Performance Analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET)

Abdul Kalam Kunnel Aboobaker

Technical Report
RHUL–MA–2010–02
31st March 2010

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

Performance Analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET)

Abdul Kalam Kunnel Aboobaker

Student Number: 100542563

Supervisor: Dr. Stephen Wolthusen

Submitted as a part of the requirements for the award of MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature: Date: 02-09-2009

Contents

List of Figures

List of Tables

Abbreviations

AU	Application Unit
BP	Baseline Pseudonym
C2C-CC	CAR 2 CAR Communication Consortium
CA	Certification Authority
CALM	Continuous Communications Air Interface for Long and Medium Range
CAMP	Crash Avoidance Metrics Partnership
CICAS	Cooperative Intersection Collision Avoidance System
COMeSafety	Communication for eSafety
CRL	Certificate Revocation List
DoS	Denial of Service
DOT	Department of Transportation
DRP	Distributed Revocation Protocol
DSRC	Dedicated Short Range Communication
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ELP	Electronic License Plate
ETC	Electronic Toll Collection
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GPRS	General Packet Radio Service

GPS	Global Positioning System
GS	Group Signature
GSM	Global System for Mobile Communications
GTA	Governmental Transportation Authority
HS	Hybrid Signature
HSDPA	High-Speed Downlink Packet Access
HSM	Hardware Security Module
HT	Hot Spots
I2V	Infrastructure to Vehicle
IEEE	Institute of Electrical and Electronics Engineers
ISO	Intergnational Organisation for Standardisation
ITS	Intelligent Transportation Systems
LTI	Long Term Identity
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
OBU	On Board Unit
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RCCRL	Revocation protocol using Compressed Certificate Revocation Lists
RSU	Road Side Unit
RTPD	Revocation protocol of the Tamper-proof Device
SEVECOM	Secure Vehicle Communication
STI	Short Term Identity
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TPM	Trusted Platform Module

TRH	Tamper Resistant Hardware
TTL	Time to Live
UMTS	Universal Mobile Telecommunications System
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Ad Hoc Network
VC	Vehicular Communication
VII	Vehicle Infrastructure Integration
VIIC	Vehicle Infrastructure Integration Consortium
WiMax	Worldwide Interoperability for Microwave Access

Acknowledgement

Sincere thanks to Dr. Stephen Wolthusen, my project supervisor, for his exceptional guidance and support. His feedback was most valuable for the completion of this work.

Special thanks to my wife Sapna, for her help with the thesis, and for her unwavering support to me and our family during my M.Sc. This work is dedicated to her.

Abstract

Traditionally traffic safety was addressed by traffic awareness and passive safety measures like solid chassis, seat belts, air bags etc. With the recent breakthroughs in the domain of mobile ad hoc networks, the concept of vehicular ad hoc networks (VANET) was realised. Safety messaging is the most important aspect of VANETs, where the passive safety (accident readiness) in vehicles was reinforced with the idea of active safety (accident prevention). In safety messaging vehicles will message each other over wireless media, updating each other on traffic conditions and hazards. Security is an important aspect of safety messaging, that aims to prevent participants spreading wrong information in the network that are likely to cause mishaps.

Equally important is the fact that secure communication protocols should satisfy the communication constraints of VANETs. VANETs are delay intolerant. Features like high speeds, large network size, constant mobility etc. induce certain limitations in the way messaging can be carried out in VANETs. This thesis studies the impact of total message size on VANET messaging system performance, and conducts an analysis of secure communication protocols to measure how they perform in a VANET messaging system.

1 Introduction

1.1 Motivation

Traffic safety is a major challenge recognised by the major players in the automotive industry and by many governments. According to [31], in 1999 alone 450,000 road accidents were reported in Germany . During the same year, Europe reported three times this number of accidents with fatalities of 42,000. Similar situations exist in other parts of the world like United States [84]. More health care money is spent treating crash victims than any other cause of illness [40]. Traffic delays continue to increase, wasting many hours for peak time travellers. This has prompted the launch of various research projects [65] around the world to primarily come up with solutions addressing the issues of traffic safety and efficiency. Apart from traffic safety and efficiency, features like internet access, entertainment, payment services and information updates into can be integrated into vehicles to improve passenger comfort comfort.

Traffic incidents are often a result of the driver's inability to assess quickly and correctly the driving situations. Normally a driver, has incomplete information about road conditions, speed and location of vehicles around them, and is forced to make decisions like breaking and lane changing without the benefit of whole data. Real time communication between vehicles or between vehicles and road-side infrastructure can improve traffic safety and efficiency [84]. For example, if a vehicle needs to slow down due to an accident ahead, it will broadcast warning messages to neighbouring vehicles. The vehicles behind it will thus be warned before they actually see the accident, helping the drivers react faster, thereby avoiding rear ending of vehicles. In another scenario, if vehicles can transmit traffic congestion information to other vehicles in its range, it can help other vehicles receiving the information to chose alternate routes and avoid traffic congestion.

Vehicular Ad Hoc Networks (VANETs), an extension of mobile ad hoc networks (MANET) [43], were developed with a view to enable real-time communication between mobile nodes (either vehicles or road side infrastructure) over wireless links, primarily with a view to enable traffic safety and efficiency. The communication between nodes in a VANET face many unique challenges [80]. This is especially true for safety-critical applications like collision avoidance, pre-crash sensing, lane change etc [55]. Factors like high

vehicle speeds, low signal latencies, varying topology, total message size, traffic density etc induce challenges that makes conventional wireless technologies and protocols unsuitable for VANETs [9, 55].

Apart from the performance challenges, there are security issues unique to VANETs like authenticating message sender, verifying validity of message data (like vehicle position), providing node privacy with non-repudiation, certificate revocation, availability etc. All these performance and security requirements contribute to make VANET safety applications challenging unlike other wireless applications.

1.2 Purpose of Thesis

Security is an important aspect of safety communications in VANET. Since safety applications also have challenging performance requirements, it is essential that the secure communication protocols also meet the performance requirements. The scope of this work is limited to VANET applications that are safety-critical (2.2.1) and that involve direct vehicle to vehicle (V2V) communications. In this thesis, safety-critical applications are first defined, and an evaluation of secure communication protocols will is performed to see how well they meet the security and performance requirements demanded by safety-critical applications.

In a safety-critical application, the total message size is determined by message payload and cryptographic overhead. The performance evaluation of authentication protocols involves analysing the impact of total message size (and hence cryptographic overhead) and messaging rates on message latency, channel throughput, and message processing delay, and its implications on safety-critical applications and authentication protocols. Also it is investigated if the authentication protocols address the security requirements (authentication, privacy and auditability) of safety-critical applications.

1.3 Content Outline

Chapter 1 explains the motivation behind the thesis topic, as well as the purpose of this thesis. Also, outlined are the contents of different chapters that forms the thesis. Initial part of Chapter 2 does a brief review of MANETs and the latter part specifically dwells on the applications, characteristics, and technologies associated with VANETs. In chapter 3, application characteristics of VANET applications are studied and safety-critical V2V applications are identified and listed. Chapter 4 discusses attacks on VANETs, and identifies and lists the security requirements associated with applications listed in

Chapter 3. Moreover, the performance requirements for the applications listed are also identified and laid down in Chapter 4.

In Chapter 5, the security architecture and its components, for listed applications, are discussed in detail. A security architecture consists of the different elements that are required to sustain a secure functioning of VANET applications. In Chapter 6, authentication protocols are identified that are applicable for applications identified in Chapter 3. Then, an evaluation is performed where the protocol computation overheads are calculated, cryptographic features are analysed and the impact of application message size on message delay and throughput are studied. The impact of messaging rate on the time available for processing each message is also analysed. Chapter 7 gives concluding remarks on protocol analysis and associated findings and gives further comments on the areas that are still open.

2 Background

The primary objective of Vehicular Ad Hoc Networks (VANETs) is to provide traffic safety and efficiency. Since VANETs are an extension of Mobile Ad Hoc Networks (MANETs), a discussion of MANETs is essential to understand VANETs. This chapter gives an introduction to MANETs and VANETs, their characteristics, applications and complexities.

2.1 Mobile Ad Hoc Networks (MANETs)

With the proliferation of mobile devices (cell phones, personal digital assistants (PDA), laptops, and other handheld digital devices), and the exponential growth in the wireless sector in the past decade, there is a revolutionary change in the way information is being handled [21]. Users carry mobile devices that run applications and provide network services, among which data services are the most demanded by users. Currently most of these connections between mobile devices are infrastructure based [21, 38]. For example, two or more laptops communicate with each other using a wireless access point; cell phones are connected via cell phone towers.

Setting up infrastructure for mobile device communication is potentially costly. Users will also face instances where the infrastructure required for desired communication is simply not available. Additionally many of the mobile devices in use like laptops and PDAs have only short range wireless capability. This has prompted the development of an alternative way for mobile device communication in which each mobile device (node) communicates with each other over wireless without the support of an infrastructure, forming a mobile ad hoc network (MANET) [38, 91].

2.1.1 Characteristics and Complexities of MANET

In a MANET, nodes operate in a peer to peer mode independent of any infrastructure or a centralised administration. To communicate with nodes beyond the range, intermediate nodes forward messages to destination node over multiple hops. Each node acts as an independent router and generates independent data. Fault detection and network

management becomes distributed and hence more difficult. Nodes in MANETs are mobile causing the network topology to change frequently and unpredictably. This causes nodes to move in and out of wireless range resulting in node unavailability, changes in packet routes, and possibly loss of packets. Since MANETs do not rely on any form of central administration or control, nodes in the wireless range dynamically discover each other and establish connection with each other. This helps to maintain the ad hoc network even in situations where nodes keep moving in an out of each others wireless range. Thus MANETs can be rapidly deployed and maintained with minimum user intervention.

Since mobile nodes run on batteries , the processing power available for each node is limited. Since each node is acting as an end user system as well as a router, more energy is consumed to support the function of forwarding packets to destination. Wireless links have a significantly lower capacity compared to wired links [21]. Wireless links often suffer from the effects of multiple access, fading, noise, and interference conditions that prevents it from delivering a throughput equal to the maximum throughput. Each node may be equipped with one or more wireless interfaces operating across different frequencies. Each mobile node might also have a different hardware/software configuration with different capabilities. Designing protocols and algorithms for such heterogeneous, asymmetric links becomes a complex process.

Due to the pervasive nature of mobile nodes, we cannot assume that they will always be under the control of their owners. Nodes could be stolen or tampered with. The shared wireless medium is accessible to both legitimate and illegitimate users. The possibility of eavesdropping, spoofing, and denial-of-service attacks are more prevalent compared to fixed line networks [27]. The applications involving MANETs range from those that involve a small number of nodes to those containing tens of thousands of nodes. Scalability is an important aspect of successful deployment of ad hoc networks. Compared to small networks, the network management algorithms of large networks has to deal with altogether different challenges in areas such as addressing, routing, location management, interoperability, security, mobility, wireless technologies etc. Some of the current and future radio technologies for MANET applications are summarised in Table 2.1 [38].

2.1.2 MANET Applications

The origin of MANETs dates back to the DARPA Packet Radio Network Project in 1972 [32]. The research in MANETs was confined to military for a long time, and in the middle of 1990, with the advent of commercial wireless standards, the potential of MANETs began to be tapped outside the military. Mentioned in Table 2.2 are some of the current and potential areas of MANET applications [38].

Technology	Bit Rate (Mbps)	Frequency	Range
802.11b	Upto 11	2.4 GHz	25-100 m (indoor)
802.11g	Upto 54	2.4 GHz	25-50m (indoor)
802.11a	Upto 54	5 GHz	10–40 m (indoor)
802.15.1	1	2.4 GHz	10 m (up to 100 m)
802.15.3	110-480	3-10 GHz	˜10 m
HiperLAN2	Upto 54	5GHz	30–150 m
IrDA	Upto 4	Infrared (850nm)	˜10 m (line of sight)
HomeRF	1-10	2.4 GHz	˜50 m
802.16	32-134	10-66 GHz	2-5 km
802.16 a/e	15-75	<6 GHz, < 11 GHz	7-10 km, 2-5 km

Table 2.1: MANET wireless technologies

Application	Description
Tactical networks	Military communication and operations • Automated battlefields
Commercial and Civilian environment	Electronic payments anytime and anywhere environments • Dynamic database access, mobile offices • **Vehicular Ad Hoc Networks** • Networks of visitors at airports, sports stadiums, trade fairs, shopping malls • Networks at construction sites
Emergency services	Search and rescue operations • Disaster recovery • Replacement of fixed infrastructure in case of environmental disasters • Policing and fire fighting • Supporting doctors and nurses in hospitals
Entertainment	Multi-user games • Wireless P2P networking • Outdoor Internet access • Theme parks
Education	Universities and campus settings • Virtual classrooms • Ad hoc communications during meetings or lectures

Table 2.2: MANET applications

2.2 Vehicular Ad Hoc Networks (VANETs)

To improve safety and traffic efficiency in vehicles, there has been significant research efforts [65] by government, academia and industry to integrate computing and communication technologies into vehicles, which has resulted in the development of Intelligent Transportation Systems (ITS) [69]. Vehicular communication (VC) is an important component of ITS where vehicles communicate with other vehicles and/or road-side infrastructure, analyse and process received information, and makes decisions based on the analysis.

Such a network of self organised vehicles and road-side infrastructure communicating with each other over wireless, with a view to improve traffic safety and efficiency forms a

VANET. It is envisioned that VANETs will be deployed over the next decade, to achieve considerable market penetration around 2014 [79, 57].

2.2.1 Application Scenario

Integration of communication and computational features into vehicles are being done with an objective to realise vehicular communication. Apart from traffic safety and efficiency, VANETs also support other applications like electronic toll collection, internet access, parking, infotainment, traffic updates etc. Yet safety has remained the primary focus of VANET research. Many literature are available on the classification of VANET applications [5, 3, 73, 69, 25, 48, 54, 22].

[5] has classified VANET applications on the basis of requirements on the communication system. Applications here are classified on the basis of whether the communication is V2V (vehicle to vehicle), V2I (vehicle to infrastructure), I2V (infrastructure to vehicle), single-hop/multi-hop, one-way/two-way etc. In [3], VANET applications are broadly classified as safety and non-safety applications. In [54], applications are categorised into information and warning functions (dissemination of road information like congestion, surface condition etc.), communication based longitudinal control (vehicle platooning), cooperative assistance systems (like lane merge warning, curve warning).

In another classification [22], VANET applications are classified into 3 main categories: safety (life-critical, time critical applications like collision avoidance), traffic monitoring and optimisation (providing traffic information so as to reduce traffic jams), infotainment (internet and payment services). Raya and Hubax [73] has categorised VANET applications as safety-related applications and other applications (traffic optimisation, electronic toll collection, internet access, location based services to find nearby restaurants/gas stations etc). Safety applications are further categorised as traffic information, general safety and liability-related.

[48] has classified safety messages into safety-related (related to safety, but latency not critical) and safety-critical (latency critical safety message). [69] has classified safety applications as life-critical safety applications (latency critical) and safety warning application (safety related, latency not critical). Additionally it gives an added classification called Group communications (e.g. cooperative platooning). In [25], the classification of VANET applications are further refined by taking into account the various situations in which a VANET application is performed.

Application Classification and Definition

For the purpose of this thesis we will classify VANET applications as given in Table 2.3. The classification will be derived the above literature, but tuned to the focus of this thesis (V2V safety-critical applications).

Application Type	Classification	Sub Classification
Safety	Safety-critical applications	V2V based
		V2I/I2V based
	Safety-related applications	V2V based
		V2I/I2V based
Non-safety	Traffic Optimisation	
	Infotainment	
	Payment Services	
	Roadside Service Finder	

Table 2.3: VANET application types

In the table, we have divided the applications into two major categories: safety and non-safety.

1. **Safety applications:** Safety applications has the ability to reduce traffic accidents and to improve general safety. These can be further categorised as safety-critical and safety-related applications. In the design of security, it should be made sure safety messages are not forged.

    a) **Safety-critical**: These are used in the case of hazardous situations (e.g. like collisions). [48]. It includes the situations where the danger is high or danger is imminent [80]. Such applications can access the communication channel with highest priority. In this case latency ($\leq$100 ms) and reliability of messages play an important role in realising the safety function. Safety-critical applications involve communication between vehicles (V2V) or between vehicles and infrastructure/infrastructure and vehicles (V2I/I2V).

    b) **Safety-related**: These include safety applications where the danger is either low (curve speed warning) or elevated (work zone warning), but still foreseeable [80]. In safety-related applications, the latency requirements are not as stringent as in the case of safety-critical ones. Safety-related applications can be V2V or V2I/I2V.

2. **Non-safety applications:** These are applications that provide traffic information and enhance driving comfort. Non-safety applications mostly involve a V2I or I2V communication [3, 48] . These services access the channels in the communication system, except the control channel. They access the channel in a low priority mode compared to safety applications. Non-safety applications include applications for

a) **Traffic optimisation:** Traffic information and recommendations, enhanced route guidance etc.

b) **Infotainment:** Internet access, media downloading, instant messaging etc.

c) **Payment services:** Electronic toll collection, parking management etc.

d) **Roadside service finder:** Finding nearest fuel station, restaurants etc. This involves communication of vehicles with road side infrastructure and the associated database.

2.2.2 Challenges of VANET

VANETs are an instantiation of mobile ad hoc networks (MANETs) [43]. MANETs have no fixed infrastructure and instead rely on ordinary nodes to perform routing of messages and network management functions. However, vehicular ad hoc networks behave in different ways than conventional MANETs. Driver behaviour, mobility constraints, and high speeds create unique characteristics of VANETs. These characteristics have important implications for designing decisions in these networks. Thus, numerous challenges need to be addressed for inter-vehicular communications to be widely deployed [43, 80, 84].

Node Velocity

One of the most important aspects of mobility in VANETs is the potential node velocity [84]. Nodes either denote vehicles or road side units (RSUs) in this case. Node velocity may range from zero for stationary RSUs or when vehicles are stuck in a traffic jam to over 200 km per hour on highways. In particular, these two extremes each pose a special challenge to the communication system. In case of very high node velocities, the mutual wireless communication window is very short due to a relatively small transmission range of several hundred meters [80]. For example, if two cars driving in opposite directions with 90 km/h each, and if we assume a theoretical wireless transmission range of 300m, communication is only possible for 12 seconds.

