSMO packet structure is composed of relevant headers intended for message delivery, payload, which carries application layer data and security related fields.



MAC Header	C2C Header	GEOB Header	STP Header	SEC Header	Payload	Signature
20 Bytes	36 Bytes	44 Bytes	8 Bytes	Varies	Varies	Varies

COSMO Message Header

Pseudo-ID	Certificate Specific Inf.	Public Key	CA Signature
8 Bytes	18 Bytes	Varies	Varies

Pseudo-Certificate

Public Key Size (Bytes)	
ECDSA 224	>28
ECDSA 256	>32
RSA 2048	256
RSA 3072	384
NTRU 1576	197
NTRU 1784	223

Signature Size (Bytes)	
ECDSA 224	56
ECDSA 256	64
RSA 2048	256
RSA 3072	384
NTRU 1576	197
NTRU 1784	223

Figure 5.Pseudo Certificate and COSMO Message Structures

CPU Load

As discussed in chapter 5 computational power is one of the limitations of the system that must be considered when heavy weight operations such as security operations are involved. The CPU load where monitored, while signing and verifying. For each added node, CPU load percentages where logged and the average of them are shown in Chart.2. The test where performed for different frequencies.

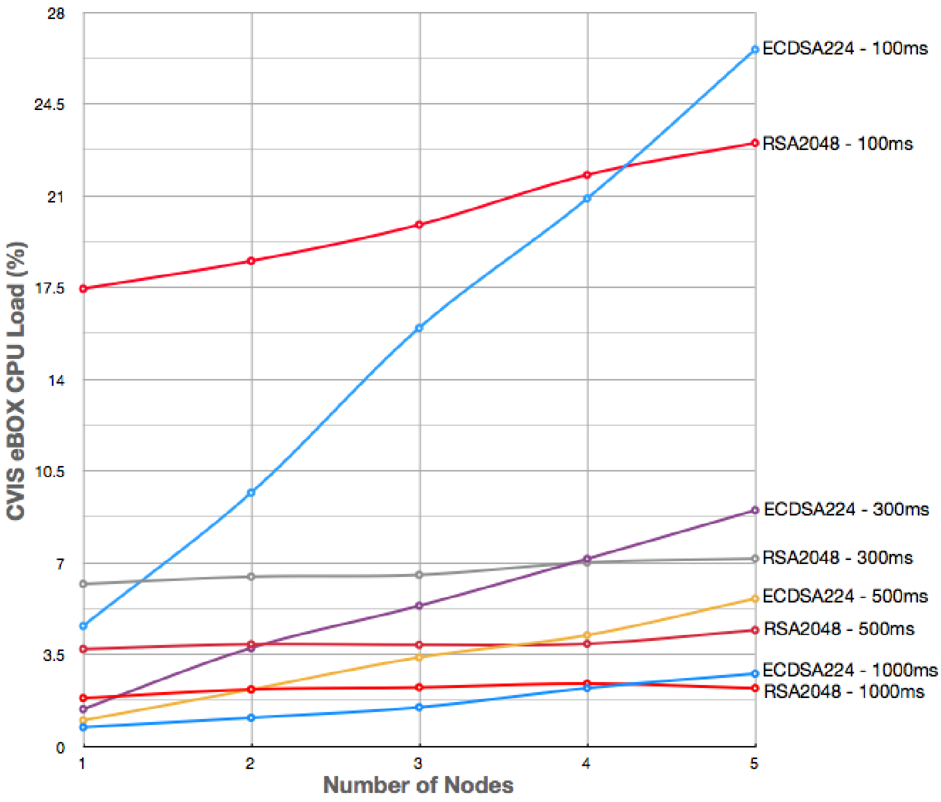


Figure 6.CVIS eBOX CPU Load vs. Number of Nodes

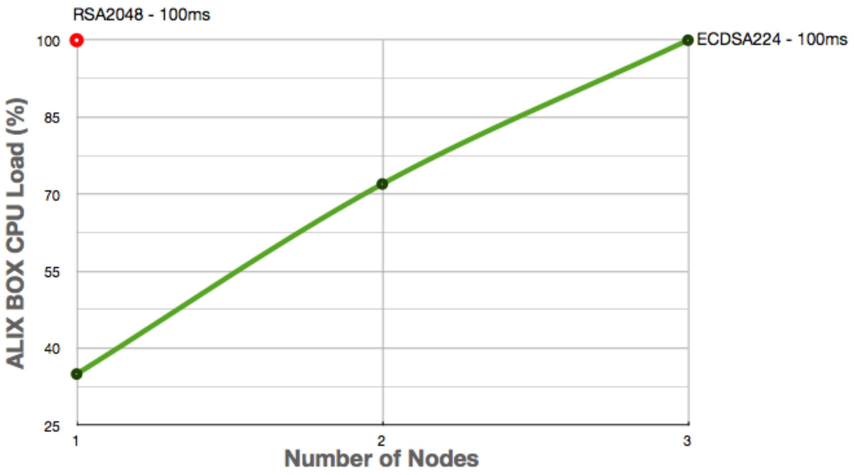


Figure 7.Alix BOX CPU Load vs. Number of Nodes

Packet Loss Rate

Chart.3 shows the Packet Loss Rate (PLR) when the number of nodes scales. To perform this test, we added two counters to the implementation to take track of the number of messages sent and number of messages successfully received. Subtracting these two numbers will show the number of packets that are lost during transmission. The final data is calculated as the total number of loss rates of different nodes divided by total number of received messages from those nodes in percent. The test is performed for sending up to 2000 messages from each node.

