ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Alexander Technological Educational Institute of Thessaloniki, Department of Informatics

"Vehicular Ad-Hoc Networks (VANETs): A detailed study and research extensions"

Author: Kadas George | 2582/04

12/7/2011

Supervisor: Dr. Periklis Chatzimisios

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Dr. Periklis Chatzimisios, without whose support and constant guidance this thesis would not have been completed. Moreover, I would like to extend my gratitude to my good friends Konstantinos Paparas and Leonidas Simopoulos. It is because of their help, advice and constant reviewing of my work that I managed to avoid numerous obstacles towards completing this thesis.

PREFACE

This dissertation was developed and submitted under the auspices of the Department of Informatics (Alexander Technological Educational Institute of Thessaloniki), as a part of my undergraduate thesis in partial fulfillment of the requirements for Bachelor's Degree in IT (Information Technology). It tackles the issue of Vehicular Communication Networks, but more from an IT perspective since this is also the major that the aforementioned Institution offers. It contains work done from November 2010 to June 2011. The thesis has been made solely by the author; most of the text, however, is based on the research of others, and I have done my best to provide references to these sources.

I always have a keen interest about communication networks and in July 2010 I was acquainted with Vehicular Ad-hoc Networks. Taking immediate interest in that particular field, this thesis was the perfect opportunity to further my studies on the subject. The Department of Informatics offers two modules relevant to communication networks, but the subjects covered in these modules is somewhat generic and closer to data-link and physical layer of the OSI model. For this reason, an extensive research had to be completed, in order to better understand the reasoning, mechanisms and feasibility of the vehicular communication networks.

ABSTRACT

This B.Sc. thesis analyzes the basic concepts and mechanisms that are used in the new IEEE wireless standard, 802.11p in order to enhance the performance of the vehicular networks. The issues of Security, Quality of Service and Routing are extensively covered along with the existing current research and enhancement proposals by various researchers. Basic definitions as well as complex mechanisms are analyzed and presented in order to enable the average reader to fully comprehend the subject and the ideas that have been introduced. The work is separated into chapters, starting with the introduction and basic concepts of vehicular networks. In the second chapter a small introduction helps the understanding of the role of road side infrastructure in vehicular communications. The third chapter is comprised of the book chapter authored and finally accepted in the book entitled "Roadside Networks for Vehicular Communications: Architectures, Applications and Test Fields", that will be published by IGI-Global in 2012. This book chapter includes a detailed analysis on the vehicular networks and how roadside infrastructure helps improve security, quality of service and routing. In the fourth chapter, we present an introduction about the concept of intelligent transportation systems and its socioeconomic effects. In the final chapter of the current thesis, we present the paper that was submitted and finally accepted in the Panhellenic Conference on Informatics (PCI 2011), that is an overview of the past and recent scientific projects and organizations that have set their focus towards the wide acceptance of the vehicular communication networks and the intelligent transportation systems as well as their large-scale deployment.

TABLE OF CONTENTS

Index of Tables

Index of Figures

Table of Abbreviations

Table of Abbreviations (Alphabetically)

2G	2nd Generation Cellular
3G	3rd Generation Cellular
AP	Access Point
BER	Bit Error Rate
BSS	Basic Service Set
CA	Certification Authority
CCH	Control Channel
CSMA	Carrier Sense Multiple Access
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
GHz	Gigahertz
GPS	Global Positioning System
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IR	Infrared
ITS	Intelligent Transportation System
LMSC	LAN/MAN Standards Committee
MAC	Medium Access Control
MAN	Metropolitan Area Network
MANET	Mobile Ad-hoc Network
Mbps	Megabit per second
MHz	Megahertz
NAV	Network Allocation Vector
NesCom	New Standard Committee
OBU	On-Board Unit
OFDM	Orthogonal Frequency Division Multiplexing
PAR	Project Authorization Request
PC	Personal Computer
PHY	Physical
PKI	Public Key Infrastructure
QoS	Quality of Service

QoS	Quality of Service
R&D	Research & Development
RA	Road Access
RevCom	Standards Review Committee
RF	Radio Frequency
RSU	Road Side Unit
SCH	Service Channel
SG	Study Group
TA	Trusted Authority
TAG	Technical Advisory Group
TCP	Transmission Control Protocol
TPD	Tamper-proof Device
TTP	Trusted Third Party
UDP	User Datagram Protocol
V2I	Vehicle-to-Infrastructure (also termed as V2R: Vehicle-to-Roadside)
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad-hoc Network
VC	Vehicular Communications
VOIP	Voice over IP
WAVE	Wireless Access in Vehicular Environment
WBSS	WAVE Basic Service Set
WG	Work Group
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multi-Media
WSMP	WAVE Short Message Protocol

CHAPTER -1-

Chapter 1 – Introduction to Vehicular Communication Networks

Introduction to Vehicular Communication Networks

Moving means changing constantly location; this means a constant demand for information on the current location and specifically for data on the surrounding traffic, routes and much more.

In the current B.Sc. thesis, during its duration two deliverables were produced (a book chapter and a conference paper respectively), we attempt to analyze the basic functions and mechanisms of 802.11p, which is the newly released Institute of Electrical and Electronics Engineers (IEEE) standard for vehicular wireless networks. Furthermore, a brief and detailed description of all the necessary concepts and terminology is presented, as well as pre-developed technologies that are required to fully comprehend the topic of IEEE 802.11p. Topics like Quality of Service, Security, Routing, Safety, scientific efforts, R&D projects and Initiatives that attempt to solve the major issues in vehicular communications and accelerate the large scale deployment of a vehicular networks are being subject to discussion.

In order to better understand the mechanisms that are used in the IEEE 802.11p standard, we need to understand some very basic concepts and the mechanics of communication, transmission and networking. This is necessary in order to be able to completely grasp the various mechanisms of the IEEE 802.11p standard and the way it operates, as well as how that is achieved. Thus, we need to present some very basic definitions that might be needed to fully understand this thesis.

Communication is the activity of exchanging information between two or more participants. In order to achieve communication usually we need a sender, a message, one or more intended recipients and a common language. It is required that all communicating parties share an area of commonality, such as to enable the communication itself. Communication is considered successful if the receiver has acquired the whole message and is able to understand it. In computer networks and telecommunications we have wired communication as well as wireless communication. Communication is achieved through transmissions between the various stations of the network that may include PCs, hubs, switches, printers, access points and more.

Wireless communication may be used to transfer information over short or long distances depending on the technology that is used. Some of the widely deployed technologies are Infrared (IR), Bluetooth and of course radio waves. Wireless technology is used in many different areas from television and garage door openers to cell phones and computer networks. It enables communication that would otherwise be impossible or impractical to implement with the use of conventional wired technology. In local area networks, wireless transmission is mainly used as a backup communication link in case of primary network failure and sometimes for economic reasons.

1.1 Mobile Ad-hoc Network (MANET)

A Mobile Ad-hoc Network (MANET) [1] is a self-configuring infrastructure-less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each device should forward traffic unrelated to its own use, and therefore act as a router. Such networks may operate independently or may be connected to the larger

Internet. The growths of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s.

The first generation goes back to 1972 when it was developed for military use. At the time, they were called PRNET (Packet Radio Networks). In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment. What we have today can be considered the 3rd generation of mobile ad-hoc networks.

In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. And later on in mid-1990s, within the Internet Engineering Task Force (IETF), the Mobile Ad-Hoc Networking working group was formed to standardize routing protocols for ad-hoc networks.

As many mobile or handheld devices are getting smaller and cheaper, standardization organizations are looking for ways to keep those devices connected through various mobile ad-hoc networks.

1.2 Vehicular Ad-hoc Network (VANET)

In Vehicular Ad-hock Networks [2], cars and generally automobiles are used as nodes in order to create a mobile network. The specific characteristics of this network that differentiate it from a Mobile Ad-hoc Network is that the nodes are moving at high speeds resulting in a network that has a fast changing topology and is highly disconnected.

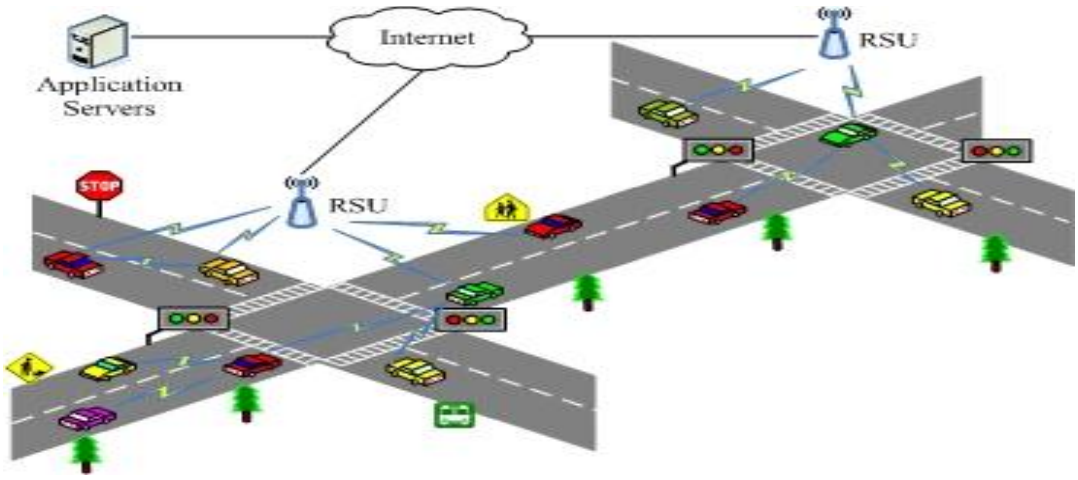

Figure 1: Vehicular Ad-hoc Network (VANET)

In VANETs, wireless technologies (WiFi, WiMax, Infrared, Radio, etc.) as well as fixed infrastructure connected to the backbone network [3], are utilized in order to complete all the necessary transactions and communications between nearby vehicles and between vehicles and nearby infrastructure.

The main motivation behind vehicular communications is safety on the road [4]. However, besides road safety, different applications caught the attention of several stakeholders. Several comfort and driver assistance applications have been or are being developed in order to increase market penetration of vehicular communications and raise the necessary funds for research and development of the vehicular networks.

1.3 Wireless Access in Vehicular Environment (WAVE)

Wireless Access in the Vehicular Environment (WAVE) [5] is an expansion of the 802.11 standard protocols, primarily used for automotive electronic wireless communications, in order to meet the intelligent transportation system applications. WAVE technology consists of IEEE 802.11p Standard, IEEE 1609.X Standard and SAE J2735 Standard. It includes the data exchange between high-speed vehicles and between vehicles and roadside infrastructure and also supports ITS applications in the licensed band of 5.9 GHz.

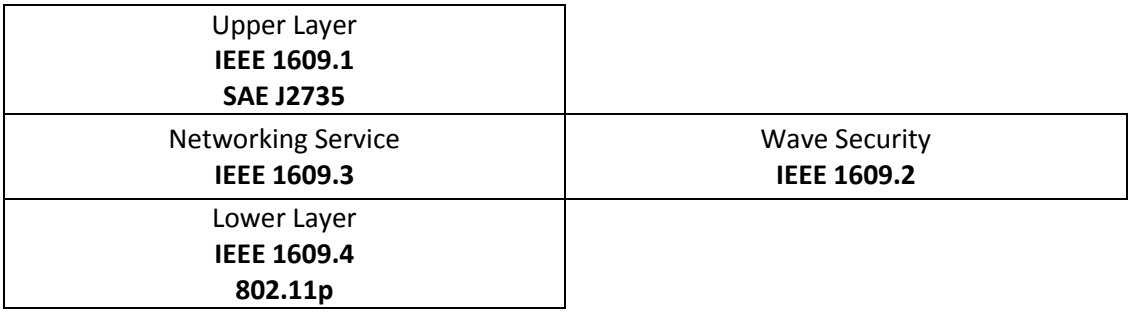

Figure 2: Wave Structure

The components of a WAVE system consists of entities called Units. Roadside units (RSUs) usually are installed in light poles, traffic lights, road signs; they can be installed in numerous fixed locations but cannot work while in transit. Onboard units (OBUs) are mounted in vehicles and can function while moving. By default, WAVE [6] units operate independently, exchanging information over a fixed radio channel known as the control channel (CCH). However, they also can organize themselves in small networks called WAVE Basic Service Sets (WBSSs), which are similar in nature to the service sets defined in IEEE 802.11

WAVE architecture supports two types of messages with respective protocols. One is the traditional Internet Protocol version 6 (IPv6) and the other is a proprietary one known as WAVE Short-Message Protocol (WSMP). The reason for having two protocols is to accommodate high-priority, time-sensitive communications, as well as more traditional and less demanding exchanges, such as Transmission Control Protocol/User Datagram Protocol (TCP/UDP) transactions.

1.4 IEEE 802.11 Standard & Standardization Process

As mentioned before, in wireless communication aside from the common physical medium there is need for a common “language” in order to successfully initiate and conclude the communication. This however is a bit more complicated matter, since there are many parameters that need to be regulated. In order for sender and receiver to correctly understand each other, there is need to have very specific rules and definitions. These are specified and documented in so called protocols by the IEEE.

1.4.1 Standardization Process

Another point of interest is how a new standard is created. The IEEE 802 standardization process [7] begins when a project is approved within a group. That group then gets a letter assigned, for example 802.11p. A study group is formed when the area is new and first investigated for standardization. The Study Group (SG) can be a part of an existing Working Group (WG) or a Technical Advisory Group (TAG). New projects within an existing group are developed by a task force, while new independent projects create new work groups. For each project, an authorization request (PAR) is submitted for approval within the first six months. Every new project, in order to prove that it meets the charter of LAN/MAN Standards Committee (LMSC), needs to provide supporting material in the form of 5 criteria. The sponsor executive committee votes on the draft PAR and afterwards goes to the IEEE Standards Board New Standard Committee (NesCom), which recommends it for approval as an official IEEE standard project. The PAR also includes information about liaisons to any outside groups that might be contributing to the project. Proposals are evaluated by the WG and a draft standard is written and voted on by the WG. The work progresses from technical to editorial and procedural as the draft matures, once the WG reaches enough consensus on the draft standard, a WG letter ballot is done to release it. It is then approved by the SEC and goes for sponsor letter ballot. After the ballot is passed, the draft standard is sent to the IEEE Standards Board Standards Review Committee (RevCom). As soon as it is recommended by RevCom and approved by the Standards Board, it can be published as an IEEE standard. Usually drafts are also sent to ISO, where it undergoes a similar, parallel approval path and then becomes an ISO standard as well.

1.4.2 WAVE Standardization History

The initial effort at standardizing DSRC radio technology took place in the U.S as part of the ASTM 2313 working group. In 2004, this effort migrated to the IEEE 802.11 standard group since DSRC radio technology is essentially IEEE 802.11a adjusted for low overhead operations in the DSRC spectrum. Within IEEE 802.11, DSRC is known as IEEE 802.11p WAVE [8], which stands for Wireless Access in Vehicular Environments. IEEE 802.11p is not a standalone standard. It is actually intended to amend the overall IEEE 802.11 standard. One particular implication of moving the DSRC radio technology standard into the IEEE 802.11 space is that now WAVE is fully intended to serve as an international standard.

The IEEE 802.11p standard is meant to:

- Describe the functions and services required by WAVE-conformant stations to operate in a rapidly varying environment and exchange messages without having to join a Basic Service Set (BSS), as in the traditional IEEE 802.11 use case.
- Define the WAVE signaling technique and interface functions that are controlled by the IEEE 802.11 MAC.

IEEE 802.11p WAVE [9] is only a part of a group of standards related to all layers of protocols for DSRC-based operations. The IEEE 802.11p standard is limited by the scope of IEEE 802.11 and is strictly a MAC and PHY level standard that is meant to work within a single logical channel. All knowledge and complexities related to the DSRC channel plan and operational concept are taken care of by the upper layer IEEE 1609 standards. In particular, the IEEE 1609.3 standard covers the WAVE connection setup and management. The IEEE 1609.4

standard sits right on top of the IEEE 802.11p and enables operation of upper layers across multiple channels, without requiring knowledge of PHY parameters.