Moreover, the transceivers have to cope with physical phenomena like the Doppler effect [80]. In the review of issues related to inter-vehicle communication in [13], it is shown that routes discovered by topology-based routing protocols get invalid (due to changing topology and link failures at high speeds) even before they are fully established. High node velocities means frequent topological changes. However, slow movements usually means stable topology, but a very high vehicle density, which results in high interference, medium access problems, etc. For such reasons, very scalable communication solutions are required.

Movement Patterns

VANET are characterized by a potentially large number of nodes that are highly mobile (i.e. according to cars' speed). This high mobility can be more or less important depending on road nature (small streets vs. highways). Vehicles do not move around arbitrarily, but use predefined roads, usually in two directions. Unpredictable changes in the direction of vehicles usually only occur at intersections of roads. We can distinguish three types of roads [80]:

- **City roads:** Inside cities, the road density is relatively high. There are lots of smaller roads, but also bigger, arterial roads. Many intersections cut road segments into small pieces. Often, buildings right beside the roads limit wireless communication.
- **Rural roads:** These roads usually have much larger segments, which means that intersections are more rare than in cities. Traffic conditions often do not allow the formation of a connected network, because too few vehicles are on the road. The overall direction of rural roads changes more frequently than the direction of highways.
- **Highways:** Highways typically form a multi-lane road, which has very large segments and well-defined exits and on-ramps. High speed traffic encountered here.

A node can quickly join or leave the network in a very short time leading to frequent network partitioning and topology changes. These movement scenarios pose special challenges particularly for the routing. Even on a highway, that gives smooth traffic in one direction, frequent fragmentation was encountered in [13]. In the simulation of 9.2 miles of a highway, in [13], a link lifetime of only about 1 minute was obtained even when driving in the same direction (assuming 500 ft radio range).

Node Density

Apart from speed and movement pattern, node density is the third key property of vehicular mobility [80]. The number of other vehicles in mutual radio range may vary from zero to dozens or even hundreds. If we assume a traffic jam on a highway with 4 lanes, one vehicle at every 20 meters and a radio range of 300m, every node theoretically has 120 vehicles in his transmission range.

In case of very low density, immediate message forwarding gets impossible. In this case, more sophisticated information dissemination is necessary, which can store and forward selected information, when vehicles encounter each other. In this case, the same message may be repeated by the same vehicle multiple times. In high density situations, the opposite must be achieved. Here, a message should be repeated only by selected nodes, because otherwise this may lead to an overloaded channel [80].

2.2.3 System Architecture

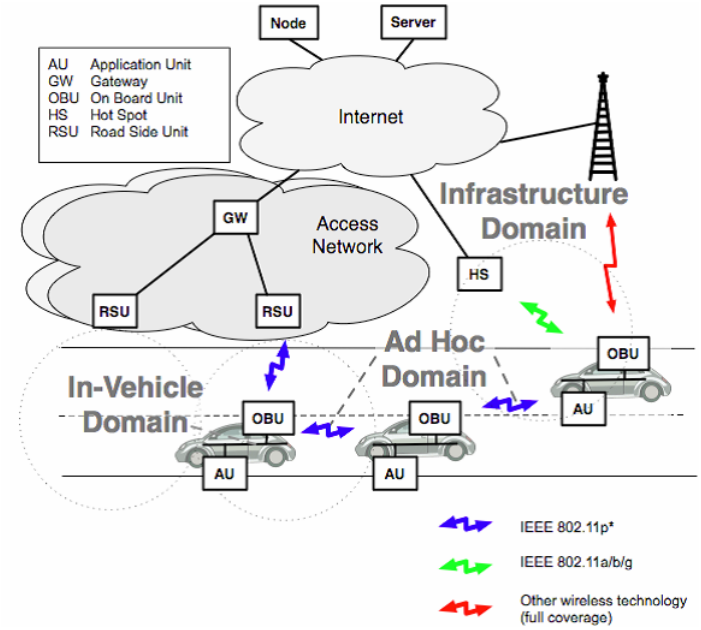

Figure 2.1: VANET System Architecture

A VANET system architecture consists of different domains and many individual components as depicted in Figure 2.1 [30]. The figure shows three distinct domains (in-vehicle, ad hoc, and infrastructure), and individual components(application unit, on-board unit, and road-side unit).

In-vehicle domain*:* This consists of an on-board unit (OBU) and one or more applications units (AU) inside a vehicle. AU executes a set of applications utilising the communication capability of the OBU. An OBU is at least equipped with a (short range) wireless communication device dedicated for road safety, and potentially with other optional communication devices (for safety and non-safety communications). The distinction between AU and OBU is logical; they can also reside in a single physical unit.

Ad hoc domain*:* An ad hoc domain is composed of vehicles equipped with OBUs and road-side units (RSUs), forming the VANET. OBUs form a mobile ad hoc network which allows communications among nodes without the need for a centralised coordination instance. OBUs directly communicate if wireless connectivity exists among them, else multi-hop communications are used to forward data.

Infrastructure domain: The infrastructure consists of RSUs and wireless hotspots (HT) that the vehicles access for safety and non-safety applications. While RSUs for

internet access are typically set up by road administrators or other public authorities, public or privately owned hot spots are usually set up in a less controlled environment. These two types of infrastructure access, RSU and HT, also correspond to different applications types. In case that neither RSUs nor HT provide internet access, OBUs can also utilise communication capabilities of cellular radio networks (GSM, GPRS, UMTS, HSDPA, WiMax, 4G) if they are integrated in the OBU, in particular for non-safety applications.

Application Units (AU)

An Application Unit (AU) is an in-vehicle entity (embedded or pluggable) and runs applications that can utilise the OBU's communication capabilities. Examples of AUs are i) a dedicated device for safety applications like hazard-warning, or ii) a navigation system with communication capabilities. Multiple AUs can be plugged in with a single OBU simultaneously and share the OBUs processing and wireless resources. An AU communicates solely via the OBU, which handles all mobility and networking functions on the AUs' behalf. The distinction between an AU and an OBU is only logical and an AU can be physically co-located with an OBU [5, 30].

On-board Unit (OBU)

The On-Board Unit (OBU) is responsible for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications [5, 30]. It also provides communication services to AUs and forwards data on behalf of other OBUs in the ad hoc domain. An OBU is equipped with at least a single network device for short range wireless communications based on IEEE 802.11p radio technology. This network device is used to send, receive and forward safety-related data in the ad-hoc domain. An OBU can be equipped with more network devices, e.g. for non-safety communications, based on other radio technologies like IEEE 802.11a/b/g/n. OBU functions and procedures include wireless radio access, geographical ad hoc routing, network congestion control, reliable message transfer, data security, IP mobility support, and others.

Road-side unit (RSU)

A Road-Side Unit (RSU) is a physical device located at fixed positions along roads and highways, or at dedicated locations such as gas station, parking places, and restaurants. An RSU is equipped with at least a network device for short range wireless communications based on IEEE 802.11p like radio technology. An RSU can also be equipped with other network devices in order to allow communications with an infrastructure network. An overview of the main functions of a RSU are given below [5, 30].

- Extending the communication range of an ad hoc network by means of re-distribution of information to other OBUs and cooperating with other RSUs in forwarding or in distributing safety information (Figure 2.2).
- Running safety applications, such as for V2I warning (e.g. low bridge warning, work-zone warning), and act as information source and receiver, respectively (Figure 2.3).
- Providing internet connectivity to OBUs (Figure 2.4).

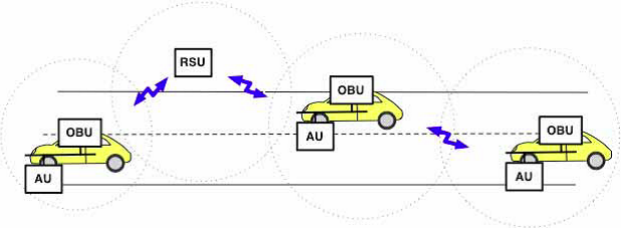

Figure 2.2: RSU extends communication range

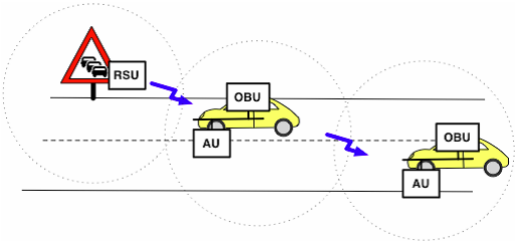

Figure 2.3: RSU acts as information source

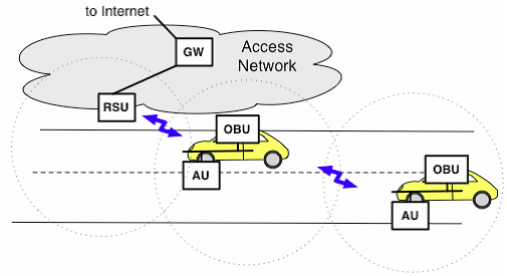

Figure 2.4: RSU providing internet access

2.2.4 Communication Patterns

As we have seen, communication in VANETs can be initiated from vehicles or infrastructure (V2V, V2I or I2V). These communications can be either one-way (no response from receiver) or two-way (involves response from receiver). The communication could also be single-hop or multi-hop. Safety applications either broadcast short status messages

periodically and with high frequency (so called awareness messages), or they generate messages when they detect a safety event and distribute them by multi-hop communication in a certain geographical area (event driven messages). In contrast, infotainment applications typically establish sessions and exchange unicast data packets in greater numbers, bidirectionally, and over multi-hop. The following communication patters can be identified in VANETs [30, 80, 61, 5].

- **Beaconing (Single-hop broadcast):** Involves continuous update of information among all neighbouring nodes, e.g. to supply them with up-to-date status data like the position, speed, heading of a vehicle to allow for cooperative awareness. Communication is single-hop and data packets are broadcast continuously and periodically to all neighbours in reception range. In few cases, the beaconing mechanism may be started by an external trigger, e.g. if an accident occurred. Communication is strictly unidirectional, even if every node uses beaconing. Many applications using beaconing have mid-range latency requirements [80, 61].
- **Restricted Flooding (Multi-hop Broadcast):** In flooding [59], messages to be disseminated throughout a targeted area, are relayed by nodes (provided the same message hasn't been relayed before). The flooding is restricted to reduce redundancy and channel overload, like e.g. in Gossipping [36]. Message propagation is restricted by the use of traditional TTL, and/or by use of geographic distance constraints (**geocast**). Geocast messages are typically sent upon a certain external event and are not sent continuously. Geocast messages are unidirectional. Due to their event-based nature, geocast messages will often require very low latency of messages to inform addressed vehicles as fast as possible.
- **Unicast:** Data is unicast from a sender to a specific destination across multiple wireless hops: the coordinates of the destination are given in the data packet, and relaying nodes forward the packet to their neighbour with the minimum remaining distance to the destination [61]. The communication may consist of only a single hop, or route messages over multiple hops towards the destination. The destination of packets is either a single node or a remote destination region. For multi-hop routing, position-based routing approaches have shown superior performance due to their adaptability to the high node movement dynamics in VANETs [80]. Unicast routing may be uni or bidirectional, triggered by external events. Applications using unicast routing have no immediate relation to safety.

2.2.5 Radio System and Communication Standards

In a VC system, the radio system is formed by the physical and data link layers. For safety applications in a VANET, the radio system needs to maintain definite quality of

service with respect to latency (transmission delay) and reliability (which includes channel throughput and packet reception rates) in the sending, receiving and forwarding of messages [55]. The latency has to be less than 500ms (referred to as lifetime of safety message), which is less than the time (700ms) it takes for a driver to react (like applying brakes) after observing an event.

During safety communication, high mobility has two effects on messaging performance. First, other vehicles may move out of the range of the sender, causing non-delivery of messages. Secondly, high mobility leads to high packet errors and decreased channel throughput. According to [90], the probability of message delivery failure has to be less than 0.01. Moreover, the quality of service for messages should remain acceptable under low or high vehicular speeds, and low or high vehicular densities.

This quality level of minimum latency and maximum reliability cannot be achieved if existing radio bands are used or/and safety and non safety communications share the same frequency and bandwidth [5]. This necessiates the need for a multi-channel radio system, having separate channels for safety and non safety applications. Dedicated short range communications (DSRC) is a wireless technology that offers communication between the vehicles and roadside infrastructure. [12]. Different DSRC standards have been in use in US, Europe, Korea and Japan, mainly for applications like electronic toll collection (ETC) and automatic vehicle identification. These standards were not designed to support V2V or safety communication in VANETs.

Currently we have at least three different organisations developing standards for safety communication in 5.9 GHz ITS band, each tailored to their specific focus, supporting 802.11p: North American IEEE 802.11p + IEEE P1609 (WAVE), European C2C-CC[1] Communication System (ETSI TC ITS) standardised by European Telecommunications Standards Institute (ETSI[2]) , and Global ISO TC204 WG16 (CALM)[3][29, 50].

- WAVE - IEEE focuses on lower layers (802.11) and simplified architecture for just 5.9 GHz communications.
- ETSI TC ITS - Supports 802.11a/b/g/p, GPRS/UMTS at lower layers. Uses a European version of 802.11p. Focuses on car-to-car multi-hopping and geo-networking.
- CALM - Focuses on multiple media (802.11p, DSRC, IR, W-LAN etc) management.

These three groups are developing separate sets of standards, but they overlap in a large number of areas. Recently, initiatives has been undertaken by members of IEEE, ISO and ETSI to come up with measures to integrate these separate standards to a single

[1] *http://www.car-to-car.org/*
[2] www.etsi.org
[3] *http://www.calm.hu/*

global standard [29].

North American DSRC and WAVE

In US, the standardisation efforts for VC [50] focusing on safety are concentrated in the Department of Transportation (DOT) funded projects like the Vehicle Infrastructure Integration Program (VII)[4] and Cooperative Intersection Collision Avoidance System (CICAS)[5]. Industry consortia that support those efforts are the Vehicle Infrastructure Integration Consortium (VIIC) and the Crash Avoidance Metrics Partnership (CAMP).

In 1999, the Federal Communications Commission (FCC) in US allocated 75 MHz in the 5.9 GHz band as a new Dedicated Short Range Communication (DSRC) spectrum, primarily for the purpose of safety use in vehicles. Figure 2.5 shows the channel allocation in North America [69].

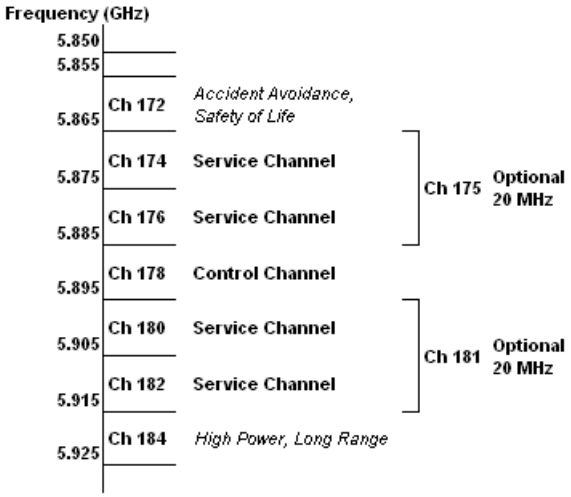

Figure 2.5: North American 5.9 GHz DSRC channel allocation

The DSRC spectrum is divided into 8 channels - one 5MHz channel reserved for future use and 7 channels of 10 MHz each [69, 82]. Channels 174, 176 and channels 180, 182 can be aggregated to form 20 MHz channels 175 and 181 respectively. Channel 178 is the control channel, meant for network control and safety communications only. Channels 172 and 184 are reserved for V2V advanced accident avoidance and high power public safety applications respectively. Rest are available as both safety and non-safety channels.

The basic idea is that RSU announces to the OBU the applications (safety or other) it supports, on the corresponding channel. OBU listens on the control channel, executes

[4] http://www.its.dot.gov/vii/
[5] http://www.its.dot.gov/cicas/

safety applications first, switches channels and then executes non-safety applications. Operating in the 10 MHz channels allows data communication rate of 27Mbps. If the optional 20 MHz channels (175, 181) are used, data rates upto 54 Mbps can be obtained.

In 2001, IEEE adopted 802.11 and 802.11a as the preferred technologies for interoperability of DSRC operations in US [82]. The IEEE 802.11p standard (still in draft mode) [4], a modified form of 802.11a, was adopted as the radio specification (physical and MAC layers) suitable for DSRC safety applications. Higher communication layers for the DSRC standard are defined in IEEE 1609.x series (1609.1, 1609.2, 1609.3, 1609.4), which have been released for trial use [6, 69]. The DSRC communication stack containing IEEE 802.11p and IEEE 1609.x is collectively termed as Wireless Access for the Vehicular Environment (WAVE)(Figure). Figure 2.6 [50] shows an overview of a WAVE protocol stack.

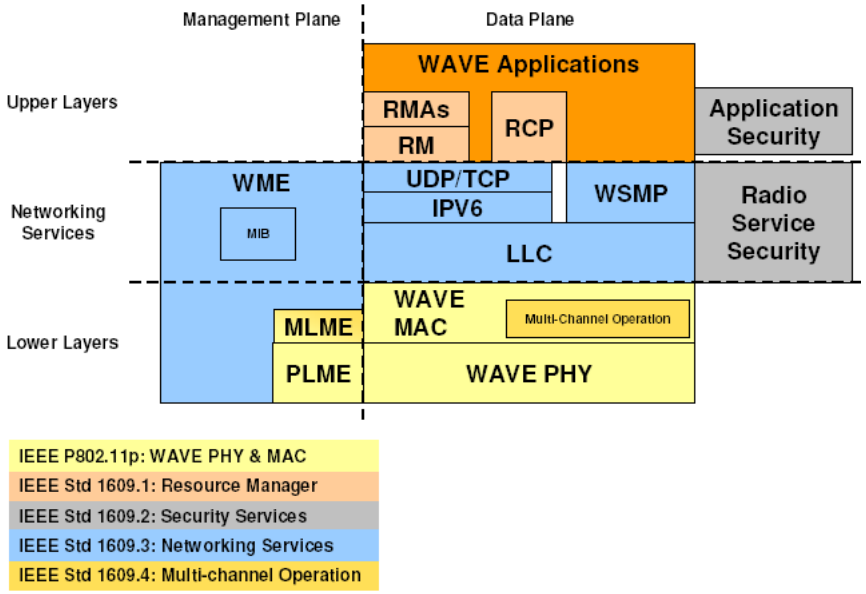

Figure 2.6: WAVE protocol stack

The functionality of the layers above the physical and the MAC layer are described in the IEEE 1609.x document series [6].