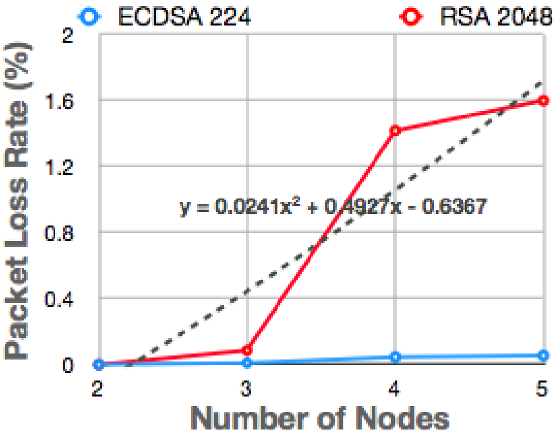


Figure 8.CVIS eBOX Packet Loss Rate vs. Number of Nodes

End-to-End Delay

End-to-End Delay consists of transmission time and time of different operations on messages (such as security operations, encapsulation and de-capsulation of outgoing and incoming messages). The End-to-end delay was calculated by subtracting the received timestamp and sent timestamp, which is included in each packet. The tests where performed by broadcasting 2000 messages per each added node.

To perform this test, the involving nodes must be timely synchronized. Network Time Protocol (NTP) is used for this purpose. In this way, instead of deriving the current time from CPU cycles, the time is repetitively fetched from a server (NTP server). NTP clients try to sync their time through frequent time update requests, which are sent to the NTP server. During this test, we used Ethernet devices provided on boxes and a switch to create a local area network to start NTP service. This should give the accuracy typically less than a millisecond. To avoid the bad results, the test where done several times to reach the smallest offset between server and clients. NTP gives enough accuracy. Chart.4 shows the End-to-End Delay when the number of nodes increases

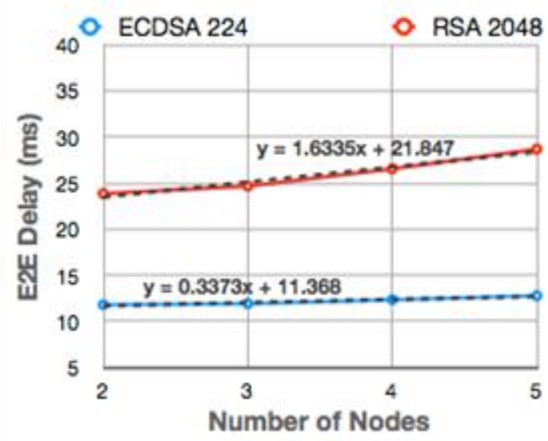


Figure 9.CVIS eBOX End to End Delay vs. Number of Nodes

6.6 Discussion on the Results

Cryptographic Libraries

The results from Table 4 and Table 5 on page 33, shows that the choice of cryptographic libraries has noticeable impact on cryptographic operations.

Table 4 and Table 5 on page 35 show that the choice of cryptographic libraries has an impact on the results.

An observation is that RSA-2048 performs better in the Crypto++ library whereas OpenSSL performs better in other situations. Another observation is that verification time of OpenSSL implementation for the ECDSA algorithm is nearly twice as fast as Crypto++. A conclusion can be drawn that the implementation affects the results and there might even be other libraries existing which are better.

CPU Load, Signing and Verification Time

Verification delay has the most impact on the computational resources, since in a time window of each periodic broadcast, a node will sign one but it must verify multiple received messages from different nodes. This means that an algorithm with smaller verification time will perform better in long run but this is true only if the signing delay is small enough to be able to sign a message in a periodic broadcast time window. For example, Table.4 shows that RSA algorithm outperforms ECDSA in verification time using CVIS eBOXes, even if signing time is larger, since it is still being under a time window of one periodic broadcast (e.g. 100ms). But on the contrary, Table.5 shows that signing time of RSA algorithm on ALIX-BOX are more than 100ms, which is a constraint, this means that it fails to handle the signing operation in time. CVIS eBox shows better results because it possesses a faster processor.