1.5 The IEEE 802.11 Family

- The IEEE 802.11 family is a set of standards for wireless communications which includes the over the air modulation techniques that are used in the various different protocols.. The first widely adopted standard was the 802.11b, which was followed by 802.11g and nowadays the 802.11n standard. However, the standard that will be the main concern of this thesis is the 802.11p standard that was created to support wireless access in vehicular environments. Moreover, we outline some of the existing standards as follows [8], [10]:
- 802.11 - First standard (1997). Specified the MAC and the original frequency hopping and direct sequence modulation techniques.
- 802.11a - Second physical layer standard (1999), but products not released till late 2000.
- 802.11b - Third physical layer standard (1999). The first widely adopted standard.
- TGc - Task group that produced a correction to the example encoding 802.11a. Since the only product was a correction, there was no 802.11c.
- 802.11d - Extends frequency hopping PHY for use across multiple regulatory domains.
- 802.11e - Recently standardized (2005) about Quality of Service (QoS) extensions for the MAC. An interim snapshot called Wi-Fi Multi-Media (WMM) was implemented before the standard was complete.
- 802.11F - Inter-access point protocol to improve roaming between directly attached access points.
- 802.11g - Recently standardized (2003) PHY for networks in the ISM band.
- 802.11h - Standard to make 802.11a compatible with European radio emissions regulations. Other regulators have adopted its mechanisms for different purposes.
- 802.11i - Improvements to security at the link layer.
- 802.11j - Enhancements to 802.11a to conform to Japanese radio emission regulations.
- TGk (future 802.11k) - Task group to enhance communication between clients and network to better manage scarce radio use.
- TGm - Task group to incorporate changes made by 802.11a, 802.11b, and 802.11d, as well as changes made by the TGc into the main 802.11 specification (Think m for maintenance).
- 802.11n - Recently standardized (2009) founded to create a high-throughput standard. The design goal was throughput excess of at least 200 Mbps, and the resulting standard was called 802.11n.
- 802.11p - Recently standardized amendment (2011) in order to add wireless access to vehicular environment (WAVE) and support Intelligent Transportation Systems (ITS)
- TGr (future 802.11r) - Enhancements to roaming performance.
- TGs (future 802.11s) - Task group enhancing 802.11 for use as mesh networking technology.
- TGT (future 802.11T) - Task group designing test and measurement specification for 802.11. Its results will be standalone, hence the uppercase letter.
- TGu (future 802.11u) - Task group modifying 802.11 to assist in interworking with other network technologies

1.6 IEEE 802.11p

IEEE 802.11p [11] is specifically targeted at vehicular environments. It operates in the 5.85 GHz – 5.925 GHz band and its PHY is identical to OFDM-based 802.11a/RA. In addition to the traditional 20 MHz channel, 802.11p can operate with reduced 10 MHz channel spacing in order to compensate for the increased delay spread in outdoor vehicular environments. Although this halves the maximum data rates to 27 Mbps, longer communication distances can be achieved by allowing a maximum radio output power of up to 760 mW. IEEE 802.11p requires radios to operate in a temperature range from -40 C to 85 C, due to the harsh environmental conditions in vehicular networks. It also enables the communication between devices moving at speeds up to 200 km/h. IEEE 802.11p defines the lower part of the MAC layer, while the IEEE 1609 family of standards address the upper part of the MAC (1609.4), networking (1609.3), security (1609.2), resource management (1609.1), communication management (1609.5), and overall architecture (1609.0). With maximum communication range of 1 km, the time for data exchange between two moving devices is limited to a few seconds before connectivity is lost. Global synchronization is crucial to vehicular ad hoc networks for coordinating multichannel accesses. 802.11p enhances the timing synchronization function to facilitate global timing synchronization based on an external source like GPS.

The 802.11p is mainly based on [12]:

- IEEE 802.11a PHY: OFDM modulation
- IEEE 802.11 MAC: CSMA/CA
- IEEE 802.11e MAC enhancement: message prioritization (QoS Support)

Table 1: Comparison of the Physical Layer in 802.11a and 802.11p

Parameters	IEEE 802.11a	IEEE 802.11p	Changes
Bit Rate (Mbit/s)	6, 9, 12, 18, 24, 36, 48, 54	3, 4.5, 6, 9, 12, 18, 24, 27	Half
Modulation	OFDM	OFDM	No Change
Modulation Mode	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM	No Change
Velocity	6 m/s	45 m/s	75% increase

Number of Subcarriers	52	52	No Change
Transmission Power	28.8 dBm	28.8 dBm	No Change
Guard time	0.8 μs	1.6 μs	Double
FFT Period	3.2 μs	6.4 μs	Double
Preamble Duration	16 μs	32 μs	Double

1.7 IEEE 1609.X Standard for Vehicular Communications

The IEEE 1609 [13] Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. Together these standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management and many others. IEEE 1609 family of standards also known as the Upper Layer Wireless Access in Vehicular Environment (WAVE) standard is used to define the architecture, communication model and mechanisms of high-speed short-range and low latency wireless communications. Together with IEEE 802.11p, IEEE 1609 standards comprise the base of WAVE architecture. The IEEE 1609 family of standards consists of 1609.0 – (Overall Architecture), 1609.1 - (Resource Manager), 1609.2 - (Security services for Applications and Management Messages), 1609.3 - (Networking Services), 1609.4 - (Multi-channel Operations), 1609.5 – (Communication Management) and 1609.11 - (Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems).

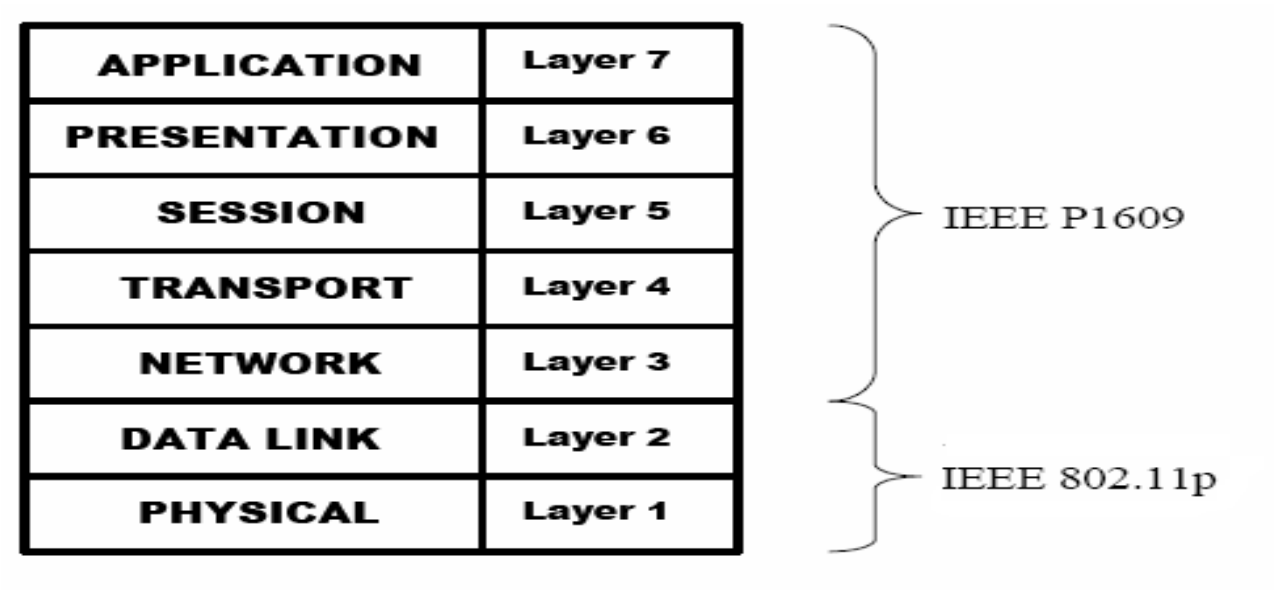

Figure 3: OSI Layers Correspondence

1.8 Dedicated Short Range Communication (DSRC)

Dedicated short-range communications [14] are one-way or two-way short- to medium-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards which was officially standardized in 2003. In October 1999, the United States Federal Communication Commission (FCC) allocated in the USA 75MHz of spectrum in the 5.9GHz band for DSRC to be used by Intelligent Transportation Systems (ITS). Also, in Europe in August 2008 the European Telecommunications Standards Institute (ETSI) has allocated 30 MHz of spectrum in the 5.9GHz band for the same reason. The decision to use the spectrum in the 5GHz range is due to its spectral environment and propagation characteristics, which are suited for vehicular environments - waves propagating in this spectrum can offer high data rate communications for long distances (up to 1000 meters) with low weather dependence. DSRC has two key benefits: 1) It complements cellular communications, where time-critical responses (less than 50 ms) or very high data transfer rates (6-54 Mbps) are required in small zones with license-protected authority, and 2) it enables a new class of communications applications that can support future transportation systems.

Table 2: Dedicated Short Range Communication (DSRC)

Parameters	Value
Radio Range	300m (1000m Max)

Data Rate	6-27 Mbps
Communication Mode	Half-duplex
Channels	7 Licensed Channels
Latency	≈50ms
Band	5.850-5.925 GHz range (divided into 7 channels)

DSRC has two types of channels, service and control, that service different requirements and needs of the applications [6].

- ***Control Channel (CCH):***
  - Broadcast Communication
  - Dedicated to short, high-priority, data and management frames
    - ✓ Safety Critical Information
    - ✓ Initialization of two-way communication on service channel
- ***Service Channel (SCH):***
  - Two-way Communications (OBU-OBU, OBU-RSU)
  - Specific Applications (Tolling, Internet Access)
  - Different kind of applications can be executed simultaneous on different service channels.
  - All of the above require the establishment of a WAVE Basic Service Set (WBSS)
- ***High Availability – Low Latency Channel (HALL):***
  - The first service channel (as shown in the figure below: seen as Critical Safety of Life) is allowed to use HALL and a control channel to keep the connection between OBU and RSU.
- ***Safety Margin:***
  - The reserved 5 Mhz at the lower end of the channel act as a safety margin.

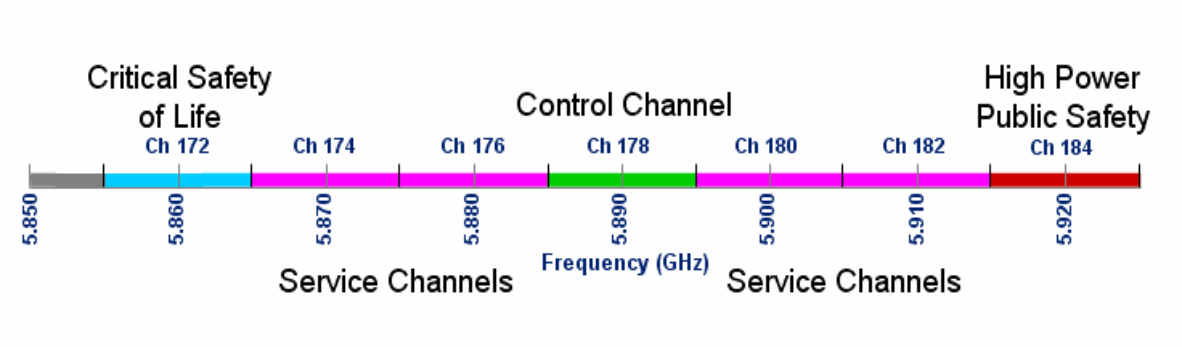

Figure 4: Wave Channel Arrangement

1.9 DSRC Message Set Dictionary – SAE J2735

The purpose of SAE J2735 [15] standard is to support interoperability among DSRC applications through the use of standardized message sets, data frames and data elements. It provides information that is useful in understanding how to produce interoperable DSRC applications. It is intended for application developers. VANET equipment manufacturers and generally the parties that is associated with the Intelligent Transportation Systems

The standard defines, among others, message formats for an a la carte message, basic safety message, emergency vehicle alert message, generic transfer message, a probe vehicle data message and a common safety request message.

SAE J2735 supports many message categories that are used by applications to exchange data over the DSRC/WAVE, as well as other, communication protocols. Some of the message categories that it includes are the following:

- General
- Safety
- Geo-location
- Traveler Information
- Electronic Payment

1.10 Physical Components of IEEE 802.11p Networks

The 4 main physical components of IEEE 802.11p networks are: Stations, Access Points, Wireless Medium and Distribution system [16].

- Stations: all computing devices with wireless network interfaces. In vehicular networks the nodes of the network are mobile at high speeds and random topologies. Vehicles become communication-enabled nodes of the network using their On-Board Units (OBUs)

- Access Points (APs): devices which can perform the wireless to wired bridging function. This is necessary because 802.11 frames need to be converted to in order to be sent and delivered over wired media. In VANET this role is fulfilled by the Roadside Units that provide a wide set of services to the mobile nodes.
- Wireless Medium: in order to transmit frames between stations a wireless medium is used. There are several different physical layers, which support the 802.11 MAC layer. Most of those are Radio Frequencies (RF), which is also the more popular option, and some are infrared (IR). Moreover in vehicular environment cellular (2G/3G), WiMax, Zigbee and WiFi are utilized to provide for easy, accurate, effective and simple communication between vehicles on dynamic mobility.
- Distribution System: in case more than one access points are interconnected there is need for communication amongst them, in order to keep track of the movement of the mobile nodes. It's basically the backbone of the network and usually is implemented using Ethernet. In VANETs, the backbone networks play an important as it is those that provide connectivity on the internet and connect the otherwise isolated network with the outside world.

1.11 Concluding Remarks

Currently, networks have only been available in hot-spots, commercial buildings, or homes. Consumers are beginning to demand access anytime from anywhere including an automobile. They require wireless Internet access whether shopping at the mall, waiting at the airport, walking around town, or driving on the highway. They also require the ability to surf the Web, download files, and have real-time video conference calls and other tasks, through a wireless communication connection to the Internet with the same data rates as their desktop. Both public and private parties support the growing effort in the particular scientific field of vehicular networks and have set as their goal, the worldwide large scale deployment of this type of network that carries many benefits for both road safety as well as commercial growth. It is definitely a growing industry that will be a major subject of research in the years to come.

CHAPTER -2-

Chapter 2 - Improving Vehicular Networks via RSU-assistance

Improving Vehicular Networks via RSU-assistance

Vehicular Communications are a new field in the area of mobile networks bringing new challenges but also several benefits towards its large-scale deployment. To that direction several solutions have been developed and proposed by the scientific community. Utilizing pre-existed or newly installed road side infrastructure to enhance the services offered by vehicular networks has been able to provide efficient solution for many of the tasks that posed a challenge in the networks operation and deployment.

2.1 Security in Vehicular Communications

To become a real technology that can guarantee public safety on the roads, vehicular networks need an appropriate security architecture that will protect them from different types of security attacks. In the following book chapter, we are exploring the different security aspects of vehicular networks, including:

- Threat Models
- Authentication
- Key Management
- Privacy
- Secure Positioning

We also investigated the potential threats, attacks and adversaries that security must be able to thwart in order to keep the network environment safe for its participants.

Security takes up a rather large portion of the scientific interest concerning vehicular communications; that is because it is, if not the most, one of the most challenging tasks in vehicular communications and its provision is synonymous to the development and wide acceptance of vehicular networks.

In the following book chapter, which was authored as part of this thesis, we investigated the Vehicle-to-Infrastructure component of vehicular security. We examined how and on what level improves the security of the network.

2.2 Quality of Service in Vehicular Communications

Quality of Service in Vehicular Networks can be provided to either safety applications or to comfort applications. However, because of the built-in channel reservation that is implemented by the lower-level protocols, quality of service provision tends to be a challenge and an issue when it comes to commercial applications and non-safety services.

We investigated how quality of service parameters, such as:

- High Throughput
- Low Latency
- Guaranteed Delivery
- Network Availability
- Fault Recovery
- Link Stability

can be provided to vehicular network services.

Quality of Service is tied with the routing process as the means of its provision, meaning that a protocol or any other mechanism should provide high quality route under the mobility of vehicles.

In the book chapter that follows, we examined the possible ways that Quality of Service provision can be implemented in vehicular networks via targeted protocols, schemes and mechanisms.

2.3 Routing in Vehicular Communications

Routing in Vehicular Networks is quite challenging due to the network's special nature. We can either use purely ad-hoc or RSU-assisted routing to route packets in a vehicular network.

- Maximization of distance of coverage,
- Access to backbone and secondary networks,
- Dissemination of information in a specified area,

are a few of the things that we attempt to improve by utilizing Road Side Units as part of the routing process in vehicular networks.

RSU-assistance tries to provide a solution to vehicular routing in cases where the use of existing routing protocols is not applicable. Certain traits of the vehicular networks prohibit the use of traditional routing protocols, such as

- Partitioning
- Large Scale
- Predictable Mobility
- Node Reliability

In the book chapter, we primarily focused on the RSU-assisted routing component of the vehicular networks. We examined several possible ways its performance can be improved, thus enhancing the networks performance. We also investigate the benefits RSU-assistance offers against traditional ad-hoc routing.

2.4 Concluding the Book Chapter

The book chapter is concluded with a glimpse in the future trends and expectations for vehicular communications and networks along with a summary of the subjects that were examined.