The benefits of North American 5.9 GHz DSRC are outlined in [3, 9]. The 5.9 GHz DSRC has a maximum range of 1000 meters within the current standards. Under most operating conditions, DSRC will be limited to less than 200 meters which is well-suited for many vehicle safety applications. DSRC offers the capability of broadcasting messages for vehicle safety applications. One of the most significant potential advantages of DSRC is that latencies of less than 100 milliseconds seem to be possible with DSRC, necessary for many of the vehicle safety applications. Such latencies do not appear to be

achievable with other wireless communications technologies.

European channel allocation and ETSI TC ITS

The European VC research is mainly driven by public funded research projects and the Car 2 Car Communication Consortium (C2C-CC). A large number of European and national funded research projects contribute valuable results in different areas of VC. This large number of projects lead to the creation of COMeSafety[6] project, which coordinates the different projects. It makes sure that the results of the different projects are compatible with each other, and that they conform to the standardisation preparation in the C2C-CC.

C2C-CC drives the standardisation process in Europe. C2C-CC prepares and supports activities like the frequency allocation process, the standardisation of which is finally carried out in ETSI. According to the documents ETSI TR 102 492-1 V1.1.1 (2005-06) and ETSI TR 102 492-2 V1.1.1 (2006-03), a dedicated bandwidth of 30 MHz (5.875 GHZ - 5.925 GHz) will be available for traffic safety applications in the 5.9 GHz band (see Figure 2.6 [5]).

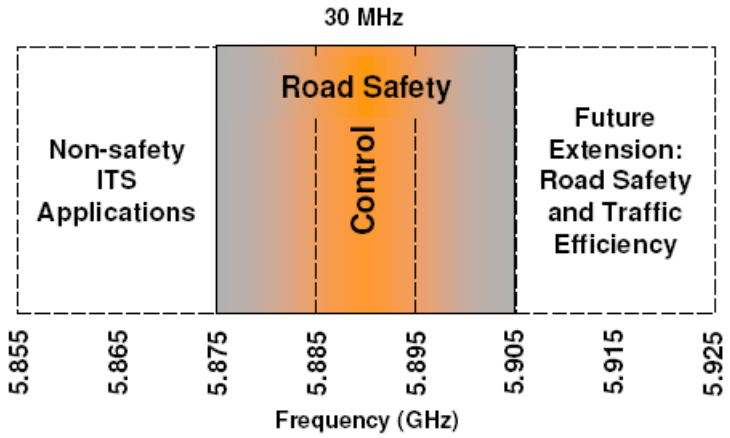

Figure 2.7: Frequency allocation in Europe

Additional 20 MHz might be available as future extension, for road safety and traffic efficiency (5.905 GHz - 5.925 GHz). Non-safety ITS applications might use 20 MHz in the band below 30 MHz. Further details on how to use the available spectrum are still under discussion, like for instance the number of channels, the placement of a control channel, or the number of radio modules that should be used (single vs. dual). An overview of the C2C Communication protocol stack is given in Figure 2.8 [5].

The C2C architecture supports three radio systems: 802.11p* (indicates IEEE 802.11p

[6] http://www.comesafety.org/

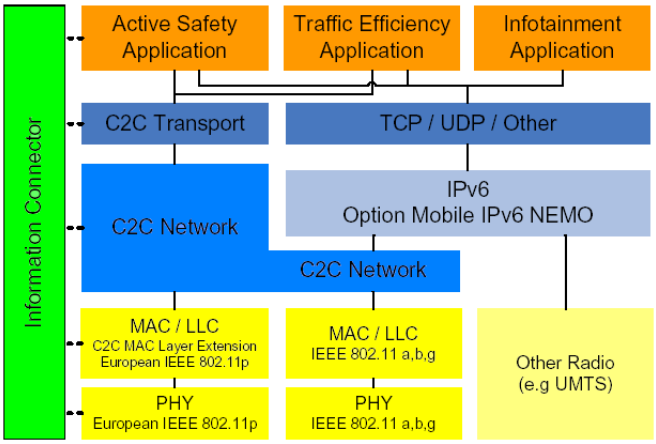

Figure 2.8: C2C Communication System protocol stack

modified to suit European conditions), 802.11a/b/g and other radio (GPRS, UMTS). Non-safety applications (or non critical safety applications may) use TCP/UDP layers and 802.11a/b/g or GPRS/UMTS for communication. Critical safety application communication is strictly confined to C2C Network and Transport layers and 802.11p* coupled with IEEE 1609.4.

3 Identifying V2V Safety-Critical Applications

An analysis of VANET classification and its basis of classification was done in chapter 2. In this chapter, we will identify potential V2V safety-critical applications and their application characteristics. As the next step, in subsequent chapters, we will identify their security and performance requirements, and then outline a security architecture for a secure VANET system. For the purpose of identifying applications, application requirements, and security requirements, the methodology outlined in [47, 48] will be referred to.

3.1 Application Characteristics

Application characteristics are the properties that are used to distinguish one VANET application from another [47]. They answer the most relevant questions about an application like importance, technical requirements and application situation. The general characteristics of a VANET application are given below [47, 3, 48].

1. **Safety influence:** Among the different applications, we find different levels on influence of safety. Applications can be safety-critical (used in hazardous situations like collision), safety-related or non-safety. The definitions have already been elaborated in Chapter 2. The safety characteristic decides how much attention an application gets, as far as security is concerned.
2. **In-Car:** This specifies if an application involves in-car systems like sensors, softwares, brakes or engines. This has security implications because these parts are critical for safe vehicle operation.
3. **Driver involvement:** This explains the extend of driver's involvement in the execution of an application. It can be represented by the following numerical values. Messages of category 3 should be absolutely trustable.

    a) 0=no driver involvement

    b) 1=driver awareness

c) 2=driver attention required

d) 3=driver reaction necessary

4. **Messaging type:** Messaging type is determined by the origin and destination of vehicular communication. Based on this it can be **V2V, V2I** or **I2V**. Security is influenced because infrastructural components of VANETs usually do not require privacy.

5. **Direction of communication:** Communication in this case can either be **one-way** (messages without response) or **two-way** (messages with response). Regarding security, typical one-way communication raises the question of whether to trust the message. In a two-way communication, like in the case of electronic payment, encryption of data is likely needed.

6. **Forwarding of messages:** Applications require either **single-hop**, **multi-hop or relevancy-based** (nodes forward message to other nodes) communications. Security in this case lies with secure routing, which is hard to obtain, because routing involves multiple (possibly fraudulent) nodes.

   a) **Single-hop:** In single-hop communication, messages are directly sent to the destination, which is within the communication range of the sender. Normally for single-hop communication, a range of at least 150 m is assumed for normal road conditions [48].

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

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

7. **Addressing:** Addressing indicates who all receives the message when it is being sent. Since many VC contains position information, securing position information is vital.

   a) **Unicast addressing:** In the case of unicast addressing, receiver is either an OBU or an RSU. Message is addressed to a single destination.

   b) **Broadcast:** In a broadcast, message is send to all entities within the wireless range of a sender. Broadcast can either be periodic and single-hop (**beaconing**) or limited multi-hop (**restricted flooding**) based on TTL (time to live) or geographical destination. In the case of flooding, receiver of message broadcasts the message until TTL=0 [80].

c) **Geocast:** Is the restricted flooding based on geographical destination. All network entities receiving a packet must check their own position to decide whether they are intended to process the packet. In case of single-hop, only those entities in the defined region are receivers (no relaying). In case of multi-hop, if sender is already in the target region, flood the packet within the region. If sender is outside the target region, packet is forwarded to the target region based on routing protocol, then flooded.

8. **Periodic or event-driven:** Describes whether the transmission is triggered by an event (i.e. event-driven), or whether it is sent automatically at regular intervals (i.e. periodic).
9. **Minimum Frequency:** This is the rate at which a transmission should be repeated (if it is periodic).
10. **Maximum Range:** Is the communication distance between two units that is needed to effectively support a particular application.
11. **Latency:** Is the maximum duration of time allowable between when information is available to be transmitted and when it is received. For safety-critical applications, latency $\leq$100 ms. For safety-related applications, latency $>$ 100 ms and latency $\leq$ 1000 ms [3].
12. **Message size:** Is the size of the message that is being sent in VANET communication, not including the cryptographic overheads. Different message sizes have been assumed for safety applications, from 100-500 bytes [88, 82, 53, 77, 68, 8].

3.2 Creating Application List

As we have seen in chapter 2, there are numerous ways in which VANET applications can be classified. Since the intend was to focus on V2V safety-critical communications, we have classified VANET applications on the basis of V2V communications and safety-critical/safety-related applications.

Classifications of VANET applications are mostly driven by the industry. In VSCC [3], a project conducted by CAMP[1] and sponsored by U. S. Department of Transportation (DOT), VANET applications have been categorised as safety and non safety applications. The safety applications are further sub-classified as shown in Table 3.1. These application categories include V2V, V2I and I2V communications for safety.

[1]CAMP comprises the following companies: BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VolksWagen

Safety applications category	Safety applications
Intersection Collision Avoidance	Traffic Signal Violation Warning · Stop Sign Violation Warning · Left Turn Assistant · Stop Sign Movement Assistance · Intersection Collision Warning · Blind Merge Warning · Pedestrian Crossing Information at Designated Intersections
Public Safety	Approaching Emergency Vehicle Warning · Emergency Vehicle Signal Preemption · SOS Services · Post-Crash Warning
Sign Extension	In-Vehicle Signage · Curve Speed Warning · Low Parking Structure Warning · Wrong Way Driver Warning · Low Bridge Warning · Work Zone Warning · In-Vehicle Amber Alert
Vehicle Diagnostics and Maintenance	Safety Recall Notice · Just-In-Time Repair Notification
Information from Other Vehicles	Cooperative Forward Collision Warning · Vehicle-Based Road Condition Warning · Emergency Electronic Brake Lights · Lane Change Warning · Blind Spot Warning · Highway Merge Assistant · Visibility Enhancer · Cooperative Collision Warning · Cooperative Vehicle-Highway Automation System (Platoon) · Cooperative Adaptive Cruise Control · Road Condition Warning · Pre-Crash Sensing · Highway/Rail Collision Warning · Vehicle-To-Vehicle Road Feature Notification

Table 3.1: VSCC safety applications list

Based on the applications identified by VSCC, the European SEVECOM[2] project has come up with its own application list, having a different classification of VANET applications. Moreover it has identified applications on the basis of whether its is safety-critical or safety-relevant. From the list of applications compiled by SEVECOM [48], we can identify twelve V2V safety-critical applications as given below.

- Cooperative Platooning, Intersection Collision Warning, Wrong-way Driver Warning, Emergency Electronic Brake Lights, Pre-crash Sensing, Blind Spot /Lane Change Warning, Cooperative Forward Collision Warning, Approaching Emergency Vehicle Warning, Emergency Vehicle At Scene, SOS Services, Post-Crash Warning, Rail Collision Warning.

[2]http://www.sevecom.org/. This is a European initiative dedicated to security in VANETs.

Safety-critical applications are also listed in [80] under a different categorisation as shown below.

- Active safety (Danger of collision): Intersection Collision Warning, Emergency Electronic Brake Lights, Blind Spot /Lane Change Warning, Cooperative Forward Collision Warning, Warning about Pedestrians Crossing, Rail Collision Warning.

- Active safety (Crash imminent): Pre-crash Sensing.

From the list of applications compiled by VSCC, SEVECOM and [80], and the definition of safe-critical applications in Chapter 2 (2.2.1), we can derive our list of four applications for further analysis as given in Table 3.2. Each application is associated with the required set of application characteristics and its corresponding values.

Application	In-Car	Driver involvement	Messaging type	Forwarding	Direction	Frequency	Addressing	Latency (ms)	Min message size (bits)	Maximum range	Deployment
Pre-crash sensing	Y	0	V2V	S	1	E	B	20	435	50	MT
Cooperative forward collision warning	N	3	V2V	M	1	P	G	100	419	150	MT
Electronic brake lights	N	3	V2V	M	1	E	G	100	288	300	NT
Blind spot/Lane change warning	N	2	V2V	S	1	P	G	100	288	150	NT

MT=Medium-term NT=Near-term P=Periodic E=Event-driven S=Single-hop M=Multi-hop B=Broadcast G=Geocast Y=Yes N=No 1=one-way

Table 3.2: V2V safety-critical applications (Application requirements)

The list of applications in Table 3.2 were chosen due to the following reasons.

- These applications meet our definition of V2V safety-critical applications in Chapter 2. They represent two high priority safety scenarios: scenarios avoiding crashes and where crash is imminent (pre-crash sensing).
- These safety-critical applications have the most stringent latency requirements of all VANET applications (20-100 ms). The other identified applications have time constraints of 100 ms or more.

- They represent the applications that have been identified as the most potential safety applications in [3] and most likely to be deployed in near future. This is indicated by 'Deployment' column in Table 3.2. 'Near-term' represents possible deployment between 2007 and 2011. 'Mid-term' represents possible deployment between 2012-2016.

A preliminary analysis of the selected applications show that

- All applications require cooperative awareness between vehicles.
- The minimum message size is small, less than 100 bytes, not including the cryptographic overhead [8, 3].
- The communication range varies from 50-300 meters.
- Applications are one-way, broadcast/geocast and periodic/event-driven.
- Except for pre-crash sensing (20 ms latency), all applications have a latency of 100 ms.

3.3 Application Description

3.3.1 Pre-crash sensing

Pre-crash sensing [3, 48] can be used to prepare for imminent, unavoidable collisions . Based on position information obtained by beaconing, the car can determine whether a crash is about to occur. This application could use communication in combination with other sensors to mitigate the severity of a crash. Countermeasures may include pre-tightening of seat-belts, airbag pre-arming, front bumper extension, etc.

- Communication Requirements: V2V, one-way communication, broadcast, event-driven
- Minimum frequency (update rate): ~50 Hz, Allowable latency: ~20 ms
- Data regularly transmitted and/or received: vehicle type, position, velocity, acceleration, heading, yaw-rate
- Maximum required range of communication: ~50 m
- Minimum message size: 435 bits

3.3.2 Cooperative (forward) collision warning

Cooperative collision warning [48, 3] collects surrounding vehicle locations and dynamics and warns the driver when a collision is likely. The vehicle receives data regarding the

position, velocity, heading, yaw rate, and acceleration of other vehicles in the vicinity. Using this information along with its own position, dynamics, and roadway information (map data), the vehicle will determine whether a collision with any vehicle is likely. In addition, the vehicle will transmit position, velocity, acceleration, heading, and yaw rate to other vehicles.

- Communication Requirements: V2V, one-way communication, geocast, periodic
- Minimum frequency (update rate): ~10 Hz, Allowable latency: ~100 ms
- Data to be transmitted and/or received: position, velocity, acceleration, heading, yaw-rate
- Maximum required range of communication: ~150 m
- Minimum message size: 419 bits

3.3.3 Emergency electronic brake lights

When a vehicle brakes hard, the Emergency Electronic Brake light application [48, 3] sends a message to other vehicles following behind. This application will help the driver of following vehicles by giving an early notification of lead vehicle braking hard even when the driver's visibility is limited (e.g. a large truck blocks the driver's view, heavy fog, rain). This information could be integrated into an adaptive cruise control system.

- Communication Requirements: V2V, one-way communication, geocast, event-driven
- Minimum frequency (update rate): ~10 Hz, Allowable latency: ~100 ms
- Data to be transmitted and/or received: position, heading, velocity, deceleration
- Maximum required range of communication: ~300 m
- Minimum message size: 288 bits

3.3.4 Blind spot warning / Lane change warning

Blind spot: This application [48, 3] warns the driver when he intends to make a lane change and his blind spot is occupied by another vehicle. The application receives periodic updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change or turn intention, the application determines the presence or absence of other vehicles/pedestrians/bicyclists in his blind spot. In case of a positive detection, a warning is provided to the driver.

Lane change: This application [48, 3] provides a warning to the driver if an intended lane change may cause a collision with a nearby vehicle. The application receives periodic

updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change intention, the application uses this communication to predict whether or not there is an adequate gap for a safe lane change, based on the position of vehicles in the adjacent lane. If the gap between vehicles in the adjacent lane will not be sufficient, the application determines that a safe lane change is not possible and will provide a warning to the driver.

- Communication Requirements: V2V, one-way communication, geocast, periodic
- Minimum frequency (update rate): ~10 Hz, Allowable latency: ~100 ms
- Data to be transmitted and/or received: position, heading, velocity, acceleration, turn signal status
- Maximum required range of communication: ~150 m
- Minimum message size: 288 bits

4 Identifying Security and Performance Requirements

Having identified the application characteristics for the selected applications, the next step would be to identify the security requirements of each application. This is necessary to protect VC messaging system from abuse. Since the safety-critical safety applications aim to provide traffic safety (like avoiding collisions) warnings in a very limited time frame, any attack on the messaging system (which results in wrong warnings or no warnings) will result in accidents.

This chapter will analyse the general threats and attacks faced by a VC system, identify the security requirements necessary to address the threats, and list the security requirements for the selected applications. Apart form identifying the security requirements of selected applications, the performance requirements of the secure communication protocols used in the communication of selected applications are studied. The varying size of safety-critical messages and its impact on the performance of the secure messaging protocol will be specially focused.

4.1 Security Challenges of VANETs

The use of wireless links and time critical nature of VANET safety applications makes it imperative that VC be reliable and trustworthy. A lack of this security element in safety-critical application can make it a lot more than annoying, since lives are at stake during the execution of a safety application. The security of a VC system is prone to vulnerabilities and requires analysis at the radio channel level [49, 84], network level [28, 18], and at the application level [60, 68, 66, 73].

Eichler in [27] gives an overview of MANET security challenges and attacks. A specific overview of the security threats to DSRC/WAVE is covered in [49]. The concept of stealth attacks, which are routing attacks carried out in a low cost manner, with a very low risk of attacker identification, are elaborated in [42]. They can be as harmful as Denial of Service (DoS) attacks. The importance of privacy, the need to protect privacy in VANETs and possible solutions are explained in [24].