Considering a broadcast time of 100ms and using CVIS eBOX, RSA would give better performance result since it can verify an estimation of 130 messages[6] in a time window which means that 130 nodes can be involved in communication. On the other hand, ECDSA can verify only 16[7] nodes. (These values are based on the fact that a certificate is only verified once when a vehicle is approaching and the number of times a certificate needs to be verified is much less compared to the number of times a signature in a message needs to be verified)

As can be seen in table 4 and 5 the pairing operator is a very heavy weight operator, on the fast CVIS eBOX, the operator would only be able to handle 2 nodes and on Alix Box not even once. It should be mentioned that in this implementation, only one pairing operator was executed, in schemes containing batch verification more pairing operations are needed.

RSA2048 would be the best choice compared to verification time but on the other hand as can be seen in chart1 RSA would not be the optimal choice compared to size.

Packet Loss Rate (PLR)

The size of the packet in transmission, the number of messages sent and an overloaded processor are sources which may cause packets to be lost. Regarding the size of the packet, ECDSA-224 and RSA-2048 have a

[6] (100ms - 18.11ms) / 0.63ms = 129.98

[7] (100ms - 4.79ms) / 5.71ms = 16.67

message size of 1130 and 382 bytes respectively[8]. The difference is caused by the size of certificate and the signature they generate. The chart shows that PLR of RSA algorithm is more likely to occur.

As discussed in previous sections, computational power limits the number of messages that can be verified in recipient sides. If the number of messages goes beyond the CPU load threshold, messages will start to drop. As calculated earlier, ECDSA-224 on CVIS eBOX can process the incoming messages of 16 nodes at most. Messages coming from 17th node will probably drop (this cannot be seen in the chart since it remains below 0.5% for 5 nodes and this is not enough to be near and affected by the threshold).

A bandwidth may also cause an increase in PLR when the number of nodes grows, this happens since bandwidth usage of the nodes increases. This limits a node from sending messages since the medium is busy.

It gets worse, if we consider wireless link congestions and collisions in the air as well. It was noticed during the experiment, that placement of the nodes affected the results and different nodes had a different number of lost messages. Probable causes are reflections and transmission power. This might be the reason why the nodes performed better in the ECDSA than in the RSA tests. Another reason might be that larger packets sizes are more probable to be lost as a result of corruption in the radio link. Still 1.6 is a very low loss rate and can be seen as acceptable. More nodes should have been added to further investigate the progress of packet loss rate. It would be interesting to find the threshold where the messages start to drop because of the limited bandwidth.

E2E Delay

End-to-End Delay depends on several factors within the system, especially the signing time, transmission time verification time, and queuing delays caused by the other messages processed within the system (e.g waiting for the medium to be accessible, or waiting for other messages to be signed/verified).

Chart.4 shows that ECDSA-224 performs better than RSA-2048. An outgoing message should be signed, transmitted and verified as an incoming message in another node.

Larger packet sizes causes a longer waiting time before it can access the medium; this is because of the higher probability that the medium is busy. When the number of nodes increases, the higher the probability get that transmission will appear on the same time, these causes a larger collision avoidance backup time.

Figure.9 shows that RSA seems to grow faster than ECDSA. This implies that the larger packet sizes of RSA have more impact on E2E delay than the verification time in case of ECDSA when the number of nodes increases.

From the results that we discussed in this chapter, it can be concluded that the total number of nodes (N) that can be involved in communication is proportional typically to Security Algorithm (SA), which is used, Bandwidth (Bw), Frequency (Fq) of periodic broadcastings, Size (S) of the messages in transmission and ComputationalPower (CPw). The proportional can be written as follow:

$$\boldsymbol{N} \sim \frac{\mathbf{Bw.CPw.SA}}{\mathbf{Fq.}\boldsymbol{S}}$$

- **Bw:** In our experiment, the bandwidth was set to 3mbps. According to DSRC, the bandwidth could have been in a range of 3-27mbps. Increasing the bandwidth would help to scale the VANET but it is not the only factor that impacts it.
- **CPw:** Adding more computation power would the number of nodes within VANET. An alternative to this is to add a Cryptographic Processor specialized for intensive mathematical operation.
- **SA and S:** A faster Security Algorithm especially in verification would defiantly impact N. For example, NTRUSign algorithm is faster in both signing and verification but in cost of bigger signature and certificate size (comparing to ECDSA. NTRUSign performs better than RSA).

The size of a certificate and signature generated by a security algorithm would affect the total size of the message that should be sent [refer to Appendix E] which eventually affects the number of nodes that can contribute in VANET.

- **Fq:** Decreasing the frequency of periodic broadcast would assist the processor by decreasing the numbers of verification needed to be done and also lower the bandwidth usage. This eventually improves the scalability of VANET. It should be mentioned that decreasing is in cost of decreased safety and should be balanced.

[8] Using COSMO Packet Structure with 100bytes of Application Data

7 Conclusion and Future Work

We reviewed and analyzed different approaches to secure vehicular communication for the purpose of cooperative intelligent transport systems. The approaches studied were from academic and industrial research as well as from various standards. We showed that although PKI-based solutions give best results, they are still far from being stable. The reason lies in the fact that most of them require computationally intensive operations and generate large security overhead which must be overcome by utilizing specialized and faster processors and/or boosting bandwidth or other considerations such as decreasing frequency of periodic broadcasting messages. As discussed in Appendix C, using an Implicit Certificate, which is smaller in size and faster in validation than an explicit certificate, could open up for future possibilities in VANET Security. Therefore, using such certificates is recommended to be studied more in the future in order to see how they can fulfill security requirement and systems constraints of a VANET.