CHAPTER -3-

Chapter 3 - The Role of Roadside Assistance in Vehicular Communication Networks: Security, Quality of Service and Routing issues

The Role of Roadside Assistance in Vehicular Communication Networks: Security, Quality of Service and Routing issues

Abstract- Vehicular Communication Networks is a subcategory of Mobile Communications Networks that have the special characteristics of high node mobility and fast topology changes. In the current chapter, we outline the basic characteristics and concepts of vehicular communications and present the standardization and network deployment efforts carried out by the scientific community. In particular, we focus our attention on the vehicle-to-infrastructure component of the network; moreover we specifically investigate security, quality of service and routing that constitute three of the most challenging aspects in the field of Vehicular Networks. We further examine the ways that infrastructure can provide efficient solutions to the problems that exist for each respective category and review several proposed solutions.

3.1. Overview and Background of VANETs

Vehicular communications is an emerging part that has attracted much interest from academia and industry. In this chapter, we explore the aspects of vehicular communications and Vehicular Ad-Hoc Networks (VANET) to draw our attention on Vehicle-to-Infrastructure traffic model. In particular, we examine certain mechanisms to security-proofing a vehicular network, to provide quality of service according to certain needs and to route data traffic.

3.1.1 What is a VANET?

A vehicular ad-hoc network (Hassnaa & Yan, 2009) is a special type of mobile ad-hoc network, utilizing vehicles as mobile nodes to create a network. This type of network can either be purely ad-hoc, meaning that all the traffic is being handled by the network nodes alone, or it may be assisted by the roadside network creating a vehicle-to-infrastructure relation in the network.

3.1.1.1 Inter-vehicle Communications

Inter-vehicle communications allow a mobile vehicle to communicate with its surrounding environment, mobile or fixed networks. More specifically, vehicular nodes can communicate with their peers either via vehicle-to-vehicle communications or through the fixed roadside infrastructure. The communication and the delivery of information may range from motion data (speed, direction, location, etc.) to internet media content, through the wide variety of supported applications that operate in a vehicular network. The demands of the applications that operate in the vehicular environment, along with the properties and special traits of the vehicular access networks define the design and the requirements of the security provision, the quality of service provision and the routing process within the network.

3.1.2 Inter-vehicle Communication Challenges

The vehicular networks pose some serious challenges (Blum, Eskandarian & Hoffmman, 2004) as the network's deployment is not an easy task. Moreover, the fact that the sparse deployment of the roadside infrastructure,

whose deployment is even more difficult and sparser, in many cases infrastructure often plays key role to the smooth operation of the network.

Furthermore, we will outline some of the major challenges that vehicular networks face and the possible ways that roadside equipment can help mitigate or even overcome those challenges.

- *Absence of central coordination:* While this is a major drawback of the purely ad-hoc part of the network, it poses no threat for the vehicle-to-infrastructure communication model, as the infrastructure assumes the role of the central coordinator for all the nodes that are in communication range with it.

- *Dynamic network:* One of the special traits of a vehicular network is its dynamic nature, which is a result of the mobile nodes and the high speed they develop considering the fact that are vehicles. This results in a highly disconnected network, where the communication windows between nodes are often narrow. However, the deployment of the infrastructure and its use as an active part of the network comes from the need to solve the previously reported problem. Thus, infrastructure is employed to provide a level of stability to the dynamic network by coordinating the communication between its participants.

- *Security concerns:* Even though it will be analyzed later in chapter, it is really important to mention the issue of security that has risen with the VANET deployment. While the need for privacy and a secure environment is imperative to the deployment of a vehicular network, such environment cannot be guaranteed without the assistance of roadside networks. In this case, a certain security policy is enforced on the network and the infrastructure is used to oversee it.

3.1.3 VANET Applications

On that regard, it is important to identify the four major categories (Kamini & Rakesh, 2010) of applications that exist in a VANET and provide numerous services:

- *Safety-oriented applications*, such as emergency break warning application or lane-change warning application. Safety-oriented applications are, as the name implies, applications that focus on providing the VANET nodes with the necessary mechanisms in order to maximize accident prevention and mitigate an accident's impact on the rest of the network.

- *Service-oriented applications*, also known as infotainment applications, aim to provide the VANET participants with several services. They strive to make the driving experience of both driver and passengers more comfortable through various applications and services. That may include internet access, media streaming, online gaming, etc.

- *Traffic efficiency applications*, target at the improvement of traffic flow, reduction of road congestion, provision of alternate routes. This can be achieved in various ways such as electronic toll collection, rail intersection management, congestion awareness and information, real-time traffic conditions etc.

- *Driver assistance applications*, aim to provide a secure and comfortable experience for the driver of the vehicle. Digital road maps downloading, navigation systems, parking assistance and automatic

emergency call are only some of the services that can be provided and add up to providing as much assistance as possible to the driver, without in any case compromising the driving experience.

It must be noted that this general taxonomy is affected by the vehicle-to-infrastructure relation. It is needless to say that certain applications could not achieve the required performance of delay, throughput and other network metrics if they were left to operate only in an ad-hoc manner.

Table 3: Characteristics and Requirements of safety and infotainment applications in vehicular networks

	Safety Applications	Infotainment Applications
Reach	Local (1-hop neighbors)	Distant
Mode	Geocast/Multicast	Unicast/Multicast
Latency	Low	Various (application dependent)
Packet Delivery Ratio	High	Various (application dependent)
Connection Duration	Short	Long
Security	Yes	Yes

3.1.4 Vehicular Communications: Vehicle-to-Infrastructure (V2I)

In this chapter, we specifically examine the V2I part of the vehicular communication model. V2I communications (Wiesbeck & Reichardt, 2010) refer to communication between road users and road side equipment that is based on short or medium range communication technology. However, it must be noted that this architecture does not rely on the infrastructure in order to operate but rather exploits it to improve the network performance. Things that surely are essential for the existence of such a relation are:

i) A hybrid network meaning the existence of both vehicles and roadside equipment (in areas where the roadside equipment is either not existent or really sparse we cannot provide vehicle-to-infrastructure communications).

ii) Protocols and mechanisms that support such a communication for both ends, vehicles and the infrastructure. Due to the special nature of the relation between vehicles and the roadside unit, the necessary interfaces are a pre-requisite. Routing protocols tailored for V2I communications are the most common example of this necessity

iii) Deployable penetration that means the existence of a sufficient number of roadside units placed alongside the highway or urban roads. We must note that another really important factor that shapes both the network penetration and deployment but also the service provision through protocol and mechanism design, is that the

network operation must be efficient with a certain minimum of deployed infrastructure, at least for the early stages of its operation.

3.1.4.1 The IEEE 802.11p Standard

In the discussion about vehicular communications, one should not miss to mention the only (up to now) standard for this kind of communications. That is the IEEE 802.11p standard that has been developed to support both vehicle-to-vehicle and vehicle-to-infrastructure communications.

This standard utilizes the Dedicated Short Range Communication (DSRC) to complete wireless transactions and operates on the licensed band of 5.9 GHz for Intelligent Transportation Systems (ITS). The IEEE 802.11p standard supports vehicle-based communications and services such as toll collection, safety services and commercial transactions via vehicles. These services involve greatly the vehicle-to-infrastructure communication model.

3.1.4.2 The IEEE P1609 Standard

The P1609 standard family (IEEE Standard – P1609) also known as the upper layer WAVE standard is used to define the architecture, communication model and mechanisms of high-speed short range wireless low latency communications. Together with 802.11p, P1609 standard family comprises the base of the Wireless Access in Vehicular Environments (WAVE) architecture. Collectively the IEEE 1609 (1609.1, 1609.2, 1609.3, 1609.4, 1609.11) Family of Standards for WAVE describes wireless data exchange, security, and service advertisement between vehicles and roadside devices.

3.1.4.3 Work In Progress

Many initiatives across the world (Olariu & Weigle, 2009) have taken up the development of vehicular networks. The main objective of vehicular network deployment is to make transport safer and in particular to address issues and scenarios that are not addressed by the V2V component of vehicular communications. However, the stakeholders take interest in promoting service-oriented and infotainment applications to improve travel comfort. In many countries worldwide, the research for vehicular communications have been aggregated under an organization or initiative (Motsinger & Hubbing, 2007) and some of those have already deployed early stages of vehicular networks, while focusing on both V2I and V2V communications, in specific cities or regions around the world. Some of the most known initiatives that strive to improve vehicular communications are Japan's Smartway project (http://www.its.go.jp/ITS/topindex/topindex_sw2007.html) which has started its deployment in Tokyo and other regions in Japan and ITS Japan (http://www.its-jp.org/english) that strives to improve road transportation systems. Also, U.S.A's VII program (currently knows as Research and Innovative Technology Administration, RITA - http://www.its.dot.gov), which also has deployed vehicular networks in certain regions across the country. Also ITS America (http://www.itsa.org) promotes ITS development in the U.S.A.

There are numerous initiatives and R&D projects in Europe; we only refer those that are most relevant to the subject of this chapter.

- ***NoW (Network-on-Wheels)*** is a German project, which mainly works on communication aspects for vehicle-to-vehicle and vehicle-to-roadside communication. The specific objective of the NoW

project is the development of a communication system which integrates both safety and non-safety applications. The NoW project ended in May, 2008. (http://www.network-on-wheels.de/)

- ***SAFESPOT (Cooperative vehicles and road infrastructure for road safety)***, addresses co-operative systems for road safety, referred to as "smart vehicles on smart roads". In order to prevent road accidents, a "safety margin assistant" that detects potentially dangerous situations in advance, has been developed. This assistant represents an intelligent cooperative system utilizing vehicle-to-vehicle and vehicle-to infrastructure communication based on IEEE 802.11p for vehicular communications. (http://www.safespot-eu.org/)

- ***CVIS (Cooperative Vehicle Infrastructure Systems)***, aims at developing a communication system that is capable to use a wide range of wireless technologies, including cellular networks (GPRS, UMTS), wireless local area networks (802.11p), short-range microwave beacons (DSRC) and infra-red (IR). Additionally, A Framework for Open Application Management (FOAM) is defined that connects the in-vehicle systems, roadside infrastructure and back-end infrastructure that are necessary for cooperative transport management. (http://www.cvisproject.org/)

- ***PRESERVE (Preparing Secure Vehicle-to-X Communication Systems)***, is a project that mainly focuses on security concerns of the vehicular communications and aggregates and extends previous projects and their results. It aims to create an integrated V2X architecture, that is easy deployable, that is scalable, low-cost, and has no open deployment issues, and close-to-market. This project started 01/01/2011and is scheduled to have duration of 48 months, until 31/12/2014. (http://www.preserve-project.eu)

- ***The European counterpart of ITS Japan and ITS America, known as ERTICO*** (http://www.ertico.com), joins together public (Ministries of Transport, European Commission) and private (European Industry) partners and work together to realize the development and deployment of ITS across Europe.

- ***The international CALM (Communications Access for Land Mobiles - since 2007)*** initiative (http://en.wikipedia.org/wiki/Communications,_Air-interface,_Long_and_Medium_range) that has set its attention to setting the standards for vehicular communications and wireless technologies and comprises the base for several other initiatives that work on different areas of vehicular communications. The rapid and efficient spread of this type of networks is obvious across the globe in the recent years with only beneficial outcomes for the vehicular traffic.

3.1.5 Chapter Overview

The vehicular communications field and the vehicle-to-infrastructure component in particular have been debated for a long period by the research and scientific field. The majority of the research in vehicular communications has been directed in the purely ad-hoc part of the network in the vehicle-to-vehicle component.

At the same time it is becoming increasingly clear that if we want to meaningfully contribute and make ground-breaking progress, we can no longer ignore the fact that the road-side network exploitation can offer vast improvement to the network performance in all its aspects and provide efficient solutions to matters where V2V architecture fails to address and solve. Many key subjects that have to be resolved efficiently include quality of service provision, security-proofing, and provision of a routing algorithm for the network and its participants.

This chapter overviews these three important aspects of the network, outline the current problems that they currently face and provide an aggregation of the proposed solutions in each respective field, always in relation with the vehicle-to-infrastructure architecture. The reader is also introduced to the basic architecture, communication model and characteristics of vehicular communications, in order to obtain a full understanding of vehicular networks.

3.2 Security Challenges in VANETs and Proposed Solutions

We cannot actually argue about a deployable VANET architecture without first concerning ourselves with the security aspects of this particular type of network. The need to of finding efficient solutions to secure-proofing the vehicular environment networks is by all means imperative and the research on possible ways to fulfill the security requirements is continuous. In the following section, we will try to aggregate and enumerate all these requirements and later on examine and present various solutions, in the form of targeted protocols, schemes or mechanisms.

3.2.1 Mandatory Security Features for Vehicular Communications Networks

In this section, we investigate the security features (Yue, Jun & Ju, 2009) that a VANET should have in order to be considered secure in all its aspects.

- *Authentication*

Authentication is a major requirement in VANET security because it ensures that the senders of messages are valid VANET members. However, the authentication process raises concerns about the privacy-protecting of the vehicular nodes and this trade-off is investigated in detail later on.

- *Message Integrity*

This requirement ensures that the messages are not changed in transit and that the messages the driver receives are not false. This requirement falls under the non-Cryptographic security of VANET and is explained later on.

- *Message Non-Repudiation*

This requirement ensures that a sender cannot deny having sent a message. Although this does not mean that the sender is identifiable. Only specific authorities should be allowed to identify vehicles by analyzing their sent messages.

- *Entity Authentication*

This requirement ensures that the sender of a message is an existing and authenticated vehicle of the network. This requirement can effectively thwart illusion attacks because the vehicles that participate in the network are real vehicles that have the necessary authorization.

- *Access Control*

Access control is required to ensure that all nodes that belong to the network, operate according to the roles and privileges authorized to them. Specifies what a node can do and what messages can generate in the network.

- *Message Confidentiality*

This is required when certain nodes want to communicate privately. This can only be performed by the law enforcement authority vehicles that communicate with each other to convey private information.

- *Node Privacy*

This characteristic is used to ensure that the information is not leaked to unauthorized people that are not allowed to view the information. Therefore, a certain degree of anonymity should be available for messages and transactions of vehicles. Moreover, location privacy is a major issue in VANET security, so that a vehicle cannot be tracked by an outsider.

- *Real-time Guarantees*

Because of the special nature of the VANET environment, that is high mobility and dynamic topology, the time windows for vehicular communications and especially Vehicle-to-Infrastructure are often narrow. Thus, it is essential in a VANET safety related applications that depend on strict time deadlines to be serviced efficiently.

- *Network Availability*

This requirement ensures that the network will be always available for its users at all times. While preventing attacks, such as Denial of Service that can compromise the availability of the network, this requirement provides all the needed bandwidth and network services to the applications so they can operate in an effective and secure manner.

The Problem

As it has already been mentioned, it is obligatory for VANET to have security provision for safety as well as infotainment applications. Due to the unique characteristics of VANETs, the aforementioned provision is not always guaranteed.

Some of the problems that have risen from the security requirements are being addressed by the solutions presented in this chapter as follows:

- Non repudiation
- Access Control
- Confidentiality
- Node Privacy
- Network Availability
- Message Integrity
- Message Authentication
- Entity Authentication
- Real-time guarantees

It is clear that researchers aim to a unified scheme that utilizes the necessary set of tools in order to supply VANET with an acceptable level of security. In the rest of this chapter, we outline and further analyze mechanisms, schemes and targeted protocols (proposed either in academia or in industry) that try to accomplish the general objective of securing VANETs. In most cases, many mechanisms and protocols are tied and work together to achieve that outcome.

3.2.2 Challenges and Problems in Vehicular Security

Being a special category of MANETs, VANETs have some unique characteristics that make their large scale deployment harder and pose some unique challenges (Stampoulis & Chai, 2007; Papadimitratos, Gligor & Hubaux, 2006). For example, the information conveyed over a vehicular network may affect life-or-death decisions, making fail-safe security a necessity. However, providing strong security in vehicular networks raises important privacy concerns that should also be considered. The deployment of vehicular networks is rapidly approaching, and their success and safety will depend on viable security solutions acceptable to consumers, manufacturers and governments.

3.2.2.1 Tradeoff between authentication and privacy

During authentication, all message transmissions need to be matched with their originating vehicles. On the other hand, personal information about vehicles should not be known to any other than the Trusted Authority (TA). In order to achieve efficient VANET security, these two completely opposite traits must come to equilibrium. This tradeoff is called resolvable anonymity. Therefore, a system needs to be introduced that enables vehicles to be anonymous to most participating nodes but also enables identification by central authorities in cases like accidents or malicious behavior.

3.2.2.2 Location Awareness

Certain location based services are essential for most applications to be truly effective, so that reliance of the VANET system on GPS or other specific location based instruments can be increased as any error is likely to effect the supported applications.

3.2.2.3 High Mobility

Due to the high mobility of the nodes in VANETs, their topologies are highly dynamic and time windows are really narrow. This in itself is a major spatial and temporal constraint of the network. The proposed mechanisms, schemes or targeted protocols, should be able to perform all their operations concerning the secure-proofing of the network, while managing to satisfy these two constraints.