[84, 76, 72, 52, 73, 66, 68, 60, 47] provides extensive information on the adversary types, security vulnerabilities/attacks, security challenges, security requirements and security architecture of VANETs.

4.1.1 Adversary Model

To have a better understanding of possible attacks on VANET systems, it is necessary for us to define the adversaries. This helps in determining the scope of resources needed to secure a vehicular system. The following broad classes of adversaries are identified in a vehicular environment [60, 66, 73].

1. **Active vs. Passive:** A passive attacker can only eavesdrop on the wireless channel. This attack varies from a noisy next door neighbour to a government agency trying to profile drivers. An active attacker can generate or modify/drop or replay messages in order to give false information to the network vehicles so that attacker can maximise his gain in the network irrespective of the costs (e.g. a greedy driver posing as an emergency vehicle and clearing way for the attacker to proceed) [73, 66].
2. **Insider vs. Outsider:** An insider is an authenticated member of the network who can communicate with other members. Being a part of the network, an insider is already in possession of some network credentials, like public keys [73]. An insider can cause more damage to the system by tampering with an OBU, than an outsider who has limited access to the system. As far as an outsider is concerned, he normally does not posses any cryptographic credentials or direct physical access to the system.
3. **Malicious vs. Rational:** A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network (e.g. terrorists who deliberately cause traffic accidents) [66, 73]. Hence, he may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target.
4. **Independent vs. Colluding:** Attackers can act independently or in collusion where they exchange information and cooperate to make attacks more effective. For example colluding vehicle can report an imaginary traffic jam or accident to convince other drivers (since the report comes from multiple vehicles others are likely to believe it) and clear way for the attackers [76].
5. **Local vs. Extended:** An attacker can be limited in scope, even if he controls several entities (vehicles or RSU), which makes him local. This is because the limited range of OBUs and RSUs make the attack scope limited. An extended attacker

controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important in privacy-violating and wormhole attacks which will explained shortly [73].

4.1.2 Attacks on VANETs

A VC system can be compromised by an attacker by manipulating either vehicular system or the security protocols. Hence two kinds of attacks can be visualised against vehicular systems: attacks against messages and attacks against vehicles. A general overview of the attacks are mentioned below [76, 73, 66, 27].

Basic Attacks Against Messages

1. **Forgery Attacks:** Attackers diffuse wrong information in the network to affect the behaviour of other drivers (e.g., to divert traffic from a given road and thus free it for themselves) (Fig. 4.1 [73]) .

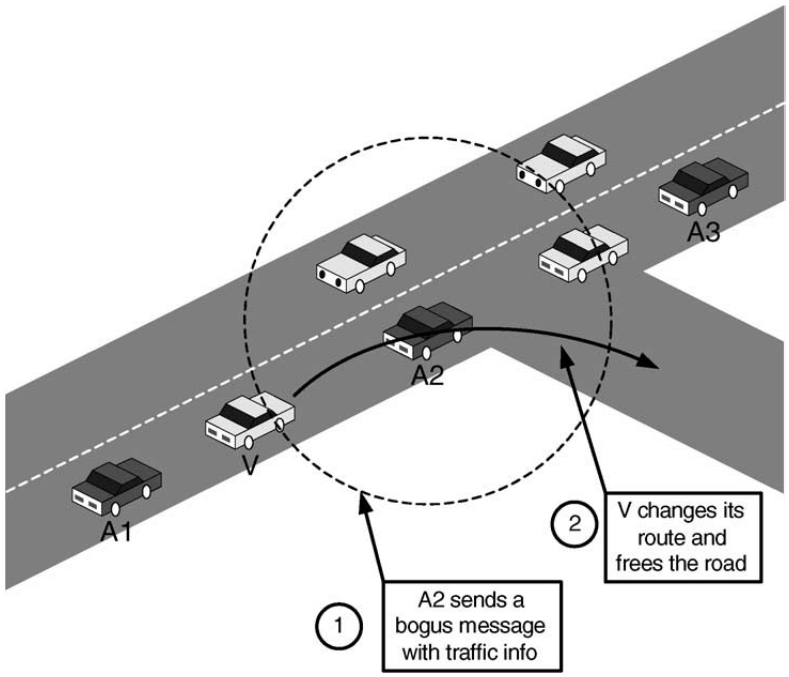

Figure 4.1: Forgery attack

In this example, colluding attackers (A2 and A3) disseminate false information to affect the decisions of other vehicles (V) and thus clear the way of attacker A1.

2. **Cheating with sensor information:** Attackers in this use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each

other, but this would require retrieving the security material and having full trust between the attackers. In cases where liability is involved, drivers may be tempted to cheat with some information that can determine the location of their car at a given time [76, 73].

3. **In-transit traffic tampering:** Any node acting as a relay can disrupt communications of other nodes: it can drop or corrupt messages, or meaningfully modify messages. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. Moreover, attackers can replay messages (e.g., to illegitimately obtain services such as traversing a toll check point). In fact, tampering with in-transit messages may be simpler and more powerful than forgery attacks [76].
4. **Masquerading:** The attacker actively pretends (impersonates) to be another vehicle by using false identities and can be motivated by malicious or rational objectives. Message fabrication, alteration, and replay can also be used towards masquerading. A masquerader can be a threat: consider, for example, an attacker masquerading as an emergency vehicle to mislead other vehicles to slow down and yield.
5. **Privacy violation:** With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy [76]. Then inferences on the drivers' personal data could be made, and thus violate her or his privacy. The vulnerability lies in the periodic and frequent vehicular network traffic. In all such occasions, messages will include, by default, information (e.g., time, location, vehicle identifier, technical description, trip details) that could precisely identify the originating node (vehicle) as well as the drivers' actions and preferences.
6. **Denial of Service (DoS):** The attacker may want to bring down the VANET or even cause an accident. There are many ways to perform this attack, either by sending messages that would lead to improper results or by jamming the wireless channel (this is called a Denial of Service, or DoS attack) so that vehicles cannot exchange safety messages.

Other Attacks

These include other sophisticated versions of basic attacks or a combination of basic attacks on messages as well as attacks on vehicles [73, 49, 27].

1. **Hidden vehicle:** In this scenario, a vehicle broadcasting warnings will listen for feedback from its neighbours and stop its broadcasts if it realises that at least one of these neighbours is better positioned for warning other vehicles [73]. This

reduces congestion on the wireless channel. A hidden vehicle attack consists in deceiving vehicle A into believing that the attacker is better placed for forwarding the warning message, thus leading to silencing A and making it hidden (has stopped broadcasting).

2. **Tunnel:** Since GPS signals disappear in tunnels, an attacker may exploit this temporary loss of positioning information to inject false data once the vehicle leaves the tunnel and before it receives an authentic position update [73]. The physical tunnel in this example can also be replaced by an area jammed by the attacker, which results in the same effects.

3. **Sinkhole attack:** In sinkhole attack, an intruder attracts surrounding nodes with unfaithful routing information, and then performs selective forwarding or alters the data passing through it [27]. The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

4. **Wormhole attack:** The attacker connects two distant parts of the ad hoc network using an extra communication channel as a tunnel. As a result two distant nodes assume they are neighbours and send data using the tunnel. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack. This also extends the range of the attacker. This attack and a possible countermeasure (the concept of packet leashes) is presented in [39].

5. **Sybil attack:** Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy [23]. The Sybil attack especially aims distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods.

6. **On-board tampering:** Other than communication protocols, an attacker may select to tinker with data (e.g., velocity, location, status of vehicle parts) at their source, tampering with the on-board sensing and other hardware. In fact, it may be simpler to replace or by-pass the realtime clock or the wiring of a sensor, rather than modifying the binary code implementation of the data collection and communication protocols [76].

4.2 VANET Security Requirements

Security requirements are the measures that are put in place in order to secure the VC system from the effects of possible attacks identified in the previous section. In identifying the security requirements, application needs and the basic attacks on VC system are considered. The security requirements are derived from primary security goals like confidentiality, integrity and availability. From a review of existing literature [47, 60, 62, 68, 48], the general security requirements of a VC system can be derived as authentication, integrity, entity authentication, confidentiality, privacy, availability, access control, auditability (non-repudiation) and physical security.

4.2.1 Authentication

In safety application, trust is important. Authentication ensures that a message is trustable by correctly identifying the sender of the message [47]. With **ID authentication**, the receiver is able to verify a unique ID of the sender. The ID could be the license plate or chassis number of the vehicle. In other cases receivers are not interested in the actual identity of nodes. They are satisfied if they are able to verify that the sender has a certain property. **Property authentication** is a security requirement that allows verifying properties of the sender, e.g. that the sender is a car, a traffic sign etc. For applications using location information, **location authentication** allows to verify that the sender is actually at the claimed position, or that the message location claim is valid.

4.2.2 Integrity

Integrity requirements demand that the information from the sender to the receiver must not be altered or dropped.

4.2.3 Entity Authentication

Entity authentication ensures that the recently received message is fresh and live. It ascertains that a message was sent and received in a reasonably small time frame [60].

4.2.4 Confidentiality

Confidentiality requires that the information flowing from sender to receiver should not be eavesdropped. Only the sender and the receiver should have access to the contents of the message. e.g. instant messaging between vehicles.

4.2.5 Privacy

Privacy is an important factor for the public acceptance and successful deployment of VANETs [24]. With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy. Then inferences on the drivers' personal data could be made, and thus violate her or his privacy. The vulnerability lies in the periodic and frequent vehicular network traffic messages which will include, by default, information (e.g., time, location, vehicle identifier, technical description, trip details) that could precisely identify the originating node (vehicle) as well as the drivers' actions and preferences [76].

Privacy, along with security, focuses on private vehicles (e.g., excluding emergency vehicles, buses, etc.) because the operation of all other VC nodes, including RSUs, does not raise any privacy concerns, and all the other nodes should be readily identifiable [60]. A primary concern for VC systems is to provide **location privacy**, by preventing others (any observer) from learning past or future locations of a VC system user (vehicle driver or passenger). We can safeguard location privacy by seeking to satisfy a more general requirement: anonymity for vehicle message transmissions.

Ideally, it should be impossible for any observer to learn if a specific vehicle has transmitted or will transmit a message (more generally, take an action according to a VC protocol), and it should be impossible to link any two or more messages (in general, actions) of the same vehicle. Even if an observer tried to guess, there should be only a low probability of linking a vehicle's actions or identifying it among the set of all vehicles, that is, the anonymity set.

Rather than aiming for this strong anonymity, a relatively weaker level of protection is required: messages should not allow for the identification of their sender, and two or more messages generated by the same vehicle should be difficult to link to each other. More precisely, messages produced by a vehicle over a protocol-selectable period of time t can always be linked by an observer that receives them. But messages m1, m2 generated at times t1, t2 such that $t2 > t1 + t$ cannot be linked.

ID privacy [47] specifies how much the identity of the sender should be kept secret. Depending on the applications, **location privacy** has different levels, which range from distributing location information freely throughout the network to totally keeping it private. Although privacy requirements apply for normal communications, public authorities wishing to have access to the identity or location information of cars may have **jurisdictional access**.

4.2.6 Availability

In safety applications like post-crash warning, the wireless channel has to be available so that approaching vehicles can still receive the warning messages. If the radio channel goes out (e.g. jamming by an attacker), then the warning cannot be broadcast and the application itself becomes useless. Hence high availability of communication systems are critical.

4.2.7 Access Control

Access control is necessary for applications that distinguishes between different access levels a node or infrastructure component has [47]. This is established through specific system-wide policies, which specifies what each node is allowed to do in the network. For instance, an authorised garage may be allowed to fully access wireless diagnostics, whereas other parties may only be granted limited access. Another form of access control can be the exclusion of misbehaving nodes (e.g. by an intrusion detection system using a trust management scheme) from the VANET by certificate revocation or other means.

4.2.8 Auditability

Auditability , the non-repudiation requirement, is the mechanism by which senders or receivers can prove that messages have been received or sent respectively [47]. In some applications, messages may only be stored for a very limited time (e.g. the last 10 seconds in a ring buffer) and made permanent only in case of an incident (e.g. crash).

4.2.9 Physical Security

This is essential to prevent unauthorised access of vehicle which could lead to unauthorised use, compromise of radio system or cryptographic credentials.

4.3 Identifying Application Security Requirements

As we have already seen, security and privacy-enhancing mechanisms are necessary for an effective VANET deployment. Based on the threats and attacks on a vehicular system discussed in 4.1.2, the security requirements of the selected applications has been derived by SEVECOM, as given in Table 4.1 [48]. None of the applications in the table intend to pass any confidential messages to vehicles around them. Rather, they broadcast messages that should be readable by vehicles in their wireless range. Hence confidentiality is irrelevant for the selected applications.

Application	ID authentication	Property authentication	Location authentication	Integrity	Entity authentication	Confidentiality	ID privacy	Location privacy	Jurisdictional access	Availability	Access control	Auditability	Physical Security
Pre-crash sensing	0	2	2	2	2	0	2	0	0	2	0	0	2
Cooperative forward collision warning	0	2	2	2	2	0	2	0	0	2	0	2	2
Electronic brake lights	0	2	2	2	2	0	2	0	0	2	0	2	2
Blind spot/Lane change warning	0	1	2	2	2	0	2	0	0	2	0	2	2

0=irrelevant 1=important 2=very important

Table 4.1: V2V safety-critical applications (Security requirements)

Pre-crash sensing is an application that comes into play when accident is imminent. Its purpose is not to avoid an accident, but to make vehicles ready for an imminent crash. Hence auditability is irrelevant. Whereas the other three applications provide surrounding vehicles with information with a view to improve driver awareness and thus reduce accidents. In the event of an accident, it becomes necessary for law enforcement agencies to prove the question of liability. Hence auditability is essential in the case of these three applications.

Authentication, integrity and entity authentication are required to make sure that the sender is authentic, message is not spoofed, modified, deleted or replayed. Property authentication verifies if the sender is a vehicle or an RSU. Location authentication verifies if the location information in the message is authentic. Also the availability of wireless media and messages has to be ensured without which the applications will fail to deliver messages successfully to intended recipients.

The applications in Table 4.1 have to advertise location information in their periodic broadcast to surroundings. Hence location privacy is not relevant. But it should not be possible to correlate two messages from the same vehicle nor should the identity of the vehicle be disclosed. Hence ID privacy is important and ID authentication is not desirable. It is essential that the cryptographic credentials should not be tampered with, for the reliability of security protocols.

4.4 Identifying Performance Requirements

For safety communication in VANETs, the application requirements has to be taken into account ,and also the safety requirements has to be satisfied. This makes sure that the safety communications are effective and reliable, free from internal or external interferences. Secure communication protocols used in safety applications are designed in such a way that they satisfy the application and security requirements for that application. Apart from security requirements, it is essential that they also meet certain performance requirements, without which they might not be suitable for use in safety applications.

In VANETs, the reliability, latency and channel efficiency deteriorate with speed, traffic density and transmission range. The traffic density depends on message rate (messages/second), size (bytes/message), message range (meters), and density of vehicles producing these messages [88]. It is important to chose VC system parameters ideally without which VANET will fail to function properly. For e.g. a message update slower than once every 500 ms is probably too slow. Driver reaction time to stimuli like brake lights can be of the order of 0.7 seconds and higher. Thus if updates come in slower than every 500 ms, the driver may realise something is wrong before the safety system. This would make the driver think the safety system is not effective.

In [88], the author has outlined different traffic parameter ranges for message rates (corresponding to high to low traffic conditions), message sizes (corresponding to established standards), vehicle density and channel data rates for safety communication, so that the performance requirements for safety communication system is met. In the case of secure communication protocols, the impact of security mechanisms on safety communication will be analysed. For communication protocols, there is an additional factor that contributes to message size and communication delay: size of cryptographic credentials and the time taken for authentication (in the case of PKCS (Public Key Cryptography Standards), the size of signature and public key and the time required to verify the signature) [72].

Deriving from the above analysis, this thesis will focus on the following parameters while doing a performance evaluation of a secure communication protocol used for safety-critical applications.

- **Message size vs. message delay:** Messages of different sizes are considered and the maximum message delay per message is calculated for both highway and city scenarios. For the protocol to meet the performance requirement, the maximum message delay per message for the protocol should to be below the maximum processing delay calculated for each message.

- **Message size vs. throughput:** Messages of different sizes are considered and the maximum message throughput is calculated for both highway and city scenarios. For the protocol to meet the performance requirement, the calculated throughput should to be less than the minimum bandwidth of the radio channel.
- **Message rate vs. processing delay:** The maximum tolerable processing delay of each message for both highway and city scenarios is calculated. For the protocol to meet the performance requirement, the signature verification delay per message for the protocol should to be below the maximum processing delay calculated for each message.

5 Security Architecture for Selected Applications

The rich features of a VC system is a double edged sword, as they also give rise to various vulnerabilities. Attacks against VC systems not only make it useless, but also make it potentially dangerous (wrong warnings or failure to issue warnings). Security requirements are measures developed to counter attacks against a VC system . Based on the security requirements that are identified, the security architecture of any VC system is designed.

A security architecture consists of the different elements that are essential in addressing security requirements and the subsequent implementation of security in a VC system. The need for security architectures and different architecture proposals are explored in [68, 46, 52, 73, 61, 34, 51, 60]. This chapter will first discuss the security architecture for the V2V safety-critical applications identified in Section 4.3 (referred to as 'selected applications') This will be followed by additional assumptions required for security and performance analysis of selected applications.

5.1 Architecture Components

5.1.1 Authorities

Authorities are trusted entities responsible for the issuance and management of identities and credentials for nodes in VANETs [62]. [68, 73] proposes a system where the authority is a governmental transportation authority (GTA) or vehicle manufacturer (VM) with which vehicles are registered. GTA or VM acts as the certification authority (CA) certifying the credentials of vehicles, and also revokes certificates in case of vehicle misbehaviour. This implies the need for a Public Key Infrastructure (PKI) where Certificate Authorities (CAs) will issue certified public/private key pairs to vehicles. The presence of on-line authorities is not required, as connectivity and communication, especially over the wireless medium, with an authority may be intermittent.

Similar to existing administrative processes and automotive authorities (e.g., city or

state transit authorities), a large number of CAs will exist [61, 60]. Each of them is responsible for the identity management of all vehicles registered in its region (national territory, district, county, etc.). To enable interactions between nodes from different regions, CAs provide certificates for other CAs (cross-certification) or provide foreigner certificates to vehicles that are registered with another CA when they cross the geographical boundaries of their region [64].