Symmetric solutions generally suffer from delayed authentication, dependency on infrastructure, and extra communication overhead. Although ID-based cryptography as a novel idea brings a lot of potential to security for computer networks, it is mostly too computationally expensive for vehicular applications, which demands real-time authentication. ID-based Batch-Verification based schemes suffer from delayed verification when a signature is found to be false due to the fact that the receiver should redo the batch-verification process over and over to find and discard the one or more false signatures inside the batch.

Privacy and revocation in vehicular ad-hoc networks are two challenging security requirements that are also discussed. Short-lived certificate with Pseudo-ID is a promising approach to manage both of these requirements. The number of Pseudonym short-lived certificates that must be stored in On-Board Units, as well as their consumption frequency and updating strategies, must be studied further.

We discussed and recommended using Cryptographic Processors, which are specialized to calculate cryptographic operations. There are some already introduced processors available, such as CS256-ECC from Crack Semiconductor. There are also similar products from IBM, but they are mostly too expensive to be used directly. This area definitely needs further work both from the industry and academic sides.

8 References

1. European Road Statistics 2010, European Union Road Federation.
2. eSafety Initiatives, http://www.esafetysupport.org/en/esafety_activities, Accessible at Jun 7th 2011.
3. CALM Concept, http://www.isotc204wg16.org/concept, Accessible at Jun 7th 2011.
4. Communications, Air-interface, Long and Medium range, http://en.wikipedia.org/wiki/Communications,_Air-interface,_Long_and_Medium_range, Accessible at Jun 7th 2011.
5. ETSI TS 302 665 V1.1.1 Final Draft, Intelligent Transport System (ITS); Communication Architecture, July 2010.
6. C. Wewetzer, M. Caliskan, K. Meier, A. Luebke, "Experimental Evaluation of UMTS and Wireless LAN for Inter-Vehicle Communication", Volkswagen Group, Wolfsburg, June 2007.
7. D. Jiang and L. Delgrossi, IEEE 802.11p, "Towards an International Standard for Wireless Access in Vehicular Environments", Mercedes-Benz Research & Development North America Inc., 2008.
8. ETSI TS 102 637-2 V1.1.1, "Technical Specification, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service", Apr 2010.
9. ETSI TS 102 637-3 V1.1.1, "Technical Specification, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service", Sep 2010.
10. A. Yuen, C. Brown, C. Zott, A. Hiller, F. Ahlers, K. Wevers, S. Dreher , T. Schendzielorz, C. Bartels, Z. Papp and B. Netten, "SAFESPOT Innovative Technologies, Local Dynamic Maps Specifications", issued in 2008.
11. ETSI TR 102 638 V1.1.1, "Technical Report, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions", Jun 2009.
12. About eSafety Support, http://www.esafetysupport.org/en/esafety_activities/about_esafety_support/index.html, Accessible at Jun 7th 2011.
13. eSafety Forum, http://www.icarsupport.org/esafety-forum, Accessible at Jun 7th 2011.
14. COMeSaftey D31 European ITS, Communication Architecture Overall Framework Proof of Concept Implementation, Version 2.0, Actual submission date 05.03.2009.
15. COMeSaftey, http://www.comesafety.org, Accessible at Jun 7th 2011.
16. B. Weyl, "Secure Vehicular Communication: Results and Challenges Ahead", Car2Car Communication Consortium C2C-CC, February 2008.
17. "Vehicle Safety Communications – Applications VSC-A First Annual Report", Submitted to the Intelligent Transportation Systems (ITS), Joint Program Office (JPO) of the Research and Innovative Technology Administration (RITA) and the National Highway Traffic Safety Administration (NHTSA), Sep 2008.
18. S. J. Murdoch and G. Danezis, "Low-Cost Traffic Analysis of Tor", IEEE Symposium on Security and Privacy (2005), pp. 183–195.
19. S. Lo, D. D. Lorenzo, P. Enge, P. Bradley, D. Akos, "Signal Authentication, A Secure Civil GNSS for Today", Inside GNSS, Sept/Oct 2009, pp.30-39.
20. M. Raya, J. P. Hubaux, "Securing Vehicular Ad Hoc Networks", J. Computer Security, vol. 15, no. 1, pp.39–68, 2007.
21. J.T. Isaac, S. Zeadally, J.S. Camara, "Security attacks and solutions for vehicular ad hoc networks", IET Commun. -- 30 April 2010 -- Volume 4, Issue 7, pp.894–903.
22. PRE-DRIVE C2X, Deliverable D1.3, "Security Architecture", Version 1.0, Dissemination level PP, 2009.
23. ETSI TR 102 893 V1.1.1, "Technical Report, Intelligent Transport Systems (ITS), Security, Threat, Vulnerability and Risk Analysis (TVRA)", Mar 2010.
24. Y. Hu, A. Perrig and D. B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, 2006: pp.370-380.
25. H. Weerasinghe and H. Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks:Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications, vol.2, no. 3, pp. 39–54, Jul. 2008.
26. M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in Proceeding of 3rd ACM Workshop Security Ad Hoc Sensor Networks, Alexandria, VA, Nov. 2005, pp. 11–21.
27. ETSI TS 102 731 V1.1.1, "Technical Specification, Intelligent Transport Systems (ITS), Security, Security Services and Architecture", Sep 2010.