3.2.3 Privacy Problems and Proposed Solutions

It is clear from the previous contents of this section that preserving privacy plays a major role in securing VANETs in such a way that they would be deployable in large scale. Towards this direction, there have been great research efforts and many targeted protocols, novel schemes and mechanisms have been proposed to achieve this goal. Furthermore, we outline and investigate proposed ways that make this privacy-preserving claim a reality.

3.2.3.1 Cryptographic Privacy

When we are referring to cryptographic privacy, we imply all the attributes that make a network secure using means of cryptography. In general, it is required that a message should be resilient against the compromise of its security as well as its sender's. Thus, it is important the privacy-preserving of the nodes and messages of the network but at the same time, efficient authentication should be achievable to make sure that malicious nodes will not be part of the network.

A. Public Key Infrastructure (PKI): Role, Use and Effectiveness

Public Key Infrastructure, also referred to as PKI, is one of the most popular ways used to secure VANET because it can meet most of the security requirements of a vehicular network environment such as anonymity, authentication, non-repudiation, etc. PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, PKI is an arrangement that binds public keys with respective user identities by means of a Certificate Authority (CA). The role of PKI that assures this binding is called the Registration Authority (RA). The term Trusted Third Party (TTP) may also be used for the Certificate Authority (CA).

As mentioned before, PKI mechanisms use digital signatures to bind a public key with the real identity of a vehicle; in such a way that the certificate can be used to ascertain that a public key belongs to a certain vehicle, thus, eliminating the problems of data authentication and message non-repudiation. Pseudonymous certificates allow us to achieve both privacy and authentication.

Another element of the PKI architecture is the Certificate Authority. that is the entity that issues the digital

certificates to the nodes (vehicles) of the network. A certificate is a vehicle's public key and identifier signed by the CA. The main function of the digital certificate is to certify that a certain vehicle (its identity is only known to the CA) is the owner of a public key. This allows vehicles or RSUs to trust the signatures or assertions that are made by the private key that corresponds to the public key (private/public key pair) that has been certified by the CA.

It is well understood from the aforementioned definition of PKI that it comprises a set of elements that all together create a security net over VANET. In this regard, we review all the elements one-by-one and all together to have a complete picture of the way public key infrastructure secures VANETs.

I. Pseudonyms

The (long-term) root certificate provided by the CA and the pseudonym certificates (short-term) with corresponding key pairs (public keys-private keys) are assumed to be able to protect the vehicle's privacy by not linking the certificates directly to vehicles.

Dötzer (2005) proposes a system for pseudonym security. The system operates under the assumptions that every vehicle is equipped with a tamper-resistant device, which offers secure memory to store secrets and secure computation as well as that the vehicle is able to execute small programs and cryptographic algorithms. It is further assumed that during production of the vehicle, a secure connection between this device and authority A is available, using Hardware Security Module (HSM). There are three operating phases in this system; the initializing phase (during which the systems of the vehicles are set up), the operational phase as the major mode of operation (during which vehicles can send messages signed according to a chosen pseudonym) and the credential revocation phase (during which predefined situations can lead to the disclosure of a vehicle's real ID and the shutdown of its system). Protection against misuse of the credentials is provided by the tamper-resistant device and the revocation mechanism provides robust network availability.

The main reason to maintain privacy in vehicular networks is to thwart any adversary that tries to compromise the network and its participants. In (K. Sampigethaya et al., 2005), the authors provide a solution to the problem of privacy preservation by allowing any vehicle to be able to achieve unlinkability between two or more of its locations in the presence of tracking by an adversary. The proposed scheme combines group navigation and a random silent period enhancement technique to provide user privacy and mitigate vehicle tracking. The assumptions of this scheme are a trusted authority and the ability for the authority to track a vehicle based on the strength of its signal. Between the pseudonym changes, the vehicle stays silent for a random period of time so the adversary cannot track it using temporal and spatial relation as observed in (Leping, Matsuura, Yamane & Sezaki, 2005).

The certificate authorities play an important role to the preservation of privacy in vehicular networks; not only to provide the legitimate nodes with the necessary certificates but also to prevent malicious nodes from harming the network. Papadimitratos et al. (2007) propose a system architecture in (Papadimitratos, Buttyan, Hubaux, Kargl, Kung & Raya, 2007) that supports privacy protection and secure communication among others. One basic aspect of this system is the cross-checking of the vehicles between CAs so that security can be achieved in regional scale. Each node, being either a vehicle or a RSU, holds a unique id and a pair of

public/private keys. The CA that manages the long-term certificates is responsible for their replacement once the old ones expire. To achieve privacy protection, each node is equipped with a set of distinct certified public keys known as pseudonyms and they are used to sign the outgoing messages of the vehicle. Frequent changes on these pseudonyms, issued by a trusted pseudonym provider, make tracking of vehicles extremely hard. Because of the variable rate of pseudonym switch depending mostly on network parameters (velocity, policy, number of nodes), the concept of pseudonym refill is also explained in which a node requests an (i+1) set of pseudonyms before his i set depletes.

Freudiger et al. (2007) propose a scheme utilizing a protocol that both aim to provide unlinkability between the vehicle and its transmitted messages and provide location privacy for the driver. For this purpose, pseudonyms are utilized to disclose the driver's private information However, updating pseudonyms in a monitored area has been proven ineffective because the location information of the messages can still be used to exploit temporal and spatial tracking on the vehicle. This chapter assumes that the vehicles have a tamper-proof device and that before entering the network a vehicle registers with the CA and receives a set of pseudonyms. The authors also proposed the creation of anonymizing regions known as mix-zones in order to force pseudonym change to take place there. Because the effectiveness of the proposed approach lies mainly on the number of vehicles and the randomness of the zone's whereabouts, the authors also proposed the placement of these regions at road intersections where vehicles mix all together and their velocity and direction usually change. However, if the mix-zones have fixed or expected locations, the adversary may know where and when to launch an attack. For this reason, a protocol named CMIX is introduced that creates cryptographic mix zones, in which every vehicle uses a symmetric key to encrypt their sending data throughout the pseudonym change process and to keep it secure the RSU, which provides that symmetric key, changes it during the update process.

Building blocks of the VANET's privacy preservation are the vehicle's credentials and keys. This information should remain private from the rest of the network. Towards this direction, Papadimitratos et al. (2008) propose a system architecture addressing the privacy-preserving of identity, credentials, key management and secure communications. This particular architecture assumes the existence of several CAs to service multiple regions as well as the ability to cross-certify vehicles when entering new regions. Every vehicle is registered with only one CA, and it has a long-term identity along with a pair of public/private keys and a log-term certificate issued by the CA (which is later renewed upon expiration) that contains attributes of the node (mostly used for access control) and lifetime of the certificate. In order to satisfy the privacy requirement, this architecture uses pseudonyms that are switched frequently so the messages signed by these pseudonyms cannot be linked back to the originating vehicle. In order to obtain certificates, a vehicle issues a message to the CA over a secure channel, identifying itself and registering to the CA (via public key). After authentication, the vehicle sends a set of pseudonyms that contain an identifier of the CA, the lifetime of the pseudonyms, the public key and the signature of the CA, covering all the private information about the vehicle. This architecture also utilizes the aforementioned pseudonym refill mechanism.

Key factor to the non-traceability of the vehicular nodes and therefore the protection of their privacy is for the use of pseudonyms for a short period of time. This concern is being addressed by Calandrielo et al. (2007). The authors propose a scheme in which every node is equipped with a set of pseudonyms. Each pseudonym is used

for limited period of time. The combination of pseudonyms and group signatures is the basic element of the proposed scheme. Every node is equipped with a group signature key and instead it generates its own set of pseudonyms and with the group signature key it generates a group signature on each pseudonym. In this scheme, the nodes can generate and self-certify their own pseudonyms.

II. Certificate Revocation

Due to the numerous threats in VANET, it is possible to revoke a certificate for one of the following reasons:

- *Key Compromise:* The private key of the vehicle or the RSU is suspected to be or is compromised.
- *Change of affiliation:* Some information about the certificate of the vehicle or the RSU or any other information is no longer valid.
- *Suspended:* The certificate is suspended.
- *Cessation of operation:* The certificate is no longer needed for its assigned purpose.
- *Change of Policy:* The CA no longer operates under the certain security policy and no longer service certificates.

The most common way to revoke a certificate is by using Certificate Revocation Lists (CRLs) that contain the certificate identities of misbehaving nodes, are used to inform the nodes of the network about misbehaving nodes with revoked privileges in an attempt to exclude those nodes from the network. However, a challenge that remains is the distribution of this list to the vehicles, because due to the size of the network in can grow exponentially. Thus, the vehicular nodes before verifying any received message, each node checks whether or not the sender is included in the up-to-date CRL. The real problem that rises with CRLs is their distribution which is prone to long delays and might not always be an easy task because of the real-time nature of the mechanism, but also their creation because of their rapidly growing size due to the fast-changing pseudonyms of the network nodes. In the case of group signatures, the group manager is responsible to reveal the credentials of the suspicious vehicle for the CA to revoke its privileges.

In place of the CRL, due to its hard distribution to the vehicles, some other approaches have been proposed for the revocation of the misbehaving vehicles. Towards that direction, P. Wohmacher (2000) proposes the Online Certificate Status Protocol (OCSP), which can verify the current validity of a certificate online. If a more timely reaction is required, the proposed protocol can be employed instead of CRLs. The protocol is utilized between a client and a server where the client queries the server for a set of certificates in order to check their validity and the server after executing the necessary checks on its part, responds with the certificate validity status to the client. A certificate response from the server can be unknown, revoked or good. Unknown means that the server has no information about the queried certificate, revoked means that the certificate has been revoked or is on hold and good may mean that the certificate has not been revoked, it has not been issued yet or the time the response was produced it was out of its validity. The OCS protocol is especially effective for attribute certificates (used to manage access control) in which the status information need to be up-to-date.

An almost certain pre-requisite to achieve privacy in vehicular networks is the existence of TPD units (Tamper-Proof Devices) on vehicles. Raya et al. (2007) take advantage of this and propose a protocol that leverages the presence of a TPD unit on board the vehicle. If the CA determines that a vehicle must be revoked, with the help of the road-side infrastructure, initiates a two-party end-to-end protocol with the tamper-proof device of the vehicle during which the CA instructs the TPD to erase all cryptographic material it stores and halt its operation upon completion of the protocol. The protocol actually "kills" the TPD, depriving the misbehaving node from its cryptographic keys and, thus, ensuring that all its messages are ignored by all other correct nodes.

Also in (Raya et al., 2007), the use of the RC2RL protocol is proposed that targets to the dramatic decrease of the time in which the nodes of a VANET can obtain an updated CRL. It is utilized when the CA (which is responsible for the revocation) wants to revoke only a subset of the vehicle's keys or when its tamper-proof device is unreachable. Given the large size of the CRL in VANETs, the protocol utilizes bloom filters (a probabilistic data structure used to test whether an element is a member of a set),thus, decreasing the CRL size to only a few KB and making it possible for it to be transmitted via radio frequency. This protocol relies on the infrastructure to broadcast the compressed CRL in frequent intervals.

Additionally in (Raya et al., 2007), the LEAVE warning system is proposed that relies on the collective information gathered from a vehicle's neighborhood. Due to the fact that LEAVE cannot sense or collect the necessary information on its own, it relies on a mechanism named MDS (Misbehavior Detection System). Since all vehicles can be attackers with the same probability, the warning messages may contain correct or wrong accusations. Given the limited amount of available evidence, vehicles rely on the assumption of honest majority and crosscheck all received accusations. An accusation issued by a node has a lower weight when this node is already accused by other participants. If the sum of weighted accusations (the eviction quotient) against a vehicle exceeds a defined threshold, it is locally evicted by LEAVE until the evicted node gets in the region of a CA and has his certificate revoked. More precisely, warning messages are transformed into disregard messages that instruct all the neighbors of the attacker to ignore its messages.

B. Group Signatures: Requirements, Effectiveness and Proposed Solutions

Group signatures address the privacy requirement by providing anonymity within a certain set of nodes, namely a group. A group consists of several group members and one Group Manager (GM). A group signature is produced by using the message to be signed, the secret signing key of the sending node, and the group public key. A Group Signature scheme lets the members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but at the same time they do not reveal the identity of the signer.

In general, a secure group signature scheme should fulfill the following requirements:

- *Unforgeability:* Only group members are able to sign messages on behalf of the group.
- *Anonymity:* Given a valid signature of a message, identifying the actual signer is computationally hard for everyone but the group manager.
- *Unlinkability:* Deciding whether two different valid signatures were computed by the same group

member is computationally hard.

- *Excludability:* Neither a group member nor the group manager can sign on behalf of other group members.
- *Traceability:* The group manager is always able to open a valid signature and identify the actual signer.

Group signature-based mechanism is another proposed way that can preserve the vehicles' privacy in vehicular networks. Jinhua et al. (2007) propose a security framework to preserve VANETs using group signatures. In this framework members of the network maintain only a small set of group public/secret key pairs and they are anonymous within the group from which they sign. This framework assumes that all the messages that exist in the network are authenticated.

Another group signature-based approach is proposed by Boneh et al. (2004). In this approach, the authors propose a group signature-based scheme that is based on the Strong Diffie-Hellman (SDH) assumption as it is explained in (Boneh & Boyen., 2004). The scheme is based on a zero knowledge protocol for SDH in which the Fiat-Shamir heuristic is applied.

Xiaoting et al. (2007) propose among others a scheme for OBU-to-RSU communication based on ID-based group signatures. An identity string is used as a public key to sign the messages. That way, the workload caused by the certificate management process can be avoided, and the public key updating and revocation operations can become rather simple.

3.2.3.2 Privacy in terms of Trustworthiness and Data Integrity

When we are referring to trustworthiness and data integrity in order to ensure privacy, we should discuss all the attributes that make a network secure, without using means of cryptography to conceal the node's information but rather to ensure the integrity and trusted origin of messages. In general, it is required that a message that exists in the network to be trustworthy and to maintain data integrity. The concepts of trustworthiness and data integrity have risen and several trust systems have been developed to fulfill them.

Dhurandher et al. (2010) propose a robust algorithm to provide trustworthiness in VANET environment, namely VSRP. The algorithm provides trustworthiness by running reputation and plausibility checks. The algorithm takes into consideration three types of messages: application of brakes, traffic jam and accident. These messages can highly affect the network if compromised. The algorithm uses a trust table in order to maintain the trust levels of its neighborhood; this table holds values from 0 to 4, 0 being the lowest trust value assigned to a malicious node. In order to manage the reputation slots for each neighbor (if a suspicious behavior is detected), the vehicle increases the counter assigned to that behavior and if it reaches a certain threshold, the general reputation counter for this vehicle drops by 1 unit.

Trustworthiness does not only reside in message trustworthiness but also to the regions in which the vehicles are moving. To ensure that the vehicles will be moving into trusted regions, Serna et al. (2008) describe a scheme to provide trust condition for the vehicle participating in VANETs, while being in a untrusted area (meaning a region that is serviced by a different CA). This scheme enables CA interoperability with no explicit agreements. Moreover, the concept of CA Federations is proposed in which an agreement is made between the

different CAs on a security minimum for all of them to inter-operate and thus, eliminating untrusted territories. In this approach, instead of distributing new sets of “compatible” certificates to the VANET nodes, the only requirement is to give them access to the trusted repository of the CA Federation to update their local certificates.

Most of the schemes, mechanisms and targeted protocols that aim to deem a network, message or region trustworthy for its participants make use of infrastructure-assistance to achieve that goal. We are examining the Kerberos approach, included in the paper by Wex et al. (2008), which is a successor of the Needham-Schroeder protocol. It relies on an online interaction with a central Key Distribution Center (KDC) for authentication in order to get a valid ”trust” token for a service (contains a session key, a validity period and the requesting node’s identity encrypted with the server’s secret key). The authorization information is kept at the services locally. Due to scalability problems in large environments, newer versions of Kerberos also allow the central management of authorization information and their integration in the issued tokens.

Gomez et al. (2011) assume the existence of fixed elements of the infrastructure with internet connectivity and certain processing capabilities that also communicate with all vehicles that pass close to them. The infrastructure elements used in this approach are Road Side Unitsthat communicate with the vehicles, with other RSUs and with the Base Stations that connect to the internet through backbone networks. An honest majority policy is applied, but the case of malicious node is not excluded entirely. The main focus of this approach is to identify and isolate such malicious users by means of an accurate trust and reputation management mechanism application. The proposed approach defines that every time it receives a message, it first checks the reputation of the sender in order to decide whether to drop, accept or accept and forward the message. These three actions represent the three levels of trust used in this approach, so a node can be not trusted (reject), more or less trustworthy (accept but not forward) and fully trusted (accept and forward). Each message has a corresponding severity to the sender’s reputation with a severity maximum for each trust level depending on the message. Additionally, a reputation score will be computed for each node taking into account three different sources of information, namely: direct previous experiences with the targeting node, recommendations from other surrounding vehicles and, when available, the recommendation provided by a central authority through Road Side Units. Concerning the recommendations provided by the infrastructure (when available), they are used to identify and isolate malicious nodes travelling throughout the country. The central authority controlling RSUs can manage a database containing all those users who have been deemed malicious.