5.1.2 Identification and Registration

Every vehicle that becomes a part of a VANET has to be identified with an electronic identifier. Each vehicle has to store the following identities that are bound to related cryptographic information:

Long-term identity (LTI): An electronic identity called an Electronic License Plate (ELP) [41] issued by a government, or alternatively an Electronic Chassis Number (ECN) issued by the vehicle manufacturer. These identities (further referred to simply by ELP) should be unique and cryptographically verifiable (this can be achieved by attaching a certificate issued by the CA to the identity) in order to identify vehicles to the police in case this is required (usually, identities are hidden from the police).

Each ELP has a pair of long-term private and public cryptographic keys, k_V and K_V respectively issued by manufacturers or authorities. A digital certificate provided by the authority binds K_V to ELP and to other data attributes of ELP like vehicle features (colour, brand etc) [62][34]. k_V is used to generate digital signatures to authenticate ELP to the CA and request for pseudonyms.

Similarly to the physical license plates, the ELP should be changed (i.e., reloaded in the vehicle) when the owner changes or moves, e.g., to a different region or country [73]. Infrastructure nodes and users may also have unique identities, registered with authorities. The identities registered with the authority helps to link it to the respective vehicle's or owner's identity. The lifetime of the certificate should be long, following the node life cycle (or a significant fraction of it).

Infrastructure nodes can be considered as more trustworthy than other nodes, with respect to specific functionality or attributes [62]. Public vehicles (police, fire etc), similarly to infrastructure nodes, are considered more trustworthy, and they can be used to assist security related operations. The user can be bound to its credentials and secrets through some token she/he uniquely knows or possesses (e.g., pass-phrase, biometric data). The user can be the owner and/or the driver of the vehicle, or in general any passenger.

Short-term identity (STI): These are anonymous key pairs that are used to preserve privacy. An anonymous key pair is a short-term public/private key pair that is authenticated by the CA but contains neither information about nor public relationship with (i.e., this relationship cannot be discovered by an observer without a special authorisation) the actual identity of the vehicle (i.e., its ELP). Normally, a vehicle will possess a set of anonymous keys to prevent location tracking [73]. The CA signs each of the public keys, and generates a set of pseudonyms [19] for the vehicle. Each pseudonym contains an identifier of the CA, the lifetime of the pseudonym, the public key, and the signature of the CA, and thus, no information about the identity of the vehicle. The CA retains a mapping of vehicle/user identity and the pseudonym for purposes of liability.

5.1.3 Hardware Security Module

Hardware security module (HSM) is the trusted computing base of a vehicle. The purpose of an HSM is to provide a physically protected environment for the storage of private keys (long-term and short-term keys), the execution of cryptographic operations (message signing and decryption of encrypted anonymous certificates) and key management functions [60]. The HSM is physically separated from the OBU that performs public key operations. The HSM must have an API through which it can provide services to the other modules of the security architecture that run on the onboard unit (OBU) [46].

This API should support the digital signature and timestamping service (to prevent replay of messages signed by HSM), the decryption service (to verify incoming pseudonyms), as well as the key and device management services described in [73]. The HSM should have its own battery, which can be recharged from the vehicle, and clock (for timestamping service), which can be securely resynchronised, when passing by an RSU. The access to this device should be restricted to authorised people. For example, cryptographic private keys are generated and stored in HSM by vehicular authorities, short term keys can be renewed at the periodic technical checkup of the vehicle, and expired certificates can be changed by the user upon authentication [68, 60]. The use of secret information such as private keys requires that HSM be a tamper resistant hardware (TRH).

TRH contains a set of sensors that can detect hardware tampering and erase all the stored keys to prevent them from being compromised. Economical options can be a TPM (Trusted Platform Module) [73] that can resist software attacks but not sophisticated hardware tampering. or other low-end tamper-resistant devices (e.g., smart cards). In particular, commercially available low-end devices do not have built-in batteries and consequently cannot provide a trusted internal clock. As pointed out in [61], without a trusted source of time, such devices are not able to produce timestamps that can be trusted by other participants in the system. For practical purposes, an HSM implemen-

tation somewhere between high-end and low-end devices is needed.

The HSM handles short-term keys for the short-term identification and long-term keys for the long-term identification of the vehicle [60]. The generation of short-term keys can be initiated by any application running on the OBU. In contrast, the long-term keys are generated at manufacturing time; however, they can be updated later by trusted authorities. If the ownership of the vehicle changes, long-term key can be changed. Device management and long-term key updates are achieved through signed commands from the CA. In order to verify the signature on these commands, the HSM stores trusted root public keys that are loaded into the device during the initialization procedure in a secure environment.

[68, 60] proposes two such root public keys, K1 and K2, in the HSM, with the corresponding private keys held by the CA. If one of the CA's private keys is compromised, the corresponding public key, say K1, can be revoked. The revocation command must be signed with the private key corresponding to K1 itself. Once K1 is revoked, a new key K3 can be loaded into the HSM by a command signed with the private key corresponding to K2. In addition, when K1 is revoked, the HSM does not accept commands aimed at revoking K2. This scheme ensures secure root key update unless both root keys are compromised. The revocation of the HSM is also discussed by [60]

5.1.4 Authentication, Integrity and Non-Repudiation

The exchange of safety messages in a VANET needs authentication but not encryption. The simplest and the most efficient method is to assign to each vehicle a set of public/private key pairs that will allow the vehicle to digitally sign messages and thus authenticate itself to receivers. These public keys should be issued and signed by a trusted authority. [73].

Under the PKI solution, before a vehicle sends a safety message, it signs it with its private key and includes the CA's certificate as follows:

$V \rightarrow *: M, Sig_{Pr_{K_V}}[M|T], Cert_V$

where V designates the sending vehicle, $*$ represents all the message receivers, M is the message, $|$ is the concatenation operator, and T is the timestamp to ensure message freshness (entity authentication). The digital signature ($Sig_{Pr_{K_V}}[M|T]$) provides authentication, integrity and non-repudiation properties to the message. It should be noted that using nonces and sequence numbers instead of timestamps is not desirable because of the burden of the inherent preliminary handshake and maintenance issues.

$Cert_V$ is the public key certificate of V issued by CA.

The receivers of the message have to verify the public key of V using the certificate and then verify V 's signature using its certified public key. In order to do this, the receiver should have the public key of the CA, which can be preloaded. Attaching a digital signature and a certificate to each safety message for the sake of security inevitably creates an overhead that can be larger than the message itself. To reduce overheads, Elliptic Curve Cryptography (ECC) and NTRU cryptosystem is preferred against RSA [72]. Additionally overhead can be reduced by signing one in every few messages (optimisation).

Raya et.al in [73] has explored other possibilities to reduce overheads like symmetric key types (pairwise, TESLA protocol [67, 40] , group keys [70]) and hybrid protocols (pseudonyms with group signatures) [17, 20] for authentication.

Symmetric cryptographic primitives are much more efficient (in terms of time and space overhead) than the asymmetric ones. According to [73] session key establishment does not scale well with the number of vehicles (even with a few vehicles) and soon exceeds digital signatures in terms of overhead. For scenarios with only few vehicles, the establishment of session keys for efficiency purposes is not justified because of the lack of congestion on the wireless channel. In addition, non-repudiation cannot be achieved with symmetric keys. Hence critical safety applications cannot rely on symmetric session keys .

In [73], it has been shown that pairwise keys result in bigger overhead than ECC even when there are only a few vehicles; group keys result in saving considerable message overhead. But group key establishment [70, 73] and membership update require more messages than the digital signature approach; the actual overhead depends on the number of vehicles as well as the dynamics of the network. Therefore, symmetric group key establishment may lead to significant savings in bandwidth consumption but at the expense of more transmissions and the complexity needed to implement group protocols. TESLA protocols were found unsuitable for delay-intolerant VANETs [73].

Hence, digital signatures seems to be the most convenient and reliable solution for authentication, even though its efficiency leaves place for improvement. With the hybrid authentication approach, on-board, on-the-fly pseudonym generation and self-certification is achieved . The use of group signatures, helps reduce the overhead associated with signatures, handle management issues associated with use of pseudonyms, and provides a stronger anonymity property than using pseudonyms alone [17].

5.1.5 Key Management

The management of credentials, both short- and long-term, is undertaken by the CAs that are also responsible for the revocation of credentials for any node if needed. Public key operations are performed by the OBU, but all private key operations are performed by the HSM, which is essentially the trusted computing base of the secure VC system.

Each node has a unique ELP decided by car manufacturers and authorities [73]. Each ELP is associated with a cryptographic key pair and a set of attributes. The attributes reflect technical characteristics of the node(e.g., type, dimensions, sensors, and computing platform), as well as the role of the node in the system. The assignment of an identity, attributes, and the generation of the certificate are performed offline at the time the node is registered with the CA.

To obtain pseudonyms, a vehicle V's HSM generates a set of key pairs (SK_{1V}, PK_{1V}) to (SK_{nV}, PK_{nV}) and sends the public keys to a corresponding CA via a secured communication channel [60]. V utilises its long-term identity ID_V to authenticate itself to the CA. The CA signs each of the public keys, PK_{jV} , and generates a set of pseudonyms for V. Each pseudonym contains an identifier of the CA, the lifetime of the pseudonym, the public key, and the signature of the CA, and thus, no information about the identity of the vehicle.

Pseudonyms are stored and managed in the onboard pseudonym pool, with their corresponding secret keys kept in the HSM. This ensures that each vehicle has exactly one key pair (its own pseudonym and private key) that is active during each time period. Moreover, once the switch from the (SK_{jV}, PK_{jV}) to the $(j+1)st$ key pair $(SK_{(j+1)V}, PK_{(j+1)V})$ is made, no further messages can be signed with SK_{jV} , even if the certificate for PK_{jV} is not yet expired. In other words, pseudonymity cannot be abused: for example, a rogue vehicle cannot sign multiple beacons, each with a different SK_{jV} , over a short period, and thus cannot appear as multiple vehicles [60].

Due to the requirement for accountability, the CA archives the issued pseudonyms together with the vehicle's long-term identity. In case of an investigation, an authorised party can ask the CA to reveal the link of a specific pseudonym to the long-term identity of the vehicle (this leading further to its registered owner).

Certificate Revocation

The advantages of using a PKI for VANETs are accompanied by some challenging problems, notably certificate revocation. For example, the certificates of a detected attacker

or malfunctioning device have to be revoked, i.e., it should not be able to use its keys or if it still does, vehicles verifying them should be made aware of their invalidity. The most common way to revoke certificates in the case of long-term keys is the distribution of CRLs (Certificate Revocation Lists) that contain the most recently revoked certificates. In the case of short-term keys (pseudonyms), since short-lived certificates are used, they are automatically revoked after a time period. These are the methods proposed in the IEEE P1609.0 draft standard [6].

But there are several drawbacks in this approach. First, CRLs can be very long due to the huge number of vehicles and their high mobility. Second, the short lifetime of certificates still creates a vulnerability window. The challenge is to distribute the CRLs effectively and efficiently. RSUs distribute CRLs onto vehicles. In areas with no RSUs, the V2V CRL distribution is initiated by vehicles that were previously in contact with RSUs. More efficient revocation methods are suggested in [44, 68]:

- RTPD (Revocation protocol of the Tamper-Proof Device): CA revokes all keys of a vehicle by sending a revocation message to the vehicle. Other VANET participants do not have to know about the revocation. After receiving the revocation message HSM of the vehicle erases all keys, sends an acknowledgement to CA, and stops signing messages. This means no more valid messages can be generated by this vehicle.
- RCCRL (Revocation protocol using Compressed Certificate Revocation Lists): Compressed CRLs (CCRLs) are used if HSM does not send an acknowledgement or if only a subset of keys should be revoked. It mainly works like an ordinary revocation list i.e. after receiving a message the recipient has to use the CCRL to check if the certificate of the sender is valid. To be able to do so the CCRL has to be distributed in the VANET.
- DRP (Distributed Revocation Protocol): If the neighbours of a vehicle observe misbehaviour they warn each other not to trust messages of the suspect vehicle. If there is enough evidence they contact CA that decides if the corresponding vehicle's ELP should be revoked permanently. DRP therefore is more a warning protocol than a revocation protocol.

Revocation lists are assumed to be not that time critical. This holds true as long as nodes can check plausibility of the warning by means of in-car sensor data (that contains a list of malicious nodes) [68], verify with messages received from other VANET participants, and features like DRP are available.

5.1.6 Privacy and Anonymity

For vehicular ad hoc networks, privacy has been identified to be profoundly important [24, 41]. In VC it is essential to authenticate senders (by electronic identifiers) and to advertise sender positions or locations [3]. As we can see from the analysis of privacy threats in [24], most issues are related to position and vehicle identifier. This involves either correlating the electronic identifier with a real-world vehicle identity, or by logging and analysing the relations of various position-identifier pairs to ultimately obtain vehicle identity (e.g., by associating him with his place of living) .

Since safety messages do not contain any confidential data about their senders, vehicle owners will be only concerned about identity and location privacy. To respond to these concerns, [41, 68, 34] proposes the use of anonymous public keys. Signed messages can be trivially linked to the certificate of the signing node. Therefore, the removal of all information identifying the user/vehicle from node certificates does make communications anonymous.

Each private vehicle is equipped with a set of distinct certified anonymous public keys that do not provide additional identifying information, denoted as pseudonyms [19, 61, 68, 34]. A node utilises the private key corresponding to a pseudonym to sign outgoing messages, and appends the pseudonym to the messages. Messages signed under the same pseudonym (i.e., using the same corresponding private key) can be trivially linked to each other.

As the vehicle changes pseudonyms, linking messages signed under different pseudonyms becomes increasingly hard over time and space. In order to preserve the driver's anonymity and minimise the storage costs of public keys, [72] proposes a pseudonym changing algorithm that adapts to the vehicle speed and takes into account key correlation by the attacker as described below.

$$min(T_{key}) = \frac{(d_v + 2d_r)}{v_t}\ seconds$$

where $min(T_{key})$ is the minimum time a pseudonym should be used unchanged, v_t is the vehicle speed, d_r is the transmission range, and d_v is the distance over which a vehicle does not change its speed and lane (the vulnerability window with respect to the correlation of keys). Ideally pseudonyms should be changed for every time period slightly greater than $min(T_{key})$.

The change of a pseudonym should be accompanied by a change of the node identifiers

like Medium Access Control (MAC), and IP addresses. Otherwise, messages generated by a node could be trivially linked according to the addresses used by the node's hardware and software [61]. From the discussions so far, we can arrive at the conclusions given below [73].

- **Identity and location privacy:** All vehicle identifiers, in particular MAC and IP addresses, must change over time. Even though anonymous keys do not contain any publicly known relationship to the true identity of the key holders, privacy can still be hijacked by logging the messages containing a given key and thus tracking the sender until discovering his identity. Therefore, anonymous keys should be changed in such a way that a pervasive observer cannot track the owner of the keys.
- **Conditional privacy:** Privacy preservation is a requirement for deploying vehicular safety applications. But safety and the implied liability requirement have higher priority. Hence, anonymity should be conditional on the scenario (e.g., if there are issues of law enforcement or national security, anonymity should be overridden). Hence, the ID disclosure capability should be distributed among multiple authorities to prevent abuse. For example, police should not be able to retrieve the identity corresponding to an anonymous key without the permission of a judge.

5.1.7 Secure Communication

Digital signatures are used for secure communication in VANETs [61], and can be used for all messages. Messages are signed with the private key corresponding to the current pseudonym . The messages also have a time-stamp, the sender's clock value, a geo-stamp, and the sender's coordinates at the sending time. This mechanism can be applied to different types of message dissemination: beaconing, restricted flooding (broadcast or geocast), and position based routing (unicast).

For beaconing, a single signature would suffice. For multihop propagation, depending on the type of message, the originator appends its signature, while hop-by-hop signatures can also be added and removed. The latter option, with the combination of signatures, is also meaningful for securing Position-Based Routing [37].

5.1.8 Secure Positioning

In VC, position is one of the most important data for vehicles. Each vehicle needs to know not only its own position but also those of other vehicles in its neighbourhood. The most common approach to positioning vehicles is by GPS. But this has several drawbacks, because the precision of GPS is to the order of several meters and degrades in urban

environments because of constructions such as buildings and tunnels that weaken GPS signals.

GPS can also be subject to a series of attacks such as signal jamming and spoofing. The authors of [41] propose a method whereby three or more base stations perform distance bounding on a vehicle before computing its location. The obvious drawback of this approach is the need for infrastructure coverage. In a different approach presented in [66], vehicles rebroadcast the public keys of other vehicles after signing them. This helps to perform relative localisation. A final solution is yet to be formulated for the issue of secure positioning.

5.1.9 Correctness of Data

It is important to verify the correctness of data (like position information) send by active safety applications in VANETs. Data is collected by the node from all available sources (for example the warning system, data that is available from telemetric monitoring and data extracted from other VANET communication). The collected data is used by every vehicle to create an independent view of its current status, its current surrounding (physical) environment and current or previous neighbouring vehicles.

Then, upon the reception of a warning message, the message (its content, origin, etc.) is evaluated and compared to the vehicle's own estimation of the current situation, which results from the previously collected data. Due to the time critical nature of a warning system, this comparison has to be done in near-real-time, otherwise the warning information would be useless [52].

5.2 Assumptions

In this section the basic assumptions required for the security and performance analysis of selected applications are laid down.

5.2.1 Choice of Communication System

5.9 GHz DSRC was the first radio spectrum be allocated for safety applications in United States [7, 9]. The standardisation of lower layers (802.11p) [4], and the upper layers [6] was performed by IEEE resulting in the WAVE communication standard. They were developed with special focus on the priority and time constraints of safety communication in VANETs

Ongoing research efforts in the Europe also rely on a similar spectrum band and a European version of 802.11p [50] for V2V safety communication system. Japan is using a modified WAVE architecture in their trial stages. For the purpose of performance analysis in this work, a 5.9 GHz DSRC messaging system will be assumed, since it forms the basis of safety messaging standards worldwide [50].