28. *Certicom Research, "SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)", V. 0.91, Working Draft, Oct 2008.*

29. *R. Kroh, A. Kung, F. Kargl, "VANETS Security Requirements Final Version", SeVeCOM, Secure Vehicle Communication, Deliverable 1.1, Version 2.0, Nov 2006.*

30. *C. Han, M. Dianati, R. Tafazolli, and R. Kernchen , "Throughput Analysis of the IEEE 802.11p Enhanced Distributed Channel Access Function in Vehicular Environment". In Proceedings of VTC Fall 2010. pp.1-5.*

31. *K.S. Bilstrup, E. Uhlemann, E.G. Strom, "Scalability Issues of the MAC Methods STDMA and CSMA of IEEE 802.11p When Used in VANETs", In Proceeding of the ICC'10 Workshop on Vehicular Connectivity, Cape Town, South Africa, 23-27 May 2010.*

32. *T. Kim, S. Jung, and S. Lee, "CMMP: Clustering-Based Multi-channel MAC Protocol in VANET", In Proceeding of the Second International Conference on Computer and Electrical Engineering, 2009, pp.380-383, 2009.*

33. *G. Samara, W. A.H. A. Alsalihy, S. Ramadass, "Efficient Certificate Management in VANET", 2nd International Conference on Future Computer and Communication (ICFCC), pp.750 - 754, 2010.*

34. *M. Raya, P. Papadimitratos, and J-P. Hubaux, "Securing Vehicular Networks," IEEE Wireless Communications, Volume 13, Issue 5, October 2006, Penang, Malaysia.*

35. *C. Zhang, R. Lu, X. Lin, P.H. Ho, X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks", The 27thIEEE Conference on Computer Communications, pp. 246-250, April 2008.*

36. *D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", In Proceedings of Crypto, LNCS, Vol. 2139, pp. 213-229, 2001.*

37. *R. Lu, X Li.n, H. Zhu, P.H. Ho, X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", In Proceedings of INFOCOM'2008. pp.1229-1237, 2008.*

38. *J. Sun and Y. Fang, "A defense technique against misbehavior in VANETs based on threshold authentication", In Proceedings of IEEE MILCOM 2008, pp.1-7, Nov. 2008.*

39. *L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications", IEEE Transactions on Vehicular Technology, vol. 59, no. 4, pp. 1606-1617, may 2010.*

40. *X. Lin, X. Sun, P.-H. Ho and X. Shen. "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, 2007.*

41. *C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications", In Proceedings of IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, 2008.*

42. *D. R. Stingson, "Cryptography: Theory and Practice, 3rd ed. Boca Raton", CRC Press, 2005.*

43. *A. Perrig, R. Canetti, J. D. Tygar, D. Song, "The TESLA Broadcast Authentication Protocol", UC Berkeley and IBM Research.*

44. *A. Studer, F. Bai, B. Bellur, A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication", J. Commun. Net., vol. 11, no. 6, pp. 894–901, Dec. 2009.*

45. *H. Krishnan and A. Weimerskirch, "Verify-on-Demand" - A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication, SAE Technical Paper, 2011.*

46. *A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services", In Proceedings of Pervasive Computer and Communications Security (PerSec), p.127 , 2004.*

47. *A Kung, "Security Architecture and Mechanisms for V2V/V2I", SeVeCom, Secure Vehicle Communication, Deliverable 2.1, Version 3.0, 2008.*

48. *P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, "Secure vehicular communications: design and architecture", IEEE Communications Magazine, vol. 46, no. 11, pp.100-109, November 2008.*

49. *P. Papadimitratos, G. Mezzour, J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems", In Proceedings of Vehicular Ad Hoc Networks, pp.86-87, 2008.*

50. *K. P. Laberteaux, J. J. Haas, Y.C. Hu. "Security certificate revocation list distribution for VANET". In Proceedings of Vehicular Ad Hoc Networks. pp.88-89, 2008.*

51. *Preliminary Conclusions of the V2V Security Network Simulations in the VSC-A project, IEEE P1609 Meeting, June 2009.*

52. *Security Innovation, http://www.securityinnovation.com, Accessible at Jun 7th 2011.*