3.2.4 Authentication Problems and Proposed Solutions

Although in the previous section we described the significance of privacy in order to maintain a secure Vehicular Network, we should not perceive it to be the only goal. A vehicular network must provide in any case and at all times robust authentication for its participants while preserving their privacy. Authentication can and should be achieved in all the privacy schemes, either PKI-based or group signature-based, that have been developed for vehicular networks as it is an integral part of the VANET security.

Subsequently, we present and examine several authentication architectures for VANET environment, in which Road-Side Units play an important role:

Chenxi et al. (2008) propose an RSU-aided message authentication scheme, called RAISE. In particular, when an RSU is detected, nearby vehicles start to associate with it. The RSU assigns a unique shared symmetric secret key and a pseudo ID that is shared among the vehicles. With the symmetric key, each vehicle generates a symmetric keyed-Hash Message Authentication Code (HMAC) and then broadcasts a message signed with this symmetric HMAC code instead. Receiving vehicles are able to verify the message by using the notice about the authenticity of the message disseminated by the RSU. The RSU knows the authenticity of the messages because it shares HMAC encryption keys vehicles they were disseminated to. In any circumstance that a vehicle cannot verify a received message, it will use the PKI-based scheme to do so.

In vehicular networks, message authentication must happen in such way that the receiver of the message knows for sure that the message is trusted. Studer et al. (2009) propose a mechanism that makes use of the public key infrastructure along with the roadside network to authenticate messages in the network. The sender signs its messages with TACK's private key and from time to time broadcasts its RA-signed certificate. The receivers can use these two pieces of information to verify the sender's validity.

Wasef et al. (2009) propose a protocol that accelerates the authentication (revocation check) process. A general PKI scheme is deployed and by utilizing it the authentication enhancement happens. Bilinear pairing and hash chains are used as tools to achieve this fastening in the authentication process. The sender calculates his revocation check and appends it in the message along with his public key, the OBU's ID, a timestamp and a HMAC which plays the role of the authentication code. The receiver checks the validity of that information and either verifies the sender or drops the message and updates the CRL adding the non-valid node.

A certain example where PKI-based and group signature-based solutions co-exist and operate in the same environment is proposed by Wasef et al. (2009). The ASIC verification scheme supports stand-alone aggregate signatures verification and aggregate certificates verification. Furthermore, it supports simultaneous aggregate signatures and certificates verification.

Perrig et al. (2002) propose an authentication protocol, named Timed Efficient Stream Loss-tolerant Authentication (TESLA). TESLA, according to its creators has low communication and computation overhead, tolerates packet loss and scales to a large number of nodes, characteristics that make it ideal for vehicular environments. TESLA also works under the assumption that all sender and receiver(s) loosely time-synchronized and on the precondition that either the sender or the receiver must buffer some messages. TESLA uses one-way hash chains to authenticate keys at the receivers. The main idea of TESLA is that the sender attaches to each packet a MAC (Message Authentication Code) computed with a key known only by the sender. The receiver buffers the received packet without being able to authenticate it. In subsequent event, the sender reveals the key to the receiver rendering him able to authenticate the packet.

While TESLA is vulnerable to Denial of Service (DoS) attacks as the sender can be flooded with time-synchronization requests to compromise its security, TESLA++, investigated in (Studer, Bai, Bellur, & Perrig, 2008) addresses exactly that particular weakness. In TESLA++, the receiver only stores a self-generated MAC to reduce the memory requirements. Since the receiver only stores a shortened version of the sent data, the sender firstly sends the MAC and then the message with its corresponding key. In TESLA++ authentication, the sender first sends the MAC to the receiver, which in turn checks to see if there is a corresponding key to it

(checking to see if the message key has been broadcasted yet); if there is, the MAC is dropped. Once the key can be disclosed, the sender will send any messages and the key that is used to calculate their MACs'. To verify a message, the receiver first verifies the validity of the key by following the one-way key chain back to a trusted key. The receiver then calculates the shortened MAC of the message and compares it with the MAC and index stored in his memory. If the receiver has a matching MAC/key index pair in memory, the receiver considers the message authentic. In any other case, the receiver considers the message unauthentic and discards the message.

The contribution of Studer et al. (2008) is a framework for message authentication using a combination of Elliptic Curves Digital Signature Algorithm (ECDSA) signatures and TESLA++. Once an OBU verifies a message using TESLA++, it can verify the ECDSA signature if non-repudiation is required. The ECDSA component also provides authentication in multi-hop communications if the OBU has no memory of the TESLA++ MAC. Due to that versatility of multiple verifications, this framework can meet many of the security needs of VANET.

3.2.5 Adversaries in VANETs

We term as an adversary or attacker any node that tries to compromise the security of the vehicular network. Such nodes can achieve that either by launching various attacks in the network, depending on what they are trying to achieve or by operating in a totally different way, than the one defined from the network policy, causing problems for the other legitimate nodes.

3.2.5.1 Greedy Driver

Following the honest majority rule, a greedy driver that is a member of the VANET will try to mislead his fellow drivers for personal gain. For example, misleading the other members of the VANET to believe that there is congestion in the road ahead while there is not, would create much better driving conditions for him.

3.2.5.2 Eavesdropper

This kind of adversary tries to obtain others' personal information and credentials and causes a serious breach in the privacy of the network. The eavesdropper may use illusion attack to impersonate another vehicle in order to gain access to certain privileges or its personal information. A very effective way to minimize this adversary's effect on the network is using cryptographic privacy and to manage the sensitive data in tamper-proof devices.

3.2.5.3 Pranksters

They are adversaries that will attempt to cause problems in the network to have fun. A prankster could also abuse the security vulnerability to Denial of Service (DoS) attacks to disable applications or prevent critical information from reaching another vehicle.

3.2.5.4 Malicious Attacker

This kind of adversary deliberately attempts to cause harm on the vehicular network. Normally, this adversary has specific targets, and has access to more resources than other adversaries. In general, such kind of

adversaries will be less in numbers than other kinds; they pose probably the most serious threat for the VANET security provision system.

3.2.6 Security Attacks against VANET

In this section, we aim to categorize the major security attacks that have been launched on VANET and we attempt to summarize some of the solutions that have been proposed in order to diffuse or minimize the effect of those attacks on the network.

The most active fields of interest when it comes to security attacks in VANET are: anonymity, key management, privacy, reputation, location.

3.2.6.1 Anonymity

While VANET security tries to preserve the anonymity of its members, attackers may aim to discover the physical identity of a vehicle, in most cases with malicious intent.

A. Malicious Vehicle

One of the most important security requirements of VANETs is privacy. To avoid being tracked, the use of randomly changing pseudonyms is suggested. This can lead to a situation where a malicious vehicle M can easily change its identity to node N without being punished.

3.2.6.2 Key Management

Key management deals with the secure generation, distribution and storage of keys. There are three main approaches for key management: key exchange, key agreement and key management infrastructure.

A. Brute Force Attack

This attack in the form of exhaustive search for all the possible keys can pose a really serious threat against the members of the VANET, since the distribution of safety-related information should not be tampered with and is of crucial importance to the ITS system.

A proposed solution to this kind of attacks as proposed in (Langley, Lucas & Huirong, 2008) operates under the condition that there is a unique identifier for each vehicle, such that one can learn if a vehicle is an authorized VANET participant. Because uniqueness in VANETs raises privacy issues, it has been decided to use Vehicle Identification Number (VIN), which is a piece of information unique to every vehicle., The process specifies calculating really large number, appending the VIN to that number and then hashing it with a hashing algorithm. Because of the uniqueness of the VIN in each vehicle and the use of random large numbers to generate the unique identifier, the probability of a security compromise from a brute force attack is dramatically decreased because not only the attacker would have to know the VIN of the vehicle, but also to guess correctly the random large number used and the hashing algorithm used to generate it.

B. Misbehaving and Faulty Nodes

While there is an honest majority policy in VANET, none can guarantee that a certified node will not develop malicious behavior. Although, the default reaction of the network to such events is known, certificate revocation is not always applicable because it requires infrastructure support and the misbehaving of the suspicious node may not always hold reason for revocation by the CA. In this regard many solutions have been developed and proposed in order to protect the members of the VANET from such malicious behavior. However it must be noted that not all suspicious behaviors must be considered malicious but there should be a malfunction threshold.

A really efficient solution to this security compromise is a known scheme examined earlier in the certificate revocation section. The LEAVE scheme along with MDS that are proposed in (Studer, Bai, Bellur, & Perrig, 2008) but also C^2RL are used to make certain that the misbehaving and faulty nodes will be dealt with in a fast and effective manner. In LEAVE scheme, we have a cooperation of the LEAVE protocol with the MDS mechanism to detect and locally isolate any misbehaving node until a CA comes in range to revoke the certificate of the misbehaving node. On top of that, what C^2RL does is that is ensures a fast and efficient distribution time for the most up-to-date CRL from the infrastructure towards the vehicular nodes so that they have the knowledge to ignore messages of revoked nodes and avoid a possible security compromise.

3.2.6.3 Privacy

Privacy is a key aspect in VANET and refers to the ability of the drivers to protect sensitive information about them and their vehicles against unauthorized observers or malicious attackers.

A. Malicious User

In vehicular networks, privacy preservation is a key aspect for them to be deemed secure. Thus keeping private the credentials and other valued information of the vehicle and the driver, from malicious users (in most cases, outsiders to the network) that have as a goal to cause damage by exploiting network vulnerabilities, is obligatory.

One solution to overcome the problem of malicious users involves the use of shared keys (Haas, Jason, Hu, Yih-Chun, Laberteaux, Kenneth, 2010), issued and certified by a trusted third party, between a set of vehicles in the authentication process, that way when a message cannot be traced back to a single vehicle because of the sharing of the same key between a set of vehicles. Moreover, during the authentication process many keys are used by the vehicles because one key may belong to different vehicles. This also helps to the detection of a malicious node, because the RSU is able to trace back the set of keys to the misbehaving vehicle.

B. Traffic analysis attacks

This category of attacks is one of the most serious threats against the privacy of VANETs and it aims to compromise the anonymity of communications. There are many attacks under this category, such as message coding attack, message volume, etc.

A robust solution against these kinds of attacks is a proposed protocol, namely VIPER (Cencioni, Di Pietro, 2007). The proposed VIPER protocol defines that the vehicles in a group, (a group is defined as all the vehicles that are registered with the same RSU) will act as mixes for the outgoing messages. In particular, the messages are being re-encrypted via public key algorithm. Additionally, in order to prevent eavesdropper attacks, every message is encrypted using the node's secret encryption factor and the public key of the RSU. Subsequently, every relay node re-encrypts the message using its own encryption factor. The RSU is the only VANET's component in this architecture that can decrypt the message using its own private key and that is what deems VIPER resilient against traffic analysis attacks.

3.2.6.4 Reputation

Reputation is usually defined as the amount of trust inspired by a particular member of a community, for the particular purposes of this chapter, a vehicular network. Reputation systems are used to trust and encourage trustworthy behavior and work under the assumption that the majority of the network nodes are honest. In VANETs, these kinds of systems can be used to defend against compromised nodes, and malicious ones.

A. Malicious Nodes

The distribution of information about local traffic or road conditions is one of the emerging VANET applications. Since it can increase traffic safety and improve mobility. However, one of the main challenges is to forward event-related messages in such a way that the information can be trusted by receiving nodes. Malicious nodes exploit exactly that by forwarding false traffic information.

While an honest majority policy is being followed in VANET environment, there are always nodes that attempt to compromise the network security. A very effective to halt the operations of pranksters, greedy drivers or malicious attackers is a trust-based system that dramatically reduces the effect of their actions. Using reputation systems (Wex, Breuer, Held, Leinmuller & Delgrossi, 2008), it is feasible for the valid or honest participants of the network to ignore messages or warnings from these nodes and maintain security.

B. Illusion Attack

Illusion attack is a new security threat on VANET applications in which the adversary intentionally deceives sensors of his own vehicle to produce wrong sensor readings. As a result, the corresponding system reaction is invoked and incorrect traffic warning messages are broadcasted to neighbors, creating an illusion condition on VANET.

A really effective solution against illusion attacks is plausibility checks (Dhurandher, Obaidat, Jaiswal, Tiwari & Tyagi, 2010; Nai-Wei & Hsiao-Chien, 2007). In a plausibility check, a node can calculate if a message he received is fake or real (trustworthy), based on measurements from its own sensor data or from data transmitted by other vehicles or even the local RSU. Based on these measurements and a set of rules to examine and filter the data, the node can make a judgment to either trust or drop the message.

Another proposal that attempts to thwart illusion attacks in vehicular communications is Trust and Reputation Infrastructure-based Proposal, in short TRIP (Marmol & Perez, In Press). In TRIP, whenever a vehicle receives a

message or warning from another vehicle it first checks the other vehicle's reputation in order to decide whether to drop or accept the message. Depending on the sender's reputation level, the receiving vehicle can drop the packet, receive but not forward it, or receive and forward it. In order for the receiving node to take this decision, a reputation score will be computed taking into account, direct experiences, recommendations from neighboring vehicles and recommendations from the central authority (through the RSUs). The RSU-provided recommendations are extremely useful as the central authority can provide information about the malicious nodes in the network. Due to the different set of recommenders, there are concerns about the accuracy of the system. However, with the contribution of RSU-acquired reputation information, there is an increased accuracy and resilience of the system.

3.2.6.5 Location

Location refers to vehicle position in a vehicular ad-hoc network. It is one of the most valuable pieces of information (used in geographic routing) and is often readily available through positioning services such as global positioning system (GPS).

A. Forging positions and Sybil attack

Position attacks can occur when the line of sight of the vehicle's sensors is blocked. An attacker can launch a position attack by modifying position packets, replaying false position packets and dropping critical position packets.

The Sybil attack is a well-known harmful attack in VANETs whereby a vehicle claims to be several vehicles either at the same time or in succession. In addition, a Sybil attack refers to an attack where the vehicle's identity masquerades as multiple simultaneous identities. The Sybil attack is harmful to network topologies, connections, network bandwidth consumption.

A solution that has been proposed in (Hubaux, Capkun, & Jun, 2004) involves the existence of tamper-proof GPS devices that can transmit the location information of the vehicle to the neighborhood of the vehicle or to an infrastructure. However this approach has many limitations due to the existence of the tamper-proof GPS device and its known weaknesses.

Another solution to this attack has been proposed in (Soyoung, Aslam, Turgut, & Zou, 2009) where an approach called "timestamps series" is being proposed. This approach specifies that vehicles obtain certified timestamps, signed and issued by RSUs. An outgoing message contains a series of the most recently obtained timestamp certificates and "shows" them when it passes from RSU regions. The proposed approach takes advantage of the spatial and temporal correlation between vehicles and RSUs and assumes that is rather rare or impossible for two or more vehicles to pass from an RSU at the same time. Based on this, Sybil attacks can be detected and thus avoided when a vehicle receives multiple messages with very similar timestamp series.

An effective infrastructure-aided solution that can thwart a Sybil attack is an infrastructure-based architecture, namely NOTICE proposed in (Rawat, Treeumnuk, Popescu, Abuelela & Olariu, 2008). In NOTICE, sensor belts (infrastructure) are embedded in the highway itself. Pressure sensors that are placed in each belt allow every message to be associated with a physical vehicle passing over the belt. Thus, a vehicle cannot pretend to be

multiple vehicles and there is no need for an ID to be assigned to vehicles. The placement of belts for the detection of passing vehicles is more effective than roadside infrastructure and the interaction is performed in a simple and secure fashion.

B. Position cheating and false position disseminating

The position of a node is periodically broadcasted in beacon packets so that every node within the wireless transmission range is able to build up a table of neighboring nodes including their positions. When a node disseminates wrong position data many, if not all the services of the VANET are affected. Wrong position information could be the result of malfunction in the positioning hardware or may be falsified intentionally by attackers to reroute data. Malfunctioning nodes may degrade the performance of a system to some extent while rerouting of data through malicious nodes violates basic security goals such as confidentiality, authenticity, integrity or accountability.

Most solutions for the mentioned attacks are decentralized without the assistance of the roadside network. However, the solution proposed in (Yan, Olariu & Weigle, 2008) involves a V2I component. In particular, all vehicles are equipped with GPS devices and numerous sensors; based on these sensors the vehicle can make judgments for itself on the authenticity of the position information it receives from its neighborhood. For thee operation of the protocol it is essentially to assign a unique ID to the vehicle that can only be issued by the central CA since the vehicle's ID can be changed by the attacker to launch an attack.