5.2.2 Vulnerabilities

Here we assume some of the obvious attacks that can be carried out by an attacker, and that are hard to defend against. The most obvious attack would be jamming attacks against the wireless channel. This can be carried out by someone inside or outside the VANET. We also assume that the physical security associated with nodes are trivial, and that revocation of nodes is not immediate (nodes can contact CA only when it encounters an RSU). Therefore it is hard to defend against the manipulations in sensor data carried by a valid sender (malicious node) in the network. Malicious nodes can send false position and other data to escape accountability in case of accidents. False allegations against nodes are made by malicious nodes so that valid nodes are revoked from the network.

5.2.3 Basic Safety Messaging Protocol

Safety communications involve periodic broadcast of messages. Depending on the traffic density conditions we assume the following [72].

- In compliance with the DSRC specifications [7, 9], we assume that each vehicle V periodically sends messages over a single hop every 300 ms within a range of 10 s travel time (the minimum range is 110 m and the maximum is 300 m).
- The inter-message interval drops to 100 ms and the range to 15 m if the vehicles are very slow or stopped (i.e., their speed is less than 10 miles/h or $\approx$ 16 km/h).
- Vehicles take decisions based on the received messages and may transmit new ones. For example, if a vehicle V receives an emergency warning from another vehicle W and, based on their mutual positions, estimates that it is also in danger, it sends out its own warning messages.
- The minimum data rate for safety communication in DSRC is 6 Mbps (and typically 12 Mbps) [88, 51].

5.2.4 Traffic Scenario

For the purpose of performance analysis, we assume the following traffic scenarios [72].

- **Highway:** A highway with 6 lanes (3 in each direction) of 3 m each. We assume a uniform presence of vehicles, with an inter-vehicle space of 30 m. Vehicles are mobile and transmit DSRC messages every 300 ms over a 300 m communication range.
- **Congestion:** Assuming the same highway as in the previous case but this time vehicles are very slow or stopped (congestion scenario) and spaced by 5 m (including the vehicle length). Each vehicle transmits a safety message over a range of 15 m every 100 ms.

6 Performance Analysis of Authentication Protocols

In this chapter, authentication protocols used for safety messaging in VANETs will be identified and their performance evaluated against the application requirements listed in 4.4, Table 3.2 and Table 4.1. For the purpose of performance analysis, the following three protocols that provides common grounds for analysis, are chosen [17, 53, 63]. Before we go into the analysis of protocols, we will briefly touch upon the network characteristics of a VANET system that should be considered prior to any study of vehicular communication.

6.1 Network Characteristics

The main challenge for communication in VANETs is the high mobility, the resulting high rate of topology changes, and the high variability in node density. Typical protocols are hard to apply, e.g. topological routing protocols suffer from outdated neighbour information [13]. Numerous literature are available that address the effect of mobility on message delay, throughput, packet losses, probability of reception etc under dense and sparse traffic conditions. Thus it can be understood that, in VANET communications, the key component is the movement pattern of vehicles, also called the mobility model. Mobility models determine the location and speed of nodes in the topology at any given instant, which strongly affects network connectivity and throughput. Some of the mobility models being used are the ones used in NS-2 simulator [1], Manhattan Grid model [26], and Random Waypoint Model [15]. An accurate analysis outcome requires a good mobility model that has captured all the aspects of mobility as explained in [56, 45]

Another challenging issue in VANETs is congestion control [87]. In case of congestion, normally the endpoints detect overload conditions at intermediate nodes and reduces its data rate. In VANETs, the topology changes within seconds and a congested node used for forwarding a few seconds ago might not be used at all at the point in time when the source reacts to the congestion. Broadcasting in a wireless network suffers from a number of drawbacks [11]. If multiple nodes transmit at the same time, they cause destructive interference. This is known as a collision of the two messages at the given receiver. Because the possibility of collision requires each node to retransmit broadcast information

with a random delay. In spite of this random delay, collisions still occur, and the result may be a portion of the network not receiving a given broadcast message.

All studies on VANETs assume an optimal coordination of CSMA/CA medium access [85]. In an actual scenario, the attenuation of a transmitted signal is caused by phenomena like free-space loss (loss in signal strength resulting from a line-of-sight path through free space, with no obstacles), path loss (which is the attenuation caused by interferences due to reflections, diffractions or scattering between the radio waves and the environment) or fading (which is the attenuation caused by the movement of the environment relative to the sender). This can lead to unexpected strong loss in the power of the transmitted signal. Radio models are available that estimate these losses for the purpose of analysis [85]. Deterministic models (e.g. Two Ray Ground) estimate the average attenuation and predict a fixed attenuation for a given travelled distance. Probabilistic ones (e.g. Nakagami) are characterised by an attenuation variance, which estimates the variation over time of the average signal power at travelled distances.

From the discussions above, we can conclude that communication in VANETs are affected by factors like mobility, signal attenuation, congestion and collision. Any analysis or simulation of VANET communication should consider these aspects to obtain accurate results. Owing to the time restrictions associated with the completion of this work, this thesis does not consider detailed mobility or radio propagation models for protocol analysis. Nor are any advanced congestion reduction or retransmission schemes considered. Some of the values [72] used for analysis are derived from simulations done using a NS-2 simulator. The analysis in this thesis will be based on the assumptions made in 5.2.

6.2 Baseline Pseudonyms

A messaging protocol that relies on the concept of pseudonymous authentication, and termed Baseline Pseudonym (BP) is presented in [17, 63]. Each vehicle generate its own pseudonyms, in order to eliminate the need of pre-loading, storing and refilling pseudonyms and the corresponding private keys. This way, the burden of key and pseudonym management is greatly reduced; and so is the cost of obtaining the pseudonyms over off-line channels (specialised infrastructure, or 3G cellular link downloads). Self-generation of pseudonyms comes at a higher transmission and processing cost and overheads, which can be reduced by optimisation.

Each node V is equipped with a set of pseudonyms, which are certified public keys without any information identifying V. For the i^{th} pseudonym K_V^i for node V , the CA provides a certificate $Cert_{CA}(K_V^i)$, simply a CA signature on the public keyK_V^i (unlike the X.509 certificates) [17]. The node uses the private key k_V^i for the pseudonym K_V^i to

digitally sign messages. To enable message validation, the pseudonym and the certificate of the signer are attached in each message. With $\sigma_{k_V^i}()$ denoting V 's signature under its i^{th} pseudonym and m the signed message payload, the message format sent by V is:

$V \longrightarrow * : m, \sigma_{k_V^i}(m), K_V^i, Cert_{CA}(K_V^i)$

$*$ represents all the message receivers in the communication range of V. On receiving the message, with the public key of the CA assumed available, receiving node validates $Cert_{CA}(K_V^i)$, and then verifies the signature using K_V^i [17]. It makes use of a Certificate Revocation List (CRL), also assumed to be distributed to vehicles via the infrastructure [76]. If K_V^i is not included in the CRL and CA signature on K_V^i is valid, the node validates $\sigma_{k_V^i}(m)$. Each pseudonym is used at most for a period τ (pseudonym period) and then discarded. The CA maintains a map from the long-term identity of V to the $\{K_V^i\}$ set of pseudonyms provided to a node. If presented with a message, the CA can perform the inverse mapping and identify the signer.

6.3 Group Signature

[53] proposes an authentication protocol based on Group Signatures (GS) for V2V communication. The short group signature scheme that was introduced by Boneh et al. [14], which is secure and considered to be best suited to the V2V application is considered in [53]. GS is a stronger property than pseudonymous authentication, as any two group signatures generated by a node cannot be linked [17].

A verifier can judge whether the signer belongs to a group without knowing who the signer is in the group. However, in an exceptional situation, the CA can perform an *Open* operation [10] and reveal the signer's identity. Therefore, the group signature technique brings up a better way to meet the anonymity and traceability requirements rather than storing all the certificates in the terminal devices [53]. In addition GS scheme requires roles like membership manager (MM) for registering vehicles and assigning private keys and group public keys, a tracing manager (TM) to reveal ID of vehicles and ability to selectively revoke the group membership of a compromised vehicle either by updating keys or releasing revocation lists (RLs) [53].

During the vehicle's registration process, the MM generates a secret group signing key gsk_V, with the group comprising as members all vehicles registered with the MM. A group public key GPK_{CA} allows for the validation (by any node) of any group signature $\Sigma_{CA,V}(m)$ generated by a group member [53, 17]. A group signature scheme allows any node V to sign a message on behalf of the group without V's identity being revealed to

the signature verifier. Moreover, it is impossible to link any two signatures of a legitimate group member. Given a message m, vehicle V signs on m before sending it out. No public key or other credentials need to be attached to a message anonymously authenticated. The message format is:

$V \longrightarrow * : m, \Sigma_{CA,V}(m)$

Once a message is received, the receiver first checks if the time information in the message payload is in the allowable time window. If so, the receiving vehicle will perform signature verification. The short group signature scheme used in [53], is also used in [17]. Hence, for the analysis of [53], the GS computation costs and overheads given in [17] will be considered.

6.4 Hybrid Scheme

The authentication protocol based on Hybrid Signature (HS) scheme is a combination of BP and GS schemes [63, 17]. Each node V is equipped with a group signing key gsk_V and the group public key GPK_{CA} (total of vehicles registered with the CA). Rather than generating group signatures to protect messages, a node generates its own set of pseudonyms (according to the BP public key cryptosystem).

For HS, the CA does not provide a certificate on K_V^i ; V uses gsk_V to generate a group signature $\Sigma C_{A,V}(K_V^i)$ on each pseudonym K_V^i instead. V attaches $\Sigma C_{A,V}(K_V^i)$ to each message, and signs with the corresponding k_V^i to generate the following message format [63].

$V \longrightarrow * : m,\ \sigma_{k_V^i}(m),\ K_V^i, \Sigma C_{A,V}(K_V^i)$

When a node receives a message, the group signature $\Sigma C_{A,V}(K_V^i)$ is verified, using GPK_{CA}. If successful, the receiver infers that a legitimate group member generated pseudonym K_V^i . As per the properties of group signatures, the receiver/verifier of the certificate cannot identify V and cannot link this certificate and pseudonym to any prior pseudonym used by V . Once the legitimacy of the pseudonym is established, the validation of $\sigma_{k_V^i}(m)$ is done. To identify the message signer, an *Open* operation [10] on the $\Sigma C_{A,V}(K_V^i)$ group signature is done; message m is bound to K_V^i via $\sigma_{k_V^i}(m)$, and K_V^i is bound to V via $\Sigma C_{A,V}(K_V^i)$[17].

Optimisations are done to reduce protocol overheads. In the case of optimisation in HS [17], at the sender side, the $\Sigma C_{A,V}(K_V^i)$ is computed only once per K_V^i , because

$\Sigma C_{A,V}(K_V^i)$ remains unchanged throughout the pseudonym period τ. The sender appends $\Sigma C_{A,V}(K_V^i)$ to all messages. At the verifier's side the $\Sigma C_{A,V}(K_V^i)$ is validated upon the first reception and stored. For all subsequent receptions, if $\Sigma C_{A,V}(K_V^i)$ has already been verified, the receiver skips its validation. Optimised HS will be considered for performance analysis.

6.5 Performance Analysis

Primarily, the two scenarios, highway and congestion, introduced in 5.2 will be considered for performance analysis. The different parameter values of both scenarios are given in Table 6.1, derived from [72]. Value of message sizs are chosen to correspond to a maximum message size of 1100 bytes, as per the message range chosen in [72]. The minimum DSRC channel capacity of 6 Mbps for safety messages will be considered. The following parameters are defined for further use in performance analysis.

m =total message size (bytes)

s = safety message size (bytes)

o = cryptographic overheads (bytes)

T = System throughput (bytes per second)

n = number of vehicles in transmission range (number of messages received per beacon)

r = messaging rate (beacons per second) per vehicle

l = maximum allowable latency/beaconing interval (ms)

d = maximum tolerable processing delay per message (ms)

In both scenarios, as explained in [72], vehicles are mobile and transmit DSRC messages every l ms over the communication range. Considering a vehicle V located in the middle of the highway, which corresponds to a maximum of received messages; V can hear n vehicles per l ms. In the worst-case, where all vehicles contend for the channel, the system throughput is T, assuming the minimum nominal capacity of DSRC, which is 6 Mbps. Before V can send a new message, it should be able to process all incoming messages within l ms. It is assumed that V receives all the n messages (although the average reception rate [86] is smaller than 1, upper bound is assumed).

In a highway scenario, considering a single lane and a transmission range of 300 m, a vehicle in the centre of traffic will hear 10 vehicles/messages (transmission range divided by inter vehicle distance) from the front and 10 vehicles/messages from the rear (total 20 in each lane), per beacon. For six lanes, no of vehicles can be calculated as

$n = 20 \times 6 = 120$. Similarly, in a congestion scenario, n = 36 and r = 10 [72]. This has been calculated assuming a vehicle hears all traffic in its range (upper bounds).

Parameters	Highway scenario	Congestion scenario
Vehicle speed (miles/hour)	> 10	≤ 10
Messaging rate (beacons/second)	3.33	10
Messaging range	300	15
Maximum tolerable latency (ms)	300	100
Inter vehicle distance	30	5
Message size (bytes)	100, 200, 300, 400, 500, 600, 700, 800	100, 200, 300, 400, 500, 600, 700, 800
Radio system	5.9 GHz DSRC	5.9 GHz DSRC
Usable DSRC bandwidth (Mbps)	6	6
Number of lanes	6	6
Number of messages received	120 per 300 ms	36 per 100 ms

Table 6.1: Traffic scenario parameters and values

Since the chosen protocols need PKI and Group Signatures (GS) for implementing security in VANETs, it is important to choose a Public Key Cryptosystem (PKCS) and GS with an acceptable implementation overhead in the vehicular context. For the purpose of performance analysis in this chapter, Elliptic Curve Digital Signature Algorithm (ECDSA[1]) [2] and the group signature (GS) proposed by Boneh and Shacham [14] will be used (Table 6.2). These are the primitives used for cryptographic operations in BP, GS and HS [17, 53, 63].

Algorithm	Security level (bits)	Signing time (ms)	Verification time (ms)	Signature (bytes)	Public key (bytes)
ECDSA-192	80	0.5	3	48	25
ECDSA-256	128	3	4.2	64	33
GS	80	17.8	15.6	151	278
GS	128	53.7	49.3	225	800

Table 6.2: Signature algorithms - computation costs and overheads

According to DSRC, safety-related messages are sent with a periodicity of 100 to 300 ms. This imposes an upper bound on the processing time overhead; this overhead is given as follows [72]:

$$T_{oh}(M) = T_{sign}(M) + T_{tx}(M|Sig_{PrK_V}[M]) + T_{verify}(M) \quad (1)$$

[1] http://grouper.ieee.org/groups/1363/P1363a/index.html

where $T_{sign}(M)$, $T_{tx}(M|Sig_{PrK_V}[M])$, and $T_{verify}(M)$ are the necessary durations to sign, transmit, and verify a message M, respectively. From expression (1), we see that processing overhead depends on signing and verification of signatures. It is safe to assume that the critical processing overhead of a given PKCS is the signature verification time, since each vehicle will periodically receive several messages that it needs to verify while it has to sign and send only one message during the same period [72].

6.5.1 Computation Cost

All measurements were made on a Centrino machine with the clock speed set at 1.5 GHz; this is a close approximation for the CVIS[2] vehicle PC. For cryptographic primitives, the individual delays are shown for each operation in Table 6.2. The values in Table 6.2 will be followed for subsequent analysis in this section. The security levels (t) are assumed to be t = 80 bits for message signatures ($\sigma_{k_V^i}(m)$) in BP and t = 128 bits for certificate signatures in BP and GS ($Cert_{CA}(K_V^i)$ and $\Sigma_{CA,V}(m)$ respectively). The assumption is that high security is not necessary for the short-lived pseudonym in BP, although it is required for the long-term GS keys [17, 63].

For BP, a sender computes a $\sigma_{k_V^i}(m)$ for each message, and each receiver will validate one $\sigma_{k_V^i}(m)$ per message and one $Cert_{CA}(K_V^i)$ for each pseudonym [17]. From Table 6.2, the costs per message will be: 0.5 ms/message for signing, and 7.2 ms/message (3 ms to verify for verification of $\sigma_{k_V^i}(m)$ and 4.2 ms to verify certificate $Cert_{CA}(K_V^i)$). For GS, each vehicle will need to generate and verify one $\Sigma_{CA,V}(m)$ per message, either transmitted or received. This costs around 53.7 ms/message for signing and 49.3 ms/message for verification [17, 53].

In HS, the cost is one $\sigma_{k_V^i}(m)$ generation and verification per message and one $Cert_{CA}^H(K_V^i)$ generation and verification per pseudonym. The costs are 54.2 ms/message for signing (0.5 ms to generate $\sigma_{k_V^i}(m)$ and 53.7 ms to generate $Cert_{CA}^H(K_V^i)$), and 52.3 ms/message for verification (3 ms to verify $\sigma_{k_V^i}(m)$ and 49.3 ms to verify $Cert_{CA}^H(K_V^i)$). Considering optimisation, we assume τ = 60s. For HS, due to optimisation, we also have to take into account the highway and congestion scenarios to calculate the computing and message overheads [17].

Highway scenario: In this case $r = 3.33$, and $\tau = 60s$. During the pseudonym period, vehicle issues 60× 3.33≈200 messages. The signing costs include 54.2 ms/message for signing (0.5 ms to generate $\sigma_{k_V^i}(m)$ and 53.7 ms to generate $Cert_{CA}^H(K_V^i)$) the first

[2]The CVIS project, http://www.cvisproject.org/

message in the pseudonym period and 0.5 ms/message (0.5 ms to generate $\sigma_{k_V^i}(m)$) for the rest of the 200 messages till τ has expired. The verifying costs include 52.3 ms/message for verifying (3 ms to verify $\sigma_{k_V^i}(m)$ and 49.3 ms to verify $Cert_{CA}^H(K_V^i)$) the first message in the pseudonym period and 3 ms/message (3 ms to verify $\sigma_{k_V^i}(m)$) for the rest of the 200 messages. Therefore, average signing cost per message during τ is ((0.5 + 53.7)+(0.5×199 messages))/(200 messages) ≈0.8 ms. Average verifying cost is ((3 + 49.3)+(3×199 messages))/(200 messages) ≈3.25 ms.

Congestion scenario: Here $r = 10$, and $\tau = 60s$. During the pseudonym period, vehicle issues 60× 10 =600 messages. Average signing cost per message during τ is ((0.5 + 53.7)+(0.5×599 messages))/(600 messages) ≈0.6 ms. Average verifying cost is ((3 + 49.3)+(3×599 messages))/(600 messages) ≈3.1 ms. The computation costs for BP, GS and optimised HS are displayed in Table 6.3.