53. *J. Korhonen and Y. Wang, "Effect of packet size on loss rate and delay in wireless links", Wireless Communications and Networking Conference, vol.3, , pp.1608-1613, Mar 2005.*

54. *A. Menezes, "An Introduction to Pairing-Based Cryptography", The University of Waterloo, Fall 2008.*

55. *N. Estibals , "Compact hardware for computing the Tate pairing over 128-bit-security supersingular curves", Pairing 2010 -- 4th International Conference on Pairing-Based Cryptography 648, pp.397-416. 2010.*

56. *A. Joux. "A one round protocol for tripartitie Diffie-Hellman", In Proceedings of Algorithmic Number Theory Symposium -ANTS IV, volume 1838 of Lecture Notes in Computer Science, pp.385-394, 2000.*

57. *P. Agrawal and R. K. Ghosh, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", In Proceedings of ICUIMC'2008. pp.310-314.*

58. *C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks", in Proceedings of IEEE International Conference on Communications, Beijing, China, May 19-23, 2008.*

59. *Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters", V. 1.0, Sep 2000.*

60. *Vehicle Safety Communications Project Task 3 Final Report. Technical report, The CAMP Vehicle Safety Communications Consortium, Mar 2005. Sponsored by U.S. Department of Transportation (USDOT). Available through National Technical Information Service, Springfield, Virginia 22161.*

61. *W. Hsin-Te, W. Li, S. Tung-Shih, W. Hsiehz, "A Novel RSU-Based Message Authentication Scheme for VANET", Fifth International Conference on Systems and Networks Communications 2010, pp. 111-116.*

62. *A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", Advances in Cryptology in Proceedings of CRYPTO 84, Lecture Notes in Computer Science, pp. 47-53, 1984.*

63. *D. Boneh, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing", Journal of Cryptology 17, pp. 297–319.*

64. *Y. Zheng, "Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)", Advances in Cryptology, CRYPTO'97, pp.165-179, 1997.*

65. *J.l. Huang, L.Y. Yeh and H.Y. Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, pp. 248-262, 2011.*

66. *C. P. Pfleeger, S. L. Pfleeger, W. H.Ware, "Security in Computing", 4th Ed. PRENTICE HALL PTR. 9780132390774, 2006*.

67. *Wolfram Alpha, Germany Vehicles, http://www.wolframalpha.com/input/?i=germany+vehicles , Accessible at Jun 13th 2011.*

68. *R. Baskerville and M. D.Myers, "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice—Forward", MIS Quarterly Vol. 28 No. 3, pp. 329-335, Sep 2004.*

69. *OpenSSL Library Website, http://www.openssl.org/ , Accessible at Jun 13th 2011.*

70. *Crypto++ Library Website, http://www.cryptopp.com/ , Accessible at Jun 13th 2011.*

71. *PBC Library Website, http://crypto.stanford.edu/pbc/ , Accessible at Jun 13th 2011.*

72. *National Institute of Standards and Technology (NIST), FIPS Publication 186-3: Digital Signature Standard, November 2008.*

73. *L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in IEEE Wireless Communications and Networking Conference (WCNC 2005), New Orleans, LA, March 2005.*

74. *Jiun-Long Huan,; Lo-Yao Yeh, Huang-Yu Chien; "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Network" in, IEEE Transactions on Vehicular Technology, Volume 60, Issue:1, 2011 Page(s) 248-262.*

75. Z. Li, Z Wang and C.Chigan, "security of vehicular adhoc Netowks in intelligent transport systems" in wireless Technlogies for intelligent Transportation System," Nova Science Publishers, 2009(in press)

76. *PP Papadimitratos, G Mezzour, JP, "Certificate revocation list distribution in vehicular communication systems", Proccedings of the fifth ACM workshop on Vehicular Networks, 2008*

77. *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments, IEEE Std. 1609.2-2006,2006.*

9 Appendices

Appendix A - Computer Security Terms

Hash Functions

The cryptographic hash function takes an arbitrary length of data and produces a fixed size data block as the output, which is called message digest. The hash function is a one-way function meaning that it is mathematically (nearly) impossible to derive original data from its digest. Same data input to the same hash function always produce the same output. To be considered as secure one, a hash function should create the message digest using all bits of the original message. Hash function is mostly used to see if the messages are changed in transition or not. Even if a bit of original message changes in transition (e.g. modification attack), message digest would change drastically. At recipient side, message digest would be calculated again from original message to be compared with the digest appended to the message by sender. If they differ then received message is different from original message sent.

It should be mentioned that hash function cannot protect message from modification standalone since an attacker can change the message and its unprotected digest in transition to fool the recipient about the trustfulness of the message. In computer security, message should be protected using a digital signature. SHA-1, SHA-256 and MD5 are the most well known hash functions. A hash function can also be used in combinations with symmetric keys, so called Message Authentication Code (MAC). In the context of ID-based cryptography, a different kind of hash function, so called Map To Point hash, is introduced which is used to map a stream of bits to a point on a curve (refer to ID-based Cryptography).