3.2.6.6 Availability

Availability is defined as the ability of a user to access the network and its resources in order to service his request. When considering life critical information, unavailability of the network should not be a case. In general, unavailability of the network resources is a network state that we do want to anticipate.

A. Denial of Service

A Denial-of-Service (DoS) attack is an attempt to make the resources of a network unavailable to its authorized users. Considering VANETs, this attack may be a serious threat to the network because of the safety and life-critical messages disseminated in the network.

An effective solution against DoS attacks in VANETs is proposed in (Rawat, Treeumnuk, Popescu, Abuelela & Olariu, 2008), where the NOTICE architecture dictates that a road belt will not react to a single incident reported by a vehicle. On the contrary, the belt will wait for subsequent corroborations of the reported incident before deciding to propagate the information to the other participants in the traffic. Thus, injecting false information into the belt (targeting to denial of service) is thwarted by this mechanism of NOTICE.

Concluding this section, we have extensively analyzed vehicular communications, and especially vehicle-to-infrastructure communications that is one of the most challenging tasks. We have introduced the basic requirements for secure vehicular networks and how these requirements can be fulfilled in order to have an efficient security provision of vehicular networks. We have also outlined the main challenges and trade-offs that

the researchers currently face towards this direction. Moreover, we have overviewed several works on privacy preservation, authentication efficiency and security attacks against vehicular networks. We have also performed a survey of vehicle-to-infrastructure security schemes, mechanisms and targeted protocols and categorized them into a detailed taxonomy. This approach allowed us to identify the current problems to that particular field of vehicular communications and discuss various proposed solutions.

3.3 Heterogeneous Quality of Service (QoS) in VANETs

3.3.1 Quality of Service Provision: Definition, Metrics and VANET implementation

Quality of Service (QoS): the term refers to resource reservation control mechanisms. Basically it enables the provision of different priorities for different applications, users or data flows.

In order to define and fully comprehend Quality of Service, there are some terms that need to be explained.

- *Bit rate:* also referred to as data rate, is the number of bits that are conveyed per unit of time.
- *Communication duration:* is the time during which there is an established connection between two elements of the VANET. Due to the network's highly dynamic nature, we usually attempt to increase the connection's duration, maximize data throughput during that time, or even both.
- *Delay / Latency:* the time it takes for data to travel across the network from the sender to the receiver.
- *Jitter:* Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This delay variation is known as jitter and can seriously affect the quality of streaming audio and/or video.
- *Packet loss / Dropped Packets:* The routers might fail to deliver some packets if their data is corrupted or they arrive when their buffers are already full. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.
- *Bit Error Rate (BER):* is the number of bit errors divided by the total number of bits transmitted during a certain amount of time.
- *Voice over IP (VoIP):* is the widely used technology used to deliver voice communication over the Internet Protocol (IP).

Quality of Service provision guarantees a certain level of performance to a data flow, by meeting a required bit rate, delay, jitter, packet loss probability, Bit Error Rate and communication duration. Depending on the needs

of applications and the transmitted data, such as life critical information, it is understandable that relaying messages over a large area without infrastructure support would have a negative effect on the delay and delivery ratio of messages and thus affecting negatively the quality of service provision in vehicular networks. If we can improve QoS of VANETs in terms of delay, response time, and throughput, we could in many ways improve both safety and comfort of the driver and passengers of any vehicle.

3.3.2 Quality of Service Challenges in Vehicular Environment

Quality of service is a very important feature for safety-related applications (real-time) such as emergency break warning, congestion warning etc. Service-oriented applications such as VoIP, streaming multimedia and online gaming are also affected by quality of service requirements. Due to the fast-changing environment of VANETs, the fulfillment of those requirements per application is a challenging task.

There are two major categories of applications in vehicular communications that require QoS provision and their requirements are totally different:

- Safety-oriented Applications (time-sensitive)
- Service-oriented Applications (not time-sensitive)

Safety-related applications, deliver critical life-or-death messages. This means that the data packets are small, compared to service-oriented messages but the network must be able to deliver those small data packets with short delays and high reliability. Unlike safety-related services, in service-oriented services the main objective is to maximize the amount of data that each vehicle receives, especially in the case of vehicle-to-infrastructure communications since this should happen before the vehicle leaves the coverage area of the roadside beacon. Based on the above, we can safely assume that in VANETs, the real QoS challenges are packet delivery ratio and connection duration rather than typical QoS metrics such as end-to-end delay and jitter.

3.3.2.1 Vehicular Network Characteristics that limit Quality of Service Provision

Due to the special nature of the VANET environment, there are some limitations imposed either by the network itself or by the vehicles participating in it (Cheng, Shan & Zhuang, In Press). These restrictions make the quality of service provision in VANETs a rather challenging task. Such limiting characteristics are:

- *Dynamic Network Topology:* Since the nodes participate in an ad-hoc wireless network, they do not have any restriction on mobility and the network topology changes dynamically. Hence, the admitted QoS sessions may suffer due to frequent path breaks, thereby requiring such sessions to be re-established over new paths.
- *Lack of Central Coordination:* Unlike wireless LANs and cellular networks, ad-hoc networks do not have central controllers to coordinate the activity of nodes. This further complicates QoS provisioning in network.
- *Physical Level Restrictions:* In a broadcast medium, usually the radio waves suffer from several impairments such as attenuation, multi-path propagation and interference during propagation of the messages.

- *Limited Resource Availability:* Network resources such as bandwidth, battery life, storage space, and processing capability are limited in the network.
- *Operational Factors:* Due to the possibility of vehicle malfunction, the position information disseminated in the network might be false. This can greatly affect the QoS provision in VANETs, as safety or data packets cannot arrive to their intended recipients inside the time limits set by their respective services.
- *Security Concerns:* Due to the possible insecurity of the network and under the threat of a potential attack, the information disseminated by the vehicle might not be trusted and be false. This can greatly affect the QoS provision of the network, as data packets cannot reach their destination either in a certain time limit or even not at all.

In the following subsections, we examine several proposed ways to completely nullify or mitigate the effect of those VANET traits on the quality of service provision.

3.3.3 Heterogeneous QoS in VANET

Many different categorizations have been proposed to distinguish the individual needs of VANET's applications, with each one focusing on a different angle of the network.

Thus, depending on the type of traffic, there are three classes of services and the associated QoS requirements (Wang, Giannakis & Marques, 2007):

- *Best effort services:* entail applications such as e-mail and http web browsing. They come with a prescribed maximum allowable bit-error rate but pose no requirements on delay guarantees.
- *Non-real-time services:* involve mission-critical but delay-tolerant applications such as file transfers. They often require minimum rate (i.e., throughput) guarantees but do not impose any delay bounds.
- *Real-time services:* such as safety-related applications, video conferencing and streaming entail guarantees on BER, throughput, and latency.

Another categorization focuses on the QoS provision depending on the application type (Sichitiu & Kihl, 2008):

- *Traffic Management:* This category of applications target to improve traffic flow by the means of traffic light scheduling, emergency vehicle assistance and traffic monitoring.
- *Safety-related Applications:* This category focuses on enabling the vehicles to be able to avoid, or mitigate to a minimum the damage caused by an accident.
- *Traveler Information:* This category aims to provide the driver with all the necessary information to assist him, such as downloading maps, navigation provision, road signs, local rest areas, etc. Moreover, the locality of this particular application category makes it even easier for it to be deployable through means of infrastructure.

- *Comfort-related Applications:* This category focuses on providing the passengers of the car with comfort by means of internet connection, video and sound streaming, games and others means of entertainment.

- *Traffic Coordination and Assistance:* This category provides services such as passing and lane change. Clearly these applications require close-range inter-vehicle communications with tight real-time constraints and can be implemented in either sparse roadside equipment environment or a ubiquitous roadside equipment environment. These applications also take into account the ZOR (Zone of Relevance) concept.

3.3.4 QoS Provision in Vehicular Environment and Proposed Solutions

Very few works focused on data transmission scheduling in roadside-to-vehicle systems so far. In this section we survey vehicle-to-infrastructure architectures that have been developed to enable QoS provision for VANET applications.

3.3.4.1 Possible Modes of QoS Provision

A. QoS through link-reliability

A wide variety of applications is expected to be developed for VANETs. These applications have different requirements for properties such as delay, jitter, bandwidth, throughput and security. Most of these properties are strongly influenced by the successful transmission rates between intermediary nodes. Therefore, a mechanism that offers a way of choosing among options with distinguished successful transmission rates expectations can be used to support policies that provide different levels of end-to-end quality for distinct applications.

B. QoS via Throughput Maximization

Another network metric that plays an important role in QoS provision is network throughput. Taking into account the dynamic nature of the VANET and short time-frame that exists for Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications, it is imperative that a mechanism that can maximize the data throughput during that sort duration is a must. This mechanism applies mostly on service-oriented applications where a large amount of data must be transferred in short time.

C. QoS through End-to-End Delay Minimization

An attribute that is really important to safety-oriented applications is minimum delay. Due to the real time nature of all safety-oriented applications as well as the critical life-or-death information that are being disseminated, the delay of the messages must be kept to a minimum. Thus, bandwidth of the network is often reserved to service only this kind of messages, in order to fulfill the minimum delay requirement. This kind of QoS provision is tied to the VANET large-scale deployment and must be serviced at all times.

The above are only a few of the ways that quality of service can be provided in vehicular networks. As previously mentioned, we considered high throughput and link-reliability, which in turn grants higher connection duration, to be of key importance to the vehicular quality of service provision.

3.3.4.2 QoS Provision, Proposed Solutions for Vehicle-to-Infrastructure Environment

Subsequently, we outline several proposed solutions for quality of service provision for the vehicular environment and in particular for the vehicle-to-infrastructure communication model, which plays an important role in achieving this goal.

As found in Saleet et al. (2009) presented a protocol to provide quality of service in VANET routing, called AMR. This protocol ensures minimum end-to-end delay while maintaining a threshold for the connectivity probability and the hop count through each selected path. In the center of the cell there is a fixed infrastructure which is a Road Side Unit. This RSU is responsible of aggregating the location information about all vehicles within its cell. In AMR, the RSU located in the center of each cell acts as a location server. Therefore the RSU is responsible for saving current location information about all the vehicles that belong to that cell. Each vehicle updates its location information to the RSU each time it moves one transmission range far from its previous location. This enables the local RSU to have a local view of the network composed by the vehicles it manages. Therefore, a map of routes will be constructed between the RSU and the vehicles.

A routing protocol is proposed by Ksentini at al. (2010), that strives to achieve QoS in routing via RSU-assistance and proxy vehicle use, namely PVR. In PVR, a mechanism based on IEEE 802.11 is utilized, where the vehicular networks use the "cooperative and opportunistic" concept to shorten the access delay and to reduce the interference problem within the range of a RSU in a highway environment. In fact, vehicles which are located far apart of the gateway send data, by greedy forwarding, to some particular vehicles called proxies during the long disconnection period. When vehicles enter the RSU transmission range, only the proxy vehicle is allowed to transmit data to the RSU.

Exploiting travel information is a really efficient way to improve quality of service. Sun et al. (2006) propose a QoS-enabled routing protocol using travel information to a large extent, namely GVGrid. This protocol assumes that every node (vehicle) has a short range wireless device that has the same transmission range across the network nodes. GVGrid partitions the geographic region into squares of equal-size called grids. During route discovery, GVGrid attempts to find the route that is expected to have long lifetime, based on the position of each vehicle. This expected lifetime of a route is determined by the vehicles' movement on that route and characteristics (such as traffic signals and stop signs) of the roads on which the route is based.

There have been many proposals as to how to provide quality of service through infrastructure exploitation. A particular architecture proposed by Zhang et al. (2007) operates under the assumption that the vehicles know the service deadlines of their requests. Thus, the RSU knows the deadline (duration) of the communication since the vehicles send the relevant information to the RSU when they enter its range. Due to the high mobility of the network, when a vehicle's request has not been serviced yet and the vehicle exits the regions of the RSU, the request is automatically dropped. With the aforementioned as a given, there have been proposed two

scheduling schemes based on the parameters of data size and deadline. In the data size scheme, if the vehicle can communicate with the RSU at the same transmission rate, the data size can decide the duration of the communication. In the deadline scheme, if a request cannot be serviced by the RSU by its deadline it is automatically dropped.

Another approach is the proposal of a routing protocol to provide quality of service in vehicular environment. In their proposal, Korkmaz et al. (2006) assume the existence of road-side gateways that have two interfaces that the vehicles are connected to access internet services, one for the wireless traffic and one for the wired (internet) traffic. It is also assumed that the transmission range of the RSU can be extended via multi-hop communication, but also that the downlink and the uplink packets have separate channels so there is no contention over the same medium. Another assumption made is that all the vehicles are equipped with GPS devices and the position information is exchanged via one-hop neighbors, therefore an access point to the wireless medium is also assumed to be equipped on the vehicles. CVIA-QoS protocol is designed to provide throughput guarantees and fixed delay bound to soft real-time applications like safety-related applications, voice and video streaming in linear vehicular networks. The best effort traffic is handled with the remaining bandwidth after allocating resources for real-time traffic. In CVIA-QoS, one time slot is divided into two periods, the High Priority Period (HPP) and Low Priority Period (LPP) respectively. In CVIA-QoS, packets admitted to HPP are delivered to the gateway in one time slot. Furthermore, an admission control mechanism is introduced where admission decisions are made by the gateways and executed by the temporary routers.

Alcaraz et al. (2009) propose a mechanism to enhance the quality of service provision. The proposed mechanism attempts to minimize the backlog of data, meaning unprocessed requests/data, which is equivalent of maximizing the throughput. This is being achieved by this particular mechanism by assigning different weights (relative importance factor) to vehicles according to their estimated connection lifetime.

Despite its numerous advantages, QoS provision via RSU assistance has some drawbacks, one of these being its ineffectiveness in sparse or no RSU environment. Ramirez et al. (2007), propose a QoS-enabled routing protocol, namely AODVM that aims to connect the two network segments that comprise a vehicular network that is the mobile network and the fixed infrastructure respectively. The gateway discovery process, by the vehicles that need to communicate can happen in three different ways - proactively, reactively and in hybrid manner – and in every way the existence of infrastructure is mandatory, so in sparse infrastructure environment this protocol would face several issues.

Unlike rural areas where the traffic load might be low, in urban areas where the traffic is dense, message relay may face unavoidable delays. To that end, a routing protocol, namely DTRP, is proposed by Saleet et al. (2010). In DTRP, the gateway constructs a set of routes between itself and the mobile nodes based on its view about the local network topology. Nevertheless, one should note that if these routes consist of intermediate mobile nodes, they cannot be considered to be stable due to intermediate nodes' mobility. To increase their stability, DTRP builds routes based on intermediate and adjacent road intersections towards the gateway. These routes are called backbone routes. In order to meet the end-to-end delay requirement, the selected backbone routes should have high connectivity probability. In low density roads, one way to increase the connectivity probability is to increase the road density increases, the transmission range should be reduced to avoid high interference, but the transmission range should still guarantee high connectivity. Hence in DTRP, the gateway will decide on

the transmission range that each vehicle should use in order to achieve high route connectivity. It is worth noting that VANETs exhibit different behaviors depending on the traffic volume. This implies a variation in the traffic patterns, which DTRP aims to mitigate.

In many of the proposed architectures, the authors also take into account the absence of fixed roadside network providing the VANET participants with mobile gateways. A multi-layer cooperation framework is proposed by Iera et al. (2007) that explores exactly this possibility. In this architecture the gateway, which can be either fixed roadside equipment or a mobile node, has a central role. The gateway must have the ability of both the external network and the vehicular network to match user preferences and QoS requirements. Furthermore, the gateway has to be provided with communication and negotiation capability towards the external network and also the VANET nodes. The roadside (fixed) gateways are more prone to route internet traffic, but there is no limitation since the "best" route is always chosen based on certain criteria. What's innovative in this approach is that while searching for the most efficient route the packets exchanged between the gateway and the sender node contain network information concerning delay, throughput, link lifetime, etc. The gateway, which is capable of interpreting that information, uses them additionally to make a decision about the best possible route.

Table 4: Characteristics of the reviewed QoS-enabled protocols for vehicular networks

	Link-Reliability	Maximization Throughput	End-to-End Delay Minimization
AMR	YES	N/A	YES
PVR	N/A	YES	YES
GVGrid	YES	N/A	N/A
CVIA-QoS	N/A	YES	YES
AODVM	N/A	N/A	YES
DTRP	YES	NO	NO

In this section, we have investigated vehicle-to-infrastructure communications, and the challenges that they pose to efficient QoS provision in vehicular environment. We explored the trade-offs that can greatly affect the quality of service provision in vehicular networks and presented additional detail on the weaknesses and strengths of the current research. We have also overviewed several vehicle-to-infrastructure quality of service provision schemes, mechanisms and targeted protocols and categorized them by employing various criteria. This categorization allowed us to identify the current problems of QoS provision in vehicular-to-infrastructure communications. We carefully reviewed these issues and illuminated the proposed solutions for each of them.