Authentication scheme	Signing time (ms)	Verification time (ms)	Message overhead (bytes)
BP	0.5	3	137
GS	17.8	15.6	225
HS optimised (highway scenario)	0.8	3.25	298
HS optimised (congestion scenario)	0.6	3.1	298

Table 6.3: Processing costs for authentication schemes

6.5.2 Cryptographic Overhead

Cryptographic overhead is the additional data in bytes that is added to the original message due to cryptographic operations. The message overheads for different authentication schemes are given in Table 6.3 [17]. For BP, K_V^i and $Cert_{CA}(K_V^i)$ are 89 bytes. Along with $\sigma_{k_V^i}(m)$ (48 bytes (Table 6.2)), the overhead is 137 bytes per message. For GS, the overhead is $\Sigma_{CA,V}(m)$ (225 bytes per message (Table 6.2)). For Hybrid, the overhead is $\sigma_{k_V^i}(m)$, K_V^i and $Cert_{CA}(K_V^i)$, in total 298 bytes per message [17].

6.5.3 Total Message Size vs. Throughput

The system throughput in the case of a VANET can be defined as the bandwidth currently demanded by vehicular communication in the communication channel. It can be calculated as follows [72].

$$T = \frac{n \times r \times m \times 8}{1024 \times 1024} \, Mbps$$

(2)

The total message size $m = s + o$. For e.g. in BP m=s+137 bytes (Table 6.2). In GS scheme, the overhead m=s+225 bytes. In Hybrid scheme, m = s + 298 bytes [17]. To analyse the effect of message size on throughput, different message sizes has been chosen (Table 6.1). The different values of s are substituted in equation 2 for highway (n=120, r=3.33) and congestion (n=36, r=10) scenarios. Table 6.4 gives the different throughput values (equation 2) for different message sizes under different authentication schemes .

	Message size (s)							
	100	200	300	400	500	600	700	800
Throughput (Mbps) (BP, highway scenario)	0.72	1	1.33	1.63	1.94	2.24	2.55	2.85
Throughput (Mbps) (GS, highway scenario)	0.99	1.29	1.6	1.9	2.21	2.51	2.82	3.12
Throughput (Mbps) (HS, highway scenario)	1.21	1.51	1.82	2.12	2.43	2.73	3.04	3.34
Throughput (Mbps) (BP, congestion scenario)	0.65	0.92	1.2	1.47	1.74	2.02	2.2	2.57
Throughput (Mbps) (GS, congestion scenario)	0.89	1.16	1.44	1.71	1.99	2.26	2.54	2.81
Throughput (Mbps) (HS, congestion scenario)	1.09	1.36	1.64	1.91	2.19	2.46	2.74	3.01

Table 6.4: Message size vs. System throughput for different authentication protocols

From Table 6.4 can be seen that the throughput increases linearly with message size. Safety message sizes are of the order of 100-500 bytes [88, 82, 53, 77, 68, 8]. Assuming HS (maximum overhead≈300), a maximum message size of 500 bytes (total message size of 800 bytes) and highway scenario (this scenario demands the maximum throughput), the throughput is 3.35 Mbps. This is well below the minimum 6 Mbps wireless bandwidth of DSRC even assuming upper bounds. Hence, as far as throughput is concerned, the three protocols work well for the selected applications.

In practical scenarios, the throughput does not increase linearly with message size. One of the reasons is that with increase in message size, there is a drop in number of messages received. [72] shows by simulation that for a total message size of 800 bytes (message size=500 bytes, assuming HS), messages received per second ($n \times r$) is 75 for highway

scenario and 60 messages per second for congestion scenario, which is well below the value of n in Table 6.1 . With these values of $n \times r$, the throughput of HS calculated from equation (2) becomes 0.46 Mbps (highway scenario) and 0.37 Mbps (congestion scenario). Thus we can see that practical values are much less than the upper bound calculated in Table 6.4.

There is a drastic drop (roughly 20-25 messages/sec for every 100 byte increase in total message size) in the number of received messages after 300 bytes, and it slowly stabilises with increase in message size until 1000 bytes [72]. At the same time throughput increases drastically with message size until 300 bytes, after which it stabilises until 1000 bytes . Considering the selected applications in Table 3.2, we see that the minimum message size varies from 35-60 bytes. Assuming a safety message size of 100 bytes [53, 8], BP gives a total message size of 237 bytes, GS gives 325 bytes and HS gives a total message size of 398 bytes. Hence HS has maximum impact on message losses and throughput.

From the simulation results in [72], we see that a total message size of 100-300 bytes is ideal for safety messaging (drastic message losses after 300 bytes). HS already has an overhead of 298 bytes, and the total message size will easily exceed 300 bytes. For a given message size, the best option for authentication scheme to minimise message losses and reduce throughput is BP.

6.5.4 Total Message Size vs. Message Delay

Message delay is the time taken to deliver the message from sender to receiver. According to [72], the average message delay does not vary considerably when the message size increases because the low contention on the medium and the high transmission rate minimise the effect of the message size. In different scenarios, the maximum message delay incurred can be roughly estimated as follows [72].

Total message size (bytes)	Maximum message delay (ms) (highway scenario)	Maximum message delay (ms) (congestion scenario)
100	*20*	*20*
200	*30*	*30*
300	*40*	*42*
400	*42*	*50*
500	*50*	*52*
600	*60*	*48*
700	*50*	*48*
800	*50*	*48*

Table 6.5: Message size vs. Message delay

Table 6.3 was compiled for digital signatures using ECDSA (28 bytes) [72]. From a total message size of 300-400 bytes, the average message delay does not vary much, in both scenarios. Considering the applications listed in Table 3.2, the maximum allowable latency is 20 ms for pre-crash sensing and 100 ms for other applications (lane change, cooperative forward collision warning, electronic break lights). Referring to Table 6.5, in both scenarios, the average message delay corresponds to 20 ms which is the upper bound for latency in pre-crash sensing.

For pre-crash sensing, assuming a message size of 100 bytes [8, 53] and overhead of 137 bytes (BP), the total message size goes to 237 bytes. From Table 6.5 this corresponds to a maximum message delay of between 30 and 40 ms (we can assume more or less the same delay as BP uses ECDSA signature (48 bytes)). According to the application requirements of pre-crash sensing the maximum allowable latency cannot go above 20 ms. The use of even BP with pre-crash sensing for authentication becomes really challenging. Lower message sizes and smaller signature sizes will have to be considered for pre-crash sensing. Other authentication schemes (GS and HS) are associated with even more message delays due to larger total message sizes (larger signature sizes).

For other applications in Table 3.2, the maximum allowable latency is 100ms. The values given in Table 6.5 falls well below this upper bound. Assuming similar message delay values for BP, GS and HS, these schemes can be used for the three remaining applications in Table 3.2.

6.5.5 Messaging Rate vs. Processing Delay

Processing delay per message can be defined as the time taken by a vehicle to verify each message it receives. The processing delay varies with the messaging rate as shown below [72].

$$d = \frac{l}{n}$$

- *Highway scenario:* In this case latency=300 ms and number of vehicles n=120 (Table 6.1). Therefore maximum tolerable processing delay=300/120=2.5 ms. Now, each vehicle has maximum 2.5 ms to process a message between consecutive messages.
- *Congestion scenario:* Here latency=100 ms and number of vehicles n=36. Therefore maximum tolerable processing delay=100/36=2.78 ms. Each vehicle has maximum of 2.78 ms to process a message.

From the table, for BP, GS and HS (highway) schemes, the overheads are 3 ms, 15.6 ms and 3.25 ms, which is above the maximum tolerable delay (here e have assumed vehicles receive all messages from neighbours). GS is nowhere close to being used for the selected applications. In real life scenarios, a vehicle won't hear all the neighbours in it's range because of losses [86]. From the simulation in [72], it can be understood that the average actual processing delays for a total message of size 800 bytes are around 1s/75msg = 13.33 ms in highway scenario and 1s/60msg = 16.67 ms in congestion scenario. For message sizes between 100-300 bytes, it is 5.5 ms and 8 ms for highway and congestion scenarios respectively. Referring to Table 6.3, it can be seen that the verification times of BP and HS are well below those of 800 bytes and 10-300 bytes. GS falls on the border of upper bound verification value for 800 bytes, and needs faster algorithms or faster platforms to support lower message sizes (100-300 bytes) .

Another very promising candidate for PKCS in BP and HS is NTRU[3] [72]. It gives a signing time of 1.587 ms and verification time of 1.488 ms, calculated on a Pentium II platform (Table 6.2 calculations are based on a Centrino 1.5 GHz platform). Thus it can be noticed that NTRU signatures meet the maximum tolerable processing delay requirements, and will perform even better on modern platforms. BP, HS are authentication schemes that can be comfortably used for applications listed in Table 3.2. The signature verification delay associated with GS makes it unsuitable for safety-critical communication (until GS algorithms that can be compute faster or faster platforms than Centrino 1.5 GHz are available). Processors faster than Centrino 1.5 GHz are already available in market.

6.6 Security Analysis

To do a security analysis of the protocols identified in 6.1, we refer to the VANET applications identified in Table 4.1. In BP, GS and HS, the authentication of the sender is done by verifying the sender signature using sender public key (pseudonym K_V^i in HP and BP, group public key GPK_{CA} in GS). Use of digital signatures provide authentication and integrity, and prevents masquerade attacks. The public key does not give any ID information of sender, but is certified by the CA, which in turn authenticates the sender public key. Assuming the property identification of sender is included in the certificate provided by CA, property authentication of the message can be provided. None of the protocols (BP, GS or HS) provides location authentication; there is no way to verify if the received location information is correct.

Entity authentication is provided by the time stamps included in the message signa-

[3] http://www.ntru.com/

ture. Time stamps used with signatures in messages guarantees message freshness and provide protection against replay attacks. In BP, GS and HS, since the ID of any sender is not revealed in the public keys, it is not possible to trace ID of the vehicle or the owner. In BP, pseudonyms are changed frequently in a way that no two messages signed by different pseudonyms can be linked. Pseudonyms do not provide privacy if vehicle is in a monitored area [16]. GS provides a stronger version of privacy where any two group signatures by a node cannot be linked. Hence GS protocol provides stronger ID privacy than BP or HS. Ideally, applications require the privacy of GS and efficiency of BP. Auditability can be provided in the case of these three protocols, by approaching the CA who links the public key to ELP and the ELP can be linked to the owner of the vehicle.

If a node sends a forged message (with false position or false sensor values), BP, HS and GS do not provide methods to detect it. Integrity only provides a way of detecting the changes in data during message transit. Availability of the system is something that cannot be fully guaranteed. The primary vulnerability lies in wireless channel open to jamming attacks. DoS attacks against individual nodes can be realised by sending too many messages to it, giving it not enough time to process valid messages. Availability is determined to a great extent by the secure routing protocols in VANETs, securing and guaranteeing message delivery to destination. Detection and prevention of DoS also requires mechanisms like intrusion detection and prevention. The physical security of HSM is the underlying factor that ensures the valid use of keys. Without an adequately protected HSM, keys can be compromised.

7 Conclusion

As we have seen, the large number of nodes, high vehicle speeds, rapidly changing topology, varying node densities, and low message latencies are the main factors that shape the performance of a VANET. In this thesis, vehicular applications were classified, the importance of security in safety-critical applications were explained and the security architecture of safety-critical applications were elaborated. The main intent of the thesis was to study the impact of cryptographic overheads, total message size, and messaging rate on efficiency of secure communication protocols, for V2V safety-critical applications..

7.1 Contributions

In Chapter 6, apart from the applications selected in Table 32, three authentication protocols (BP, GS and HS) were also selected for analysis and their cryptographic computation costs and overheads were noted. In HS, the computation costs and overheads varies with messaging rate and pseudonym lifetime. Hence, assuming pseudonym lifetime = 60 s, computation costs and overheads were calculated for HS; in highway and congestion scenarios. The whole idea was to identify the ideal communication parameters for safety-critical applications and to study the suitability of BP, GS and HS protocols. From the analysis of these protocols conducted in Chapter 6, the following conclusions were reached.

- The optimum total message size for safety-critical applications should be between **100 and 300 bytes** in order to ensure optimum communication system performance.
- For the ideal total message size of 100-300 bytes, the maximum tolerable message processing delay was found to be **5.5 ms** for highway scenario and **8 ms** for congestion scenario.
- Any authentication protocol that has a total message size between 100 and 300 bytes and does signature verification in 5.5 ms (highway scenario) and 8 ms (congestion scenario) is an ideal candidate for safety-critical applications.
- To support all safety-critical applications (Table 3.2), there should be an average message delay of less than **20 ms** for the ideal total message size of 100-300 bytes.

- It is meaningless to have sender authentication and not have data authentication (verification of position data and other sensor data) for safety-critical applications.

7.1.1 Total Message Size

- The optimum total message size for safety-critical applications should be between **100 and 300 bytes** in order to ensure optimum communication system performance.

In the analysis of protocols on Chapter 6, it was noticed that the actual number of messages received per second by a node is less than 50% of the theoretical value (400 messages/sec for highway and 360 messages/sec for congestion). Nodes receive maximum messages in both scenarios, when the total message size is 100-300 bytes, and after that the reception rate drops drastically. The average message delay increases from a minimum of 20 ms at 100 bytes until 400 bytes, in both scenarios, and stabilises at 50 ms after 400 bytes. Similarly message throughput increases from 100 bytes to 400 bytes and stabilises afterwards. The maximum possible throughput is still 0.5 Mbps, well below DSRC minimum of 6 Mbps. From these observations, it can be inferred that the ideal total message size for safety-critical applications should be between **100 and 300 bytes** in order to ensure maximum reception, minimum message delay and minimum throughput.

7.1.2 Message Processing Delay

- For the ideal total message size of 100-300 bytes, the maximum tolerable message processing delay was found to be **5.5 ms** for highway scenario and **8 ms** for congestion scenario.

In highway scenario, for the total message size of 100-300 bytes, the total messages received/node/sec is 180, which is the maximum reception. [72]. Similarly it is 125 in congestion scenario. Therefor maximum processing delay is 1/180=5.55 ms and 1/125=8 ms for highway and congestion scenarios respectively.

7.1.3 Message Delay:

- To support all safety-critical applications, there should be an average message delay of less than 20 ms for the ideal total message size of 100-300 bytes.

For both highway and congestion scenarios, in Table 6.5, the minimum message delay is 20 ms. This makes the communication system unsuitable for pre-crash sensing application identified in Table 3.2, which has a maximum allowable latency of only 20 ms, and demands a latency less than this upper limit. This means for a feasible total message

size between 100-300 bytes, we should have a message delay less than 20 ms to support applications like pre-crash sensing. The message delay can be brought down by reducing message size or by using improved wireless media access schemes [89]. For the other applications in Table 3.2, the message delay stays well below their maximum tolerable latency (100 ms) for 100-300 bytes.

7.1.4 Performance Analysis:

- Any authentication protocol that has a total message size between 100 and 300 bytes and does signature verification in 5.5 ms (highway scenario) and 8 ms (congestion scenario) is an ideal candidate for safety-critical applications.

From the performance analysis of the three protocols, for GS and HS itself, the cryptographic overheads are 225 bytes and 298 bytes respectively. This means that for even the minimum of safety message sizes, total message sizes in GS and HS touch the upper limit (300 bytes) of optimum total message size. This affects system performance. In the case of BP, optimum system performance can be obtained upto 160 bytes of message payload. Considering message processing delay, BP and HS (in both scenarios) meet the maximum tolerable message processing delay constraints (Table 6.3). GS, taking into account the Centrino 1.5 GHz platform and algorithm [14] under consideration, does not meet the processing delay constraints. GS could meet the requirements if it works on a signature algorithm and/or platform that provides computation capabilities at least 4 times faster than what is considered in the thesis. The preferred protocols in this case are BP and HS. BP and HS can work better on faster signature algorithms like NTRU.

7.1.5 Security Analysis

- It is meaningless to have sender authentication and not have data authentication (verification of position data and other sensor data) for safety-critical applications.

In security analysis, it was noticed that BP, GS or HS could not provide location authentication (verifying sender location) and availability to the applications identified in Table 4.1. Therefore, applications remain vulnerable to attacks like forgery and wormhole, due to the inability of nodes to verify received information. But the protocols provide properties like authentication, integrity, entity authentication, id privacy and auditability. The anonymous public key (signed by the CA) is used by the receiver to authenticate the sender, and provides privacy, as vehicle details are not present in the certificate. Pseudonyms (BP and HS) [16] do not provide the strong privacy offered by GS. Auditability is provided when upon request from proper authorities, the CA maps the anonymous public key to the vehicle ELP. Registration authorities then map ELP to the vehicle owner.

7.2 Open Issues

These involve the issues that were identified in the analysis of protocols in Chapter 6. Solution to these issues either require a different approach towards solution or are topics of ongoing research efforts. These issues need to be addressed for a VANET system to be successfully tested and deployed.

7.2.1 Assumptions

For protocol analysis, the mobility patterns that were assumed were very simple; vehicles moving in same direction, with the same speed, always separated by same distance, broadcasting at the same time. Practically vehicles move in same an opposite directions, at different speeds, maintain different spacing between them, change lanes and broadcast randomly. In an ideal scenario, for purpose of analysis and simulation, a practical VANET mobility model has to be considered along with a suitable radio propagation model [86], that can be validated. This will give more accurate results for the analysis compared to simple assumptions.

7.2.2 Flexibility

With improvement in technology, protocols and cryptographic primitives change. Since VANET applications are delay sensitive and bandwidth constrained, such improvements in technology demand fast implementations, as they will considerably improve VANET performance. It is important that nodes have the facility to quickly switch and adapt to new technologies, unlike other wireless applications.

7.2.3 Sensor Manipulation

Assuming the HSM is tamper resistant, safety of private keys are assured. But it doesn't prevent the manipulation of sensor data (like speed, throttle position, position etc) by owner to disseminate false data into the VANET. This could be for malicious purposes or to avoid accountability after a hit and run. As long as the data authentication feature is not available in VANETs, manipulation of sensor data can cause serious issues.