Digital Signatures

As mentioned before public key cryptography can be utilized to authenticate senders or recipients. The reason lay in the fact that private key is kept secret for example in a smart card chip or in a trusted platform module (see TPM). A message signed (encrypted) by private key would enable the recipients to verify the authenticity of the sender.

Typically, to create a digital signature, the message is given to a hash function to produce the message digest. The message digest is then encrypted with the private key of the sender (called signing) and then concatenated to the original message. At recipient side, receiver validates the sender by decrypting the signature sent by the message using the sender's public key. Derived message digest would then be compared with calculate hash of the message. If both digests were the same, it would then be concluded that the sender is authenticated and the message is not altered.

Explicit Certificates and Certificate Authority

A certificate is a document that binds a public key to an identity. Certificates can be forged by an adversary impersonating a user in the system. Therefor, certificates must be verified by a trusted third party or so called Certificate Authority (CA) [66]. Having a certificate singed by CA, allows the users of the system to trust that a specific public key belongs to the claiming user.

CA signature is the hash of the member's certificate encrypted by CA's private key, which then will be appended as another field into the member's certificate. Having CA certificate, one can check the validity of a member certificate.

Appendix B - Bilinear Pairing

Pairing is a mathematical function that maps $\boldsymbol{Z}^* \times \boldsymbol{Z}^*$ to $\boldsymbol{Z}^*$which means that it takes two integers from two non-negative groups (can be the same group) and map them into a third group. In 1993, pairing used to break elliptic curve discrete logarithm problem (ECDLP) [55]. In 2000, A. Joux introduced one round key Diffie-Hellman key agreement protocol for three parties [56].

D. Boneh and M. Franklin employed a form of Pairing called Bilinear Pairing, $\boldsymbol{e}$, which map from an additive cyclic group $\boldsymbol{G_1}$ with $\boldsymbol{P}$ as the element to a multiplicative cyclic group $\boldsymbol{G_2}$ with the same prime order and $\boldsymbol{Q}$ as the element where DDH problem is easy but CDH problem is difficult to trace [54].

A Bilinear Pairing is a map $\boldsymbol{e}: \boldsymbol{G_1} \times \boldsymbol{G_2} \longrightarrow \boldsymbol{G_2}$ when it satisfies the conditions below:
1.Bilinearity:$\forall \boldsymbol{P}, \boldsymbol{Q} \in \boldsymbol{G} \ \boldsymbol{and} \ \forall \boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{Z}; \boldsymbol{e}: (\boldsymbol{aP}, \boldsymbol{bQ}) = \boldsymbol{e}: (\boldsymbol{aP}, \boldsymbol{bQ})^{\boldsymbol{ab}}$.
2. Non-degeneracy: $\boldsymbol{e}: (\boldsymbol{P}, \boldsymbol{P})$ is not equal to$\boldsymbol{1}$.
3. Computability: There is an efficient algorithm to compute $\boldsymbol{e}: (\boldsymbol{P}, \boldsymbol{Q})$.

If a Bilinear pair satisfies these conditions it would be called Admissible Bilinear Map. Boneh and Franklin used Admissible Bilinear Pairing to propose a solution to ID-Based Cryptography as below:

1. Private Key Generator (PKG) which is assumed as a trusted authority chooses $\boldsymbol{G_1}$ and $\boldsymbol{G_2}$ and a secret random $\boldsymbol{s} \in \boldsymbol{Z_q^*}$,called private master key (or master key), and a public key $\boldsymbol{sP}$ and two publicly available hash to point functions as follow: $\boldsymbol{H_1}: [\boldsymbol{0}, \boldsymbol{1}]^* \longrightarrow \ \boldsymbol{G_1}$,$\boldsymbol{H_2}: \boldsymbol{G_2} \longrightarrow [\boldsymbol{0}, \boldsymbol{1}]^{\boldsymbol{n}}$.

2. For $\boldsymbol{Bob}$ with identity of $\boldsymbol{ID_{Bob}}$, PKG computes $\longrightarrow \boldsymbol{H_1}(\boldsymbol{ID_{Bob}})$ as his public key and $\longrightarrow \boldsymbol{sH_1}(\boldsymbol{ID_{Bob}})$ as his private key which are given to him.

3. To create cipher text $\boldsymbol{c}$, $\boldsymbol{Alice}$ encrypts the given message $\boldsymbol{m}$ by Bob's public key. She chooses a random $\mathbf{r} \in \boldsymbol{Z_q^*}$ and computes $\longrightarrow \boldsymbol{J} = \boldsymbol{e}: (\boldsymbol{H_1}(\boldsymbol{ID_{Bob}}), \boldsymbol{sP})$ which would map Bob's and PKG's public key to $\boldsymbol{G_2}$ and then computes $\boldsymbol{c} = (\boldsymbol{rP}, \boldsymbol{m} \oplus \boldsymbol{H_2}(\boldsymbol{J^r})$.

4. Upon receiving the cipher text $\longrightarrow \boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$, Bob can retrieve the plain text using his private key, $\boldsymbol{sH_1}(\boldsymbol{ID_{Bob}})$ and calculating following equation:

$$\boldsymbol{v} \oplus \boldsymbol{H_2}(\boldsymbol{e}(\boldsymbol{sH_1}(\boldsymbol{ID_{Bob}}), \boldsymbol{u}) =$$
$$\boldsymbol{m} \oplus \boldsymbol{H_2}(\boldsymbol{J^r}) \oplus \boldsymbol{H_2}(\boldsymbol{e}(\boldsymbol{sH_1}(\boldsymbol{ID_{Bob}}), \boldsymbol{rP}) =$$
$$\boldsymbol{m} \oplus \boldsymbol{H_2}(\boldsymbol{e}: (\boldsymbol{H_1}(\boldsymbol{ID_{Bob}}), \boldsymbol{sP})^{\boldsymbol{r}} \oplus \boldsymbol{H_2}\big(\boldsymbol{e}(\boldsymbol{sH_1}(\boldsymbol{ID_{Bob}}), \boldsymbol{rP})\big) =$$
$$\boldsymbol{m} \oplus \boldsymbol{H_2}(\boldsymbol{e}: (\boldsymbol{H_1}(\boldsymbol{sID_{Bob}}), \boldsymbol{rP}) \oplus \boldsymbol{H_2}\big(\boldsymbol{e}(\boldsymbol{sH_1}(\boldsymbol{ID_{Bob}}), \boldsymbol{rP})\big) = \boldsymbol{m}$$

Appendix C - Implicit Certificate

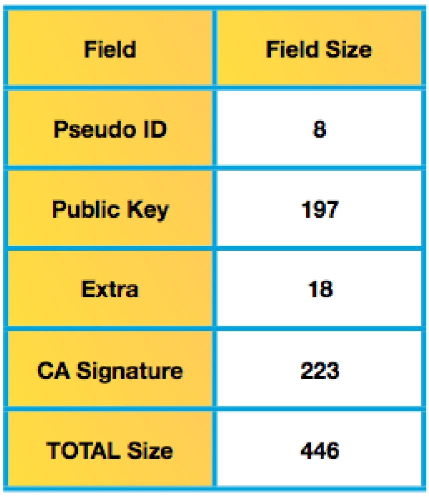
Implicit Certificate is a kind of certificate which does not directly include the public key. Instead, public key would be calculated from the information inside the certificate. Public key of the CA is used during the user's public key extraction. Therefore, if the calculation gives the result equals to what is presented in the certificate, then it can be assumed that certificate is valid and is bounded to a valid identity. Comparing to the traditional form of certificate, the public key is explicitly included in the certificate and recipient would not need to calculate anything except in form of verifying the CA signature to see if the public key and Identity of the owner are bounded to each other and therefore are trustful.

Elliptic Curve Qu-Vanstone (ECQV) is one form of implicit certificates, which utilizes the elliptic curves characteristics to perform the idea. Verifying an ECQV implicit certificate is comparably faster than traditional ECDSA certificates (introduced by 1609.2 or short-lived certificates). They are also comparably smaller due to the fact that they only include public key construction data instead of a public key or a CA signature. In Theory the size of construction Data is equal to size of a point on elliptic curve [28].

This seems very desirable to be used in Vehicular Ad-hoc Networks. In our thesis, since one of the purposes was to test and evaluate current security approaches, we decided on expressing explicit certificates (such as the ones introduced in 1609.2 and C2C-CC).

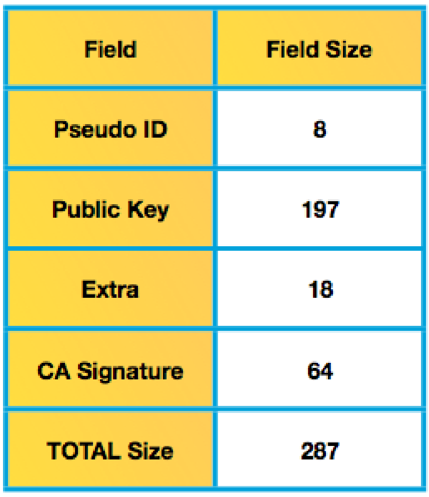
Appendix D - NTRU Certificate Size

NTRU-1576 certificate is 446bytes including a 223bytes of CA signature size which is signed by a higher level security or NTRU-1784. This size can be decreased to 287bytes by using ECDSA-256 as CA signature, which possesses the same security level as NTRU-1784.



Field	Field Size
Pseudo ID	8
Public Key	197
Extra	18
CA Signature	223
TOTAL Size	446

Table6. NTRU Cert. NTRU-1784 CA Signature



Field	Field Size
Pseudo ID	8
Public Key	197
Extra	18
CA Signature	64
TOTAL Size	287

Table7. NTRU Cert. ECDSA-256 CA Signature