3.4 Routing and Message Forwarding Issues

Routing is one of the key research issues in vehicular networks as long as it supports most emerging applications. Vehicular communications require fast and reliable communication between cars (vehicle-to-vehicle) or between a car and a road side unit (vehicle-to-infrastructure). In the context of this chapter we only examine the vehicle-to-infrastructure side of the vehicular communication routing process. The greatest advantage of infrastructure-based communication is the fact that the density of the equipped cars needed for a working application is much smaller than in the case of a VANET.

3.4.1 Characteristics of Infrastructure-assisted Routing in Vehicular Networks

In this section of the chapter, we explore the case of infrastructure exploitation by routing protocols in order to improve the routing process in vehicular networks. Due to the fact that the improvement in routing achieved by infrastructure exploitation in vehicular networks is great, there has been an emerging set of routing protocols tailored specifically for vehicle-to-infrastructure environment.

Summarizing the above, the definitive characteristic of V2I communications in order to maximize the routing performance of the network is:

- *Infrastructure exploitation:* A situation that many protocols neglect is the existence of previous infrastructure along the roads. Such infrastructure consists of devices deployed by road operators and private telecommunications companies. Routing protocols could benefit a lot from those devices, which could act as relays, buffers, and so on. Moreover, useful information about the traffic state could be obtained from them, helping algorithms to make more intelligent decisions.

Several characteristics (Toor, Muhlethaler & Laouiti, 2008) of the vehicular environment that make routing a challenging task, are:

- *Highly Dynamic Topology:* Since vehicles are moving at high speed, the topology formed by VANETs is changing fast and dynamically.
- *Frequently Disconnected Network (Intermittent connectivity):* The highly dynamic topology results in frequently disconnected network since the link between two vehicles can quickly disappear while the two nodes are transmitting information. The problem is further exacerbated by heterogeneous node density where frequently traveled roads have more cars than non-frequently traveled roads. A robust routing protocol needs to recognize the frequent dis-connectivity and provides an alternative link quickly to ensure uninterrupted communication.
- *Propagation Model:* In VANETs, the propagation model is usually not assumed to be free space because of the presence of buildings, trees, and other vehicles. A VANET propagation model should well consider the effects of free standing objects as well as potential interference of wireless communication from other vehicles or widely deployed access points.

- *Network Penetration:* In vehicular networks, especially in vehicle-to-infrastructure communication, network penetration plays a really important role. In sparse or no infrastructure environments the routing process might be halted by factors such as roadside equipment absence or thin vehicle density. This can severely affect safety-related (life critical information) or infotainment-related applications and services. In that regard, we consider that network penetration is a key factor for the success of the routing, as of any other process or service in vehicular environment.

However, there are also disadvantages in the use of infrastructure in the routing process. This could seem as no surprise that avoiding the use of single point message aggregating equipment. Due to the high degree of the centralization, the server can become a bottleneck or even a single point of failure. However, the main reason not to use a centralized system for managing traffic information could very well be non-technical; it simply does not seem to be desirable to hand the control of this data over to one central authority, potentially limiting the access to data collected jointly by all traffic participants.

On the other hand there are some special traits to vehicular networks and their participants that help in making the routing process more efficient and improve the network performance in overall. Such traits are (Nekovee, 2005):

- *Patterned Mobility:* Vehicles follow a certain mobility pattern that is a function of the underlying roads, the traffic lights, the speed limit, traffic condition, and drivers' driving behaviors. Because of the particular mobility pattern, we can predict vehicle movement and design routing protocols exploiting this particular fact to make data dissemination in vehicular environment less challenging.

- *Unlimited Battery Power and Storage:* Nodes in VANETs are not subject to power and storage limitation as in sensor networks, another class of ad hoc networks where nodes are mostly static. Nodes are assumed to have ample energy and computing power. Therefore, optimizing duty cycle is not as relevant as it is in sensor networks.

- *On-board Sensors:* Nodes are assumed to be equipped with sensors to provide information useful for routing purposes. Many VANET routing protocols have assumed the availability of GPS unit from on-board Navigation system. Location information from GPS unit and speed from speedometer provides good examples for plethora of information that can possibly be obtained by sensors to be utilized to enhance routing decisions.

3.4.2 Routing Modes in Vehicular Communications: Vehicle-to-Infrastructure Broadcast

Data broadcast is an attractive solution for large scale data dissemination. In contrast to unicast, where a data item must be transmitted many times to answer multiple requests, broadcast has the potential to satisfy all outstanding requests for the same data item with a single response. The participation of RSU in the routing process involves broadcast techniques from the RSU to the participants of the network. The two most common ways, are the pull-based approach and the push-based approach. We then outline the basics about these two concepts (Vishal & Narottam, 2010).

A. Pull-based Broadcast Dissemination

In pull-based broadcast, commonly known as on demand broadcast, the RSU disseminates data items in response to explicit requests submitted by vehicles. Compared to its push-based counterpart, pull based is more scalable to large size databases. This broadcast model is reactive.

B. Push-based Data Dissemination

In push-based broadcast, the Road Side Unit broadcasts the whole or part of the database periodically according to a static broadcast program. All vehicles listen passively to the broadcast channel to retrieve data items of interest without sending any request. This broadcast model is proactive.

3.4.3 Infrastructure-assisted Routing: Proposed Solutions

In this subsection, we study several proposed solutions for VANET routing that improve the performance of the network by utilizing the roadside network. As mentioned in the quality of service subchapter, several routing protocols make use of the roadside network to provide quality of service in it, so we also explore these scenarios from the routing scope.

A protocol that we studied under a different scope in the quality of service subchapter is also examined here. Sun et al. (2006) propose the GVGrid routing protocol, namely. This protocol assumes that every node (vehicle) has a short range wireless device that has the same transmission range across the network nodes. GVGrid partitions the geographic region into squares of equal-size called grids. During route discovery, GVGrid attempts to find the route that is expected to have long lifetime, based on the position of each vehicle. This expected lifetime of a route is determined by the vehicles' movement on that route and characteristics (such as traffic signals and stop signs) of the roads on which the route is based.

In dense urban areas, where the traffic load grows exponentially, it is expected to have certain unavoidable delays in the routing of the messages. To mitigate the effect of those delays to the network's performance, Saleet et al. (2010) propose a delay tolerant routing protocol, namely DTRP. In DTRP, the gateway constructs a set of routes between itself and the mobile nodes based on its view about the local network topology. Nevertheless, one should note that if these routes consist of intermediate mobile nodes, these routes cannot be considered to be stable due to intermediate nodes' mobility. Hence in DTRP, the gateway will decide on the transmission range that each vehicle should use in order to achieve high route connectivity. It is worth noting that VANETs exhibit different behaviors depending on the traffic volume. This implies a variation in the traffic patterns, which DTRP aims to mitigate.

In the standardized (IEEE 802.11p) communication architecture for vehicular networks, a channel is always dedicated to safety messages. Based on that, Ferreira et al. (2009) proposed an infrastructure-based solution found in (Ferreira, Meireles & Fonseca, 2009), where the RSU play a major role in rebroadcasting warning messages in the network. In this approach there exists a control channel which is dedicated to service safety messages, along with a service channel to be used for the rest services. Every CCH interval will be divided into an Infrastructure Period (IP) and a Slotted Period (SloP). The IP is reserved for RSUs coordination and for beacon transmission by RSUs, where all vehicles should listen to the channel. The beacon contains information about the SloP. By using beacons, the RSU will know the time the event was triggered and, in the next beacon, will inform that a specific slot will be used to rebroadcast the message.

The TRAFIC Initiative

In (Brahmi et al., 2010), the TRAFIC initiative is explored, that utilizes the roadside infrastructure to improve routing in vehicular environment.

The TRAFIC project is a research and industrial initiative which aims to contribute to the global academic and industry effort to develop ITS systems. More specifically, TRAFIC defines a hybrid communication infrastructure that exploits the offered opportunities of inter-vehicle cooperation, as well as the advanced capabilities of communicating devices deployed along the roads. TRAFIC hybrid infrastructure gathers several communication components: a network infrastructure and a vehicular network. In particular, the network infrastructure consists of a wired/wireless access network (such as Wi-Fi/DSRC access points, WiMAX access, 2G/3G access, etc.), a backbone, and a sensor network. The access network ensures connectivity between the vehicular network and the backbone. The sensor network helps in detecting fine granularity traffic and security statistics related to roads and vehicles conditions while the backbone ensures the IP connectivity and houses the value-added services offered to vehicle users.

Based on this initiative and what it offers, Brahmi et al. (2010) propose the TRAFIC Efficient Routing Protocol (TERP) that uses the hybrid communication infrastructure proposed in TRAFIC. It defines an end-to-end efficient routing policy based on using two routing approaches: trajectory-based using SIFTv2 (Simple Forwarding over trajectory Version 2) protocol and dynamic decision-based routing using LoP (LTT over Progress) which targeted for V2I routing. Depending on the role of the packet forwarder (source or intermediate nodes) and applications requirements, TERP selects the appropriate routing approach. However, we only examine the V2I case of the operating scenario. LoP relies on TRAFIC communication infrastructure and more specifically the road side units (RSUs) deployed at road intersections. The RSUs can communicate with the vehicles within their coverage range and have knowledge of their local road topology (each RSU knows the neighboring RSUs).

Geographic routing also known as geocast has been one of the most popular approaches in infrastructure-aided routing. Borsetti et al. (2010) propose a routing scheme, based on geographic routing, to increase the reliability and range of multi-hop communications. The proposed approach works under the assumption that all the RSU components of the network have no delays to their inter-communications and they can be thought as one node in a network graph. Using this graph representation, topology-aware routing protocols would be able to compute more optimal routes and, when it is the case, efficiently route packets through the infrastructure.

In most cases, what infrastructure assistance can offer and which is difficult to achieve in a purely ad-hoc environment, is traffic comfort and traffic efficiency services (i.e digital map download, paid services, etc.). Shen et al. (2008) propose a routing protocol with RSU-assistance for vehicular environment and especially for internet access. The authors consider a hybrid VANET composed of vehicles constrained to move on roadways and sparse RSU deployment. This protocol works under the assumptions that every vehicle is equipped with a radio transceiver and a GPS receiver and have location awareness. Each RSU is directly connected to the Internet by high capacity cables, thus assuming that information can be exchanged among RSUs via the wired network with minimal delay. Additionally, both RSUs and vehicles are assumed to transmit at the same fixed power level. When a vehicle is out of transmission range of an RSU or physical obstacle block their communications, other vehicles will be used to relay the data traffic. Whenever a vehicle sends or relays a packet, it piggybacks its

current location and mobility information, and the corresponding timestamp in the packet. This way, an RSU can obtain location and mobility information of all vehicles in the area

In both ad-hoc and hybrid vehicular environment, a factor of outmost importance for the success of the routing process is vehicular density. Gupta et al. (2010) recognizing exactly this important parameter proposed an RSU-assisted routing algorithm, namely VD4. In VD4, every time a vehicle passes an RSU, the following information is sent to it; the time of arrival of the vehicle (as a timestamp), the speed of the vehicle, the direction of movement, the data packets (if it has any). The data packets that are received by the RSU are marked with a unique sequence number which is used to check for duplicity of the packet. If the packet is already present at the RSU, it is dropped otherwise it is forwarded to the farthest in range vehicle on the most optimal path as has been calculated by the delay model. However it must be noted that this algorithm operates in a network under several assumptions. It is assumed that, the vehicles are sufficiently equipped with wireless transmitters which can transmit in a short range (100 m - 200 m) for transmitting data packet whenever a vehicle reaches the vicinity of the original data packet carrying vehicle or to the RSU. Also every roadside intersection is equipped with a RSU, which is capable of storing data packets sent by vehicles as and when required. The information necessary for the proper routing is included by the source in the packet at the time of transmission. Each vehicle and RSU knows its present location using GPS. The RSU maintains the information of vehicles such as the speed, direction etc. that passed it and also an estimate of total number of vehicles present on each path at a given point in time. This information is periodically updated so that the evaluation of the optimal path may be done with the latest information. The vehicles are assumed to move with uniform speed on a path.

A representative example of infrastructure-assisted routing and how it can improve the network's performance is presented by Yanlin et al. (2006). The authors propose an RSU-assisted routing protocol. The RAR protocol is based on three concepts: sectors, advertisements, affiliations. A sector is the road surface between several RSUs. Advertisements are used to advertise new services and are broadcasted by the RSUs. When a vehicle receives an advertisement it must decide if it will enter the new sector. If and when a vehicle changes sector, it must also change its affiliation. This change is mandatory for the RSU to be able to locate the vehicle within the sector and forward any packages to it via wireless means. In this protocol the routing is singled-phased and involves discovering the best routes and using the RSUs as shortcuts. The infrastructure network is assumed to be a special sector and can decide based on the destination's address whether it is in the infrastructure network or in VANET. If the destination is in VANET, RSUs know the destination sector by querying other RSUs. At the end of this phase the best route is discovered and routing performance is improved by limiting ad-hoc routing in a small scope (sectors) and utilizing backbone networks.

Many of the proposed routing protocols support both ad-hoc and hybrid routing for vehicular networks. This happens mainly because of the indistinguishable nature of the vehicular networks and because it would be costly to develop a protocol for a single type of communication. Rongxi et al. (2008) propose a routing scheme for hybrid vehicular environment. In the context of this chapter, we only examine the vehicle-to-infrastructure part of this scheme. The basic concept is that, upon receiving a route request from a vehicle wanting to transmit data looks into its records to find out in which local peer group the destination belongs to. If the sender and the receiver move into the same group, the RSU update the corresponding fields in the received request and broadcasts the message to one-hop neighbors but also the neighboring RSUs. In the case that the sender and the destination moving in different local peer groups, the sender's RSU forwards the message to the

destination's local peer group in an attempt to find a reliable RSU close to the destination and identify the actual destination vehicle. Once all these preconditions have been met, the destination's RSU sends a message to the corresponding RSU on sender's side which in turn informs the sender vehicle to start transmitting data that are routed via the two RSUs to the destination.

In this subchapter, we have overviewed vehicle-to-infrastructure routing, which is one of the most challenging tasks for vehicular communications. We have presented the advantages and disadvantages of the infrastructure utilization to assist vehicular communications and particularly the routing process. We have examined in what degree the infrastructure penetration in the network affects the performance of the network and what effects this might have on safety or infotainment message dissemination. We have identified and analyzed the current problems that vehicular routing faces. Furthermore, we have aggregated and categorized several proposed solutions which include mechanisms, schemes and targeted protocols for this matter.

3.5 The Future of Vehicle-to-Infrastructure Communications

It is a fact that the V2I communication model is more expensive compared to its ad-hoc counterpart; however it is also a fact that the V2I communications have much yet to offer in all aspects of the vehicular environment, from active safety to infotainment services. Vehicular communications are becoming a reality because the market has recognized the significance that they will have in the near future. This alone gives a promising development for the proposed technologies. Market penetration will play an important role in this particular field due to the funds that will push its development. However, the penetration of vehicular network technology is still weak, and hence there is a need for a minimum of infrastructure support to increase the penetration by the provision of helpful services. At the same time, deploying new infrastructure for these networks necessitate a lot of investment and at a high cost. The main conclusion of the current chapter is that Vehicle-to-Infrastructure Communications will help towards the improvement of the active and passive road safety on the road.

3.6 Concluding Remarks

Concluding this chapter, we have discussed extensively about vehicular communications networks. In particular, we have analyzed the vehicle-to-infrastructure component of this hybrid network. We have also performed a survey on some of the most challenging tasks for V2I communications, such as security and privacy, quality of service provision and routing issues. We have investigated occasions in which the infrastructure element assisted in overcoming several problems, but also when it worsened the performance of the network. In each subchapter, we have provided a detailed categorization of the problems and challenges that exist in each respective field of interest, and presented several proposed solutions that make use of the infrastructure element to provide a solution for the studied problems. However, the realization for many of those scenarios still demands heavy deployment of the roadside infrastructure to support the network and the desired needs and applications.

KEY TERMS AND THEIR DEFINITION

1. **Vehicular Ad-hoc Network (VANET):** is a form of Mobile Ad-hoc Network (MANET), to provide communications among nearby vehicles.
2. **Mobile Ad-hoc Network (MANET):** is a type of ad hoc network that can change locations and configure itself on the fly.
3. **Vehicle-to-Vehicle Communication (V2V):** wireless communication between two vehicles equipped with short and medium range wireless communication capabilities.
4. **Vehicle-to-Infrastructure Communications (V2I):** wireless communication between a vehicle and an infrastructure (also termed as vehicle-to-roadside (V2R)).
5. **Wireless Local Area Network (WLAN):** a type of network in which a mobile user can connect to a Local Area Network (LAN) through a wireless (radio) connection.
6. **The IEEE 802.11p:** is the standard that specifies the technologies for vehicular communications.
7. **Dedicated Short Range Communication (DSRC):** is a short to medium range wireless protocol specifically designed for automotive use.
8. **The Intelligent Transportation Systems (ITS):** is a worldwide initiative to add information and communications technology to transport infrastructure and vehicles.

CHAPTER -4-

Chapter 4 – Introduction to Intelligent Transportation Systems

Introduction to Intelligent Transportation Systems

The growing need for mobility has increased in turn the number of vehicles occupying the urban areas, resulting in congestion problems accompanied by unpredicted emergencies and accidents. Inefficiencies in transportation system cause losses in time and human lives, high pollution and degradation of quality of life. In this respect, several innovative and cost-effective mobile services and applications for traffic networks are under investigation, emerging as the cornerstone of the so-called Intelligent Transportation Systems (ITS) [1].

As the number of cars on the road increases, so do the dangers and economic costs from automobile accidents. In the past, safety systems have focused on reducing driver injury in case of an emergency. Thus, the introduction of seat belts, air bags, and more recently products like OnStar, which can automatically contact emergency services and help locate the scene of an accident. The current trend in safety is not just to mitigate the effects of automobile accidents, but to prevent their occurrence all together. This involves making vehicles and roadways more intelligent through advanced mechanisms and electronic systems. The hope is that these new safety systems will be able to warn drivers of dangerous situations in time to take preventative actions.

The two areas of active research in ITS that attract the most attention in R&D projects are advanced sensor technology and inter-vehicle communications. With better sensors and data communication techniques, a driver can be more aware of his or her environment. This allows the driver to react appropriately to situations such as slippery roads and poor visibility. Adding vehicle-to-vehicle communications and drivers can share this information with each other, providing warnings before danger is imminent. Drivers can also be made more conscious of each other's location, so as to avoid intersection collisions and lane changing accidents. Vehicle-to-infrastructure communications are a venue for traffic management personnel to supply real-time updates on weather conditions and accident locations. In addition to safety related information, V2I communications provide drivers information that allows them to change their proposed route or departure time to avoid heavy traffic. The most significant goal for Intelligent Transportation Systems is for vehicles to improve the levels of efficiency and safety of mobility.

4.1 What are Intelligent Transportation Systems?

The term Intelligent Transport System refers to efforts to add information and communications technology to transport infrastructure and vehicles in an effort to manage factors that typically are at odds with each other, such as vehicles, loads, and routes to improve safety and reduce vehicle wear, transportation times, and fuel consumption. The scientific interest in ITS [2] comes from the problems caused by traffic congestion and a synergy of new information technology for simulation, real-time control, and communications networks. Traffic congestion has been increasing worldwide as a result of increased motorization, urbanization, population growth, and changes in population density. Congestion reduces efficiency of transportation infrastructure and increases travel time, air pollution, and fuel consumption.

4.2 The Deployment of Intelligent Transportation Systems

The urban infrastructure is being rapidly developed, providing an opportunity to build new systems that incorporate ITS [3] at early stages. However, for a large-scale deployment, deep market penetration of these technologies is required. In turn, market penetration requires public support through a strong perception of benefits to the consumers. A cost advantage to a system using an IEEE 802.11 standard is that inexpensive, mass produced consumer electronics are already being produced for this protocol. The cost will increase if it is found that these are not suitable in automobiles, and additional design work is needed. However, even before sufficient market penetration has been reached, vehicles with on-board sensor and communication capabilities can be used in data collection to evaluate system performance and to create a general knowledge base.

4.3 Applications of Intelligent Transportation Systems

Intelligent transport systems vary in technologies applied, from basic management systems such as car navigation; traffic signal control systems; container management systems; variable message signs; automatic number plate recognition or speed cameras to monitor applications, such as security CCTV systems; and to more advanced applications [4] that integrate live data and feedback from a number of other sources, such as parking guidance and information systems, weather information and bridge deicing systems. Additionally, predictive techniques are being developed to allow advanced modeling and comparison with historical baseline data.

4.4 Research and Future Trends on Intelligent Transportation Systems

Currently there is ongoing research in the field of ITS for several scenarios. The main interest is in applications for traffic scenarios, mobile phone systems, sensor networks and future combat systems [5]. Recent research has focused on topology related problems such as range optimization, routing mechanisms, or address systems, as well as security issues like traceability or encryption. In addition, there are very specific research interests such as the effects of directional antennas for ITS and minimal power consumption for sensor networks. Most of this research aims either at a general approach to wireless networks in a broad setting or focus on an extremely specific issue.

CHAPTER -5-

Chapter 5 – Collaborative Efforts for Safety and Security in Vehicular Communication Networks

5.1 Introduction

5.2 Security in Vehicular Environment

5.2.1 Security Challenges in Vehicular Communications

5.2.1.1 The IEEE 802.11p Standard

5.2.1.2 The IEEE 1609 Standard

5.3 R&D For Security In Vehicular Communications

5.4 Collaborative Efforts For Vehicular Communications

5.4.1 ITS Organizations and Initiatives

5.4.2 Worldwide Standardization Efforts

5.5 Concluding remarks

Collaborative Efforts for Safety and Security in Vehicular Communication Networks

George Kadas
CSSN Research Lab, Department of Informatics
Alexander TEI of Thessaloniki
Thessaloniki, Greece
E-mail: geokad@it.teithe.gr

Periklis Chatzimisios
CSSN Research Lab, Department of Informatics
Alexander TEI of Thessaloniki
Thessaloniki, Greece
E-mail: pchatzimisios@ieee.org

***Abstract*— Vehicular Communication Networks is a subcategory of Mobile Communications Networks which have the special characteristics of high node mobility and fast topology changes. In this paper, we outline the basic characteristics and concepts of vehicular communications while specifically investigating one of the most challenging tasks in vehicular network deployment, which is security provision. We investigate what makes the security provision a hard task in vehicular environment and examine the standardization activities that try to overcome this problem. Moreover, we present the efforts done by the scientific community to solve many critical issues that hold back the vehicular network's deployment but also support the Intelligent Transportation Systems development. Finally, we investigate standardization efforts concerning Vehicular Communications and ITS.**

Keywords-Vehicular Communications, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Security, Safety, Initiative Intelligent Transportation System (ITS)

5.1 Introduction

Vehicular communications have attracted the interest of both academia and industry, and that is because both high-speed motor-ways and the vehicles that drive on them are becoming increasingly intelligent.

According to Wu et al. (2005) a vehicular network organizes and connects vehicles with each other, and with mobile and fixed-locations resources. We utilize these mobile and fixed components and resources to improve both the safety and driving experience of the vehicular network participants. The emerging vehicular communications offer potential for the development of a wide variety of applications, ranging from safety to infotainment. The remainder of the paper is organized as follows. In section II, we outline basic characteristics and present the current challenges that exist for security provision in vehicular networks. In section III, we present several Research & Development (R&D) projects and solutions that have been striving to solve the problems that vehicular networks face towards their deployment. In section IV, we discuss the collaborative efforts around the world concerning vehicular networks and their deployment in a large scale. Finally, we conclude the paper in section V.

5.2 Security in Vehicular Environment

Security in VANETs is crucial as the very existence of VANET relates to life-critical information. We cannot argue about a deployable VANET unless there is security provision for both safety and infotainment applications. Due to the unique characteristics of a vehicular network, this provision of security cannot always be guaranteed.

5.2.1 Security challenges in Vehicular Communications

Being a special category of MANETs, VANETs have some unique characteristics that make its large scale deployment harder and pose some unique challenges [1]. For example, the information conveyed over a vehicular network may affect life-or-death decisions, making fail-safe security a necessity. However, providing strong security in vehicular networks raises important privacy concerns that must also be considered. The large-scale deployment of vehicular networks is rapidly approaching, and their success and safety will depend on viable security solutions acceptable to consumers, manufacturers and governments.

- *Authentication or Privacy?* During authentication all message transmissions need to be matched with their originating vehicles. On the other hand, personal information about vehicles should not be known to anyone else than the authority that manages identities. In order to achieve efficient VANET security, these two completely opposite traits must come to equilibrium. This tradeoff is called resolvable anonymity. Therefore a system needs to be introduced that enables message and therefore vehicles to be anonymous to the general nodes but also enables identification by central authorities in cases like accidents or malicious behavior.

- *Location Awareness:* Location-based service is essential to some extent, for most VANET applications to be truly effective, so that reliance of the VANET system on GPS or other specific location based instruments can be increased as any error in these is likely to effect in the VANET applications.

- *Highly Dynamic Environment:* Due to the highly dynamic environment of vehicular networks (vehicles moving at high speed leading to fast-changing topologies); the time windows available for communication are really narrow. This is a major spatial and temporal constraint of the network.

- *High Scalability:* With the number of vehicles increasing so does the potential load of vehicular network. While an honest majority policy has been adopted, in this great volume of vehicles the chance of malicious behavior increases exponentially.

- *Supporting Sustainability:* Due to its dynamic nature a vehicular network is highly disconnected. Often vehicles find themselves out of service, rendering the unable to operate at some level. Costly breakdowns or recovery operations are some of the downsides that we try to avoid.

However, despite all the challenges that vehicular network present to a sufficient security provision, there are some traits that supports that same security provision [11].

- *Patterned Mobility:* Vehicles follow a certain mobility pattern that is a function of the underlying roads, the traffic lights, the speed limit, traffic condition, and drivers' driving behaviors. Because of the

particular mobility pattern, we can predict vehicle movement and design roads and infrastructure deployment areas, exploiting this particular fact to make secure data transmission in vehicular environment less challenging.

- *Unlimited Battery Power and Storage:* Nodes in VANETs are not subject to power and storage limitation as in sensor networks, another class of ad hoc networks where nodes are mostly static. Nodes are assumed to have ample energy and computing power. Therefore, optimizing duty cycle is not as relevant as it is in sensor networks.

- *On-board Sensors:* Nodes are assumed to be equipped with sensors to provide information useful for security purposes. Many of that information can be utilized combined with other security mechanisms to thwart malicious attacks. Location information from GPS unit and speed from speedometer provides good examples for plethora of information that can possibly be obtained by sensors to be utilized to enhance VANET security.

5.2.1.1 The IEEE 802.11p Standard

In the discussion about vehicular communications, one could not miss to mention the only so far standardization for this kind of communications. That is the IEEE 802.11p standard [12] which has been developed to support both vehicle-to-vehicle and vehicle-to-infrastructure communications. This standardization includes the exchange between high-speed vehicles and between vehicles and fixed roadside equipment. It utilizes the Dedicated Short Range Communication (DSRC) to complete wireless transactions and operates on the licensed band for Intelligent Transportation Systems (ITS) of 5.9 GHz. The standard supports vehicle-based communications and services such as toll collection, safety services and commercial transactions via vehicles. These services involve greatly the vehicle-to-infrastructure communication model.

5.2.1.2 The IEEE 1609 Standard

IEEE 1609 standard family [13] also known as the upper layer Wireless Access in Vehicular Environments (WAVE) standard is used to define the architecture, communication model and mechanisms of high-speed short range wireless low latency communications. Together with 802.11p, P1609 standard family comprises the base of the WAVE architecture. The IEEE 1609 consists of 1609.1- Resource Manager, 1609.2 – Security services for Applications and Management Messages, 1609.3 – Networking Services, 1609.4 – Multi-channel Operations, 1609.11 - Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS).

5.3 R&D for Security in Vehicular Communications

Nowadays more than ever the need for fast and large-scale deployment of vehicular networks worldwide has become obligatory and the research worldwide has set its focus on this. Many Research & Development (R&D) projects have as their goal to develop such means of communication to be used in future vehicular networks. It is an international effort that holds a fair share of the scientific interest and resources and strives to provide solutions to most of the challenges that vehicular communications face.

However, in order to prepare for future deployment, much research remains to be conducted. This section studies the current (up to 2011) as well as the past research and technological environment in vehicle-to-vehicle and vehicle-to-infrastructure communications.

- ***EVITA:*** EVITA is an R&D project [18] that was funded under the 7th Framework Program (FP7). EVITA started in 2008 and is planned to end in the 4th quarter of 2011. During that time its objective is to design, verify and propose an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle.

- ***PRECIOSA:*** PRECIOSA is an FP7 R&D project [19] that started in 2008 and ended in the 4th quarter of 2010. While it was active its objectives were to define communication architecture for cooperative systems. Trust models for privacy, communication architecture, data storage privacy architecture, guidelines for cooperative privacy systems. Among the public deliverables of the PRECIOSA project are mechanisms for V2X privacy, models and privacy ontology for V2X, a V2X privacy verifiable architecture and others.

- ***INTERSAFE-2:*** INTERSAFE-2 [10], a FP7 project, is the successor of INTERSAFE that started in 2008 and is scheduled to terminate its operations in the 3rd quarter of 2011. As it predecessor, it aims for the elimination of intersection back-spots in roads and accident reduction through hybrid implementation and utilization.

- ***OFAV:*** OFAV [18] is a FP7 project that started in 2008 and is scheduled to end in the 4th quarter of 2013. The objective of this project is the development of an open architecture for future autonomous vehicles to become a standard platform shared by car makers in the design of next generation intelligent vehicles.

- ***SAFESPOT:*** Safespot [6] integrated project is co-funded by the European Commission of Informatics Society and Media and EUCAR. It started in 2006 and ended in 2010 and during that time its objective has been the development of a dynamic cooperative network that enables both vehicle and roadside infrastructure to communicate and share information in order to enhance the driver's perception of his surroundings. Since Safespot is a project that integrates smaller ones, we cannot enumerate all the deliverables of the subproject. Some of the deliverables of are, probe vehicles prototypes (of the SAFEPROBE project), on vehicle diagnostics and monitoring specifications (of the SCOVA project), etc.

- ***COOPERS:*** COOPERS [9] (Co-Operative Systems for Intelligent Road Safety) started in 2006 and completed its work in the 1st quarter of 2010.The focus of this project was on using V2V and V2R communications to create a driving environment where up-to-date traffic and weather information is available in time for drivers to adapt, increasing safety and reducing congestion. A test bench for I2V interfaces, including test vehicle, testing environment and test database are part of the contributions of COOPERS

- ***CVIS:*** The focus of CVIS [9] is research related to the necessary communications systems for V2V and V2I networks. A router has been developed that can interface "mobile cellular, wireless local area networks,

and infra-red to link vehicles continuously with roadside equipment and servers. The project wants to apply and validate the ISO 'CALM' standards for continuous mobile communication". Some of the things that the CVIS project has contributed in its duration are principles for a privacy-protective, secure, safe and fault tolerant design and a cooperative architecture and requirements on content interfaces for interoperability.

- ***SEVECOM:*** The SEVECOM [4] project addresses security and privacy aspects in V2V as well as V2I communications. The project focuses on security aspects such as privacy authentication and availability but also to operational requirements such as availability, scale, trust, etc. It also investigates way to thwart malicious behavior and attacks against the vehicular network. Among the deliverables of the SEVECOM project are security architecture and mechanisms for V2V / V2I communications and a baseline security specification according to the SEVECOM project.

- ***NETWORK ON WHEELS (NoW):*** The focus of NoW's [5] work is to deal with the technical and security issues related to protocols for V2V and V2I systems. The project hopes to support both safety and entertainment systems through wireless communications. The NoW project developed a hybrid scheme of network-layer and application-layer forwarding. Another accomplishment is comprehensive security architecture.

- ***PRESERVE:*** The Preserve project [16] was initiated in January 2011 with duration of 48 months, to end in the 4th quarter of 2014. The goal of PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) is to bring secure and privacy-protected V2X communication closer to reality by providing and field testing a security and privacy subsystem for V2X systems. By the time it ends, PRESERVE will have presented a complete, scalable, and cost-efficient V2X security subsystem that is close-to-market.

- ***AKTIV:*** AKTIV [15] is a German initiative that consists of three sub-projects, Traffic Management, Active Safety and Cooperative. Active Safety is occupied with the development of driver assistance systems with focus on safety-relevant applications. Traffic Management deal with the improvement of the performance of the road network. Lastly Cooperative Car aims to develop the necessary technology for cooperative vehicles applications.

- ***PREVENT:*** PREVENT [8] is a project funded by European automakers and the European Commission, and seeks to reduce the number of accidents through active safety systems. It is an umbrella project that consists of smaller projects that each one individually strives to improve active safety. The INTERSAFE project is part of PREVENT. Since PREVENT is an umbrella project, there are many deliverables from the subjects. However among the deliverables that the PREVENT project solely contributed are a driver warning system assessment of safety impact that describes a series of tests that were conducted in cooperation with the MAP&ADAS project.

5.4 Collaborative Efforts for Vehicular Communications

In today's society, vehicles play an indispensable role in delivering people and goods. As the deployment of vehicular communications becomes a necessity to modern societies, organizations around the world have set as their goal the rapid growth of ITS (Intelligent Transportation