7.2.4 Privacy

The considered mechanisms for authentication and privacy in this thesis are BP, GS and HS. However, the BP mechanism has some limitations. It might still be possible to fully track vehicles between pseudonym changes [16]. Increasing the frequency of changes can

help, but also increases the incurred overhead. Group signatures are a promising; but require faster signature algorithms and platforms, as explained in 7.1.4. Research efforts should address attacks against privacy at any layer of the communication stack [46].

7.2.5 Revocation

The problems with malicious nodes is that they launch attacks in the VANET system and can cause revocation of benign nodes. As long as vehicles get live updates from surrounding nodes on malicious nodes, certificate revocation of malicious nodes is not time-critical. In the absence of such a mechanism, the revocation of malicious nodes from the network become time-critical, since they need to be removed from the network before they can wreak more havoc in the system. Main issue facing revocation is that fact that nodes are not in continuous communication with CA. Details on some of the current research addressing this topic are available in [75, 58, 74]

7.2.6 Data Verification

We should not only verify that the sender of the data is legitimate, but also that the data in itself is legitimate (e.g., safety warnings, traffic information, their freshness and location relevance). Wrong data leads to attacks, failure of VANET applications and possibly accidents. Even though the sender of the data may not necessarily be malicious, but vehicle's sensors may be malfunctioning. Trying to interact with possibly adversarial (faulty) data senders to determine their trustworthiness is hard: encounters are in general short-lived and have no prior associations. Dedicated research is going on to address verification of position information and other data (speed, acceleration etc) in MANETs [35, 78, 33, 83].

7.2.7 Availability

Challenges to availability can cause users to lose confidence in the system. The availability of a VANET system is challenged at all layers; jamming at physical layer, DoS attacks at MAC and upper layers. VANETs use complex information dissemination methodologies like efficient flooding, context-adaptive message dissemination, as well as data aggregation which are essentially efficient and secure means of routing information [80, 71]. Denial of service (DoS) is still possible, in-spite of the presence of cryptographic security mechanisms higher layer protocols. Detection and prevention (rate checks, consistency checks etc) of intrusions in VANETs is explored in [81].

7.2.8 Non-Technical Aspects

The biggest problem with VANETs is the sheer size of it; assuming worldwide and total adoption, a vehicular network would have millions off nodes. Such a network should have a very low tolerance for errors, and would also be a heterogeneous network at large (different countries will follow different standards, infrastructure, laws and implementations). Coordination in such a network is difficult to be achieved, for example, in the case of PKI. Law enforcement agencies would like to have total access to the transmitted information (e.g. to immediately fine violators of speed limits), while drivers would surely reject that. Also, initially only a small number of vehicles are expected to be part of such networks, making safety or other applications less effective [84].

7.3 Future Work

This work focused on finding the optimum total message length, average message delay and maximum processing delay for safety-critical applications, identified as the performance requirements of VANET messaging system. Secure communication protocols were chosen to analyse, apart from their security aspects, their suitability in adhering to the performance requirements mentioned above. Owing to the time constraints, the performance and security analysis of protocols were conducted based on observations in previous works [72].

The future work in this line would include identifying suitable mobility and radio propagation models for highway and congestion scenarios, and conducting simulations to understand the impact of total message size on message delay, throughput and message reception. Based on these simulation values, we can arrive at the optimum total message size and minimum processing delay for V2V safety-critical applications. Moreover the performance of communication protocols used for applications like platooning, having multiple protocol runs, can be analysed.

Bibliography

[1] The network simulator - ns-2. http://www.isi.edu/nsnam/ns/.

[2] IEEE 1363a 2004. IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques, 2004.

[3] 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.

[4] IEEE Draft P802.11p/D2.0, November 2006. Wireless Access in Vehicular Environments (WAVE).

[5] CAR 2 CAR Communication Consortium Manifesto version 1.1. Technical report, CAR 2 CAR Communication Consortium (C2C-CC), Aug 2007. Available through http://www.car-to-car.org/. Last accessed: Aug 2009.

[6] IEEE Draft P1609.0/D01, February 2007. IEEE Trial-Use Standards for Wireless Access in Vehicular Environments (WAVE).

[7] 5.9 GHz Noth American DSRC, Last accessed: Aug 2009. http://grouper.ieee.org/groups/scc32/dsrc.

[8] Crash Avoidance Metric Partnership. Vehicle Safety Communication Project Final Report, Aug 2009. Available through U.S. Department of Transportation.

[9] Dedicated Short Range Communications (DSRC), Last accessed: Aug 2009. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm.

[10] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. pages 136–153. Springer-Verlag, 2004.

[11] Edoardo S. Biagioni. CollisionFree Broadcasting in Wireless AdHoc Networks using Cooperative Diversity. Information and Computer Sciences, University of Hawai, April 2007.

[12] Kathrin Bilstrup. A Survey Regarding Wireless Communication Standards Intended for a High-Speed Vehicle Environment. Technical report, School of Information Science, Computer and Electrical Engineering, Halmstad University, Sweden, Feb 2007.

[13] J. J. Blum, A. Eskandarian, and L. J. Hoffman. Challenges of Intervehicle Ad Hoc Networks. *Intelligent Transportation Systems, IEEE Transactions on*, 5(4):347–351, 2004.

[14] Dan Boneh and Hovav Shacham. Group Signatures with Verifier-Local Revocation. In *Proceedings of CCS 2004*, pages 168–177. ACM Press, 2004.

[15] Josh Broch, David A. Maltz, David B. Johnson, Yih chun Hu, and Jorjeta Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. pages 85–97, 1998.

[16] L. Buttyan, T. Holczer, and I. Vajda. On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs. In *European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2007)*, July 2007.

[17] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. Efficient and Robust Pseudonymous Authentication in VANET. In *Proceedings of the ACM International Workshop on Vehicular Ad hoc Networks (VANET)*, pages 19–28, September 2007.

[18] Srdjan Capkun, Levente Buttyán, and Jean-Pierre Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 2:52–64, 2003.

[19] David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[20] David Chaum and E van Heyst. Group Signatures. *EUROCRYPT*, pages 257–265, 1991.

[21] Imrich Chlamtac, Marco Conti, and Jennifer J Liu. Mobile Ad Hoc Networking: Imperatives and Challenges. *Ad Hoc Networks*, 1(1):13–64, Jul 2003.

[22] Y Do, S Buchegger, T Alpcan, and J P Hubaux. Centrality Analysis in Vehicular Networks. Technical report, 2008.

[23] John R. Douceur. The Sybil Attack. In *IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 251–260, London, UK, 2002. Springer-Verlag.

[24] Florian Dötzer. *Privacy Issues in Vehicular Ad Hoc Networks* , volume 3856/2006 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, Jun 2006.

[25] Florian Dötzer, Markus Straßberger, and Timo Kosch. Classification for traffic related inter-vehicle messaging. In *5th International Conference on IST Telecommunication*. BMW Group Research and Technology, Germany, Jun 2005.

[26] S. Eichler. Performance Evaluation of the IEEE 802.11p WAVE Communication Standard. *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pages 2199–2203, Oct 2007.

[27] Stephan Eichler. Security Challanges in MANET-based Telematics Environments. In *Proceedings of the 10th Open European Summer School and IFIP WG 6.3 Workshop*, Jun 2004.

[28] Stephan Eichler, Florian Dötzer, Christian Schwingenschlögl, Jörg Eberspächer, and Francisco Javier Fabra Caro. Secure Routing in a Vehicular Ad Hoc Network. In *Proceedings of the 2004 IEEE 60th Vehicular Technology Conference*, Sep 2004.

[29] Knut Evensen. Global Co-operation. In *ETSI TC ITS WORKSHOP*, Sophia, Antipolis, Feb 2009.

[30] A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch. NoW - Network on Wheels: Project Objectives, Technology and Achievements. In *Proceedings of 6th International Workshop on Intelligent Transportation (WIT 2008)*, Hamburg, Germany, Mar 2008.

[31] Andreas Festag, Holger Füßler, Hannes Hartenstein, Amardeo Sarma, and Ralf Schmitz. FleetNet: Bringing Car-to-Car Communication into the Real World. In *Proceedings of 11th World Congress on ITS, Nagoya, Japan*, Oct 2004.

[32] James A. Freebersyser and Barry Leiner. A DoD perspective on Mobile Ad Hoc Networks. *Ad Hoc Networking*, pages 29–51, 2001.

[33] Julien Freudiger, Maxim Raya, and Jean-Pierre Hubaux. Towards Self-Organized Location Privacy in Mobile Networks. Technical report, 2008.

[34] Matthias Gerlach, Andreas Festag, Tim Leinmuller, Gabriele Goldacker, and Charles Harsch. Security Architecture for Vehicular Communication. 2008.

[35] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in vanets. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37, New York, NY, USA, 2004. ACM.

[36] Zygmunt J. Haas, Joseph Y. Halpern, and Li Li. Gossip-Based Ad Hoc Routing. *IEEE/ACM Trans. Netw.*, 14(3):479–491, 2006.

[37] Charles Harsch, Andreas Festag, and Panagiotis Papadimitratos. Secure Position-Based Routing for VANETs. In *2007 IEEE 66th Vehicular Technology Conference (VTC 2007).*

[38] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An Overview of Mobile Ad Hoc Networks: Applications and Challenges. *The Communications Network*, 3(3), 2004.

[39] Y. C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. volume 3, pages 1976–1986 vol.3, 2003.

[40] Yih-Chun Hu and Kenneth P. Laberteaux. Strong VANET Security on a Budget. In *In Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, 2006.

[41] Jean-Pierre Hubaux, S. Capkun, and Jun Luo. The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy Magazine*, 2(3):49–55, 2004.

[42] M Jakobsson, XiaoFeng Wang, and S. Wetzel. Stealth Attacks in Vehicular Technologies. *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, 2:1218–1222, Sep 2004.

[43] Moez Jerbi, Rabah Meraihi, Sidi-Mohammed Senouci, and Yacine Ghamri-Doudane. An Improved Vehicular Ad Hoc Routing Protocol for City Environments. *IEEE International Conference on Communications (ICC '07)*, pages 3972–3979, 2007.

[44] Daniel Jungels, Imad Aad, Maxim Raya, and Jean-Piere Hubaux. Certificate Revocation in Vehicular Ad Hoc Networks. Technical report, EPFL, 2006.

[45] Mohamed Kafsi, Panos Papadimitratos, Olivier Dousse, Tansu Alpcan, and Jean-Pierre Hubaux. VANET Connectivity Analysis. In *IEEE Workshop on Automotive Networking and Applications (Autonet)*.

[46] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. *IEEE Communications Magazine*, 46(11):110–118, 2008.

[47] Frank Kargl, Zhendong Ma, and Elmar Schoch. Security Engineering for VANETs. In *4th Workshop on Embedded Security in Cars (escar 2006)*, Berlin, Germany, 11/2006 2006.

[48] Rainer Kroh, Antonio Kung, and Frank Kargl. VANETS Security Requirements Final Version. Technical report, Secure Vehicle Communication (Sevecom), Sep 2006. Available at http://www.sevecom.org/Pages/ProjectDocuments.html. Last accessed Aug 2009.

[49] Christine Laurendeau and Michel Barbeau. *Threats to Security in DSRC/WAVE*, volume 4104 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, Jul 2006.

[50] Tim Leinmüller, Robert K. Schmidt, Bert Böddeker, Roger W. Berg, and Tadao Suzuki. A Global Trend for Car 2 X Communication, 2007.

[51] Tim Leinmueller, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Rainer Kroh, Panagiotis Papadimitratos, Maxim Raya, and Elmar Schoch. SEVECOM - Secure Vehicle Communication. 2006.

[52] Tim. Leinmuller, Elmar. Schoch, and Christian. Maihofer. Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks. *Fourth Annual Conference*

on Wireless on Demand Network Systems and Services (WONS '07)., pages 84–91, Jan 2007.

[53] X. Lin, X. Sun, P.-H. Ho, and X. Shen. GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications. *Towards a Security Architecture for Vehicular Ad Hoc Networks.*

[54] Jun Luo and Jean-Pierre Hubaux. A Survey of Inter-Vehicle Communication. Technical report, 2004.

[55] Xiaomin Ma, Xianbo Chen, and Hazem H. Refai. Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis. *EURASIP J. Wirel. Commun. Netw.*, 2009:1–13, 2009.

[56] A. Mahajan, N. Potnis, K. Gopalan, and A. Wang. Urban Mobility Models for VANETs. In *Proc. of 2nd Workshop on Next Generation Wireless Networks*, 2006.

[57] K. Matheus, R. Morich, I. Paulus, C. Menig, A. Lübke, B. Rech, and W. Specks. Car-to-Car Communication-Market Introduction and Success Factors. In *ITS 2005: 5th European Congress and Exhibition on Intelligent Transport Systems and Services*, Jun 2005.

[58] Tyler Moore, Maxim Raya, Jolyon Clulow, Panagiotis (Panos) Papadimitratos, Ross Anderson, and Jean-Pierre Hubaux. Fast Exclusion of Errant Devices from Vehicular Networks. In *IEEE SECON 2008*, 2008.

[59] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu. The broadcast storm problem in a mobile ad hoc network. In *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, pages 151–162, New York, NY, USA, 1999. ACM.

[60] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communications Magazine*, 46(11):100–109, 2008.

[61] Panagiotis Papadimitratos, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Antonio Kung, and Maxim Raya. Architecture for Secure and Private Vehicular Communications. In *The 7th International Conference on ITS Telecommunications (ITST)*, 2007.

[62] Panagiotis Papadimitratos, Virgil Gligor, and Jean-Pierre Hubaux. Securing Vehicular Communications - Assumptions, Requirements, and Principles. In *Workshop on Embedded Security in Cars (ESCAR) 2006*, pages 5–14, 2006.

[63] Panagiotis (Panos) Papadimitratos, Giorgio Calandriello, Jean-Pierre Hubaux, and Antonio Lioy. Impact of Vehicular Communications Security on Transportation Safety. In *IEEE INFOCOM MOVE 2008.*

[64] Panagiotis (Panos) Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux. Certificate Revocation List Distribution in Vehicular Communication Systems. In *The Fifth ACM International Workshop on VehiculAr Inter-NETworking (VANET 2008)*.

[65] Panos Papadimitratos and Jean-Pierre Hubaux. Report on the "Secure Vehicular Communications: Results and Challenges Ahead" Workshop. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, 12(2):53–64, 2008.

[66] Bryan Parno and Adrian Perrig. Challenges in Securing Vehicular Networks. In *Proceedings of Workshop on Hot Topics in Networks (HotNets-IV)*, November 2005.

[67] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA broadcast authentication protocol. *Cryptobytes*, 5(2), 2002.

[68] Klaus Plößl and Hannes Federrath. A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks. *Computer Standards & Interfaces*, 30(6):390 – 397, 2008. Special Issue: State of standards in the information systems security area.

[69] Y. Qian and N. Moayeri. Design of Secure and Application-Oriented VANETs. In *Vehicular Technology Conference*, pages 2794–2799. VTC Spring 2008, IEEE, 2008.

[70] Sandro Rafaeli and David Hutchison. A Survey of Key Management for Secure Group Communication. *ACM Comput. Surv.*, 35(3):309–329, September 2003.

[71] Maxim Raya, Adel Aziz, and Jean-Pierre Hubaux. Efficient secure aggregation in VANETs. In *VANET 2006*, 2006.

[72] Maxim Raya and Jean-Pierre Hubaux. The Security of Vehicular Ad Hoc Networks. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21, New York, NY, USA, 2005. ACM.

[73] Maxim Raya and Jean-Pierre Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, 15(1):39 – 68, 2007.

[74] Maxim Raya, Mohammad Hossein Manshaei, Mark Felegyhazi, and Jean-Pierre Hubaux. Revocation Games in Ephemeral Networks. In *ACM CCS 2008*, 2008.

[75] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and Jean-Pierre Hubaux. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, 25(8):1557–1568, 2007.

[76] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing Vehicular Communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, 13(5):8–15, 2006.

[77] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing Vehicular Networks. 2006.

[78] Maxime Raya, Panagiotis (Panos) Papadimitratos, Virgil Gligor, and Jean-Pierre Hubaux. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In *IEEE Infocom 2008*, 2008.

[79] P. Samuel. Of Sticker Tags and 5.9 GHz. In *ITS International*, 2004.

[80] Elmar Schoch, Frank Kargl, Michael Weber, and Tim Leinmuller. Communication Patterns in VANETs. *IEEE Communications Magazine*, 46:119–125, Nov 2008.

[81] Elmar Schoch, Moritz Keppler, Frank Kargl, and Michael Weber. On the Security of Context-Adaptive Information Dissemination. *Security and Communication Networks*, 1(3):205–218, 2008.

[82] Michael Shulman and Richard Deering. Vehicle Safety Communications in the United States. Technical report, Ford Motor Company, General Motors Corporation, 2006.

[83] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung. Secure Location Verification for Vehicular Ad-Hoc Networks. *IEEE Global Telecommunications Conference (IEEE GLOBECOM 2008)*, pages 1–5, 2008.

[84] A. Stampoulis and Z. Chai. Survey of Security in Vehicular Networks. Technical report, 2007. Project CPSC 534.

[85] Marc Torrent-Moreno, Steven Corroy, Felix Schmidt-Eisenlohr, and Hannes Hartenstein. Ieee 802.11-based one-hop broadcast communications: understanding transmission success and failure under different radio propagation environments. In *MSWiM '06: Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems*, pages 68–77, New York, NY, USA, 2006. ACM.

[86] Marc Torrent-Moreno, Daniel Jiang, and Hannes Hartenstein. Broadcast Reception Rates and Eeffects of Priority Access in 802.11-based VehicularAad-Hoc Networks. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 10–18, New York, NY, USA, 2004. ACM.

[87] Lars Wischhof and Hermann Rohling. Congestion Control in Vehicular Ad Hoc Networks, 2005.

[88] Qing Xu, Tony Mak, Jeff Ko, and Raja Sengupta. Vehicle-to-Vehicle Safety Messaging in DSRC. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 19–28, New York, NY, USA, 2004. ACM Press.

[89] Xue Yang, Jie Liu, Feng Zhao, and Nitin H. Vaidya. A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning. *Mobile and Ubiquitous Systems, Annual International Conference on*, 0:114–123, 2004.

[90] Jijun Yin, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 1–9, New York, NY, USA, 2004. ACM.

[91] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks. *IEEE Network Magazine*, 13:24–30, 1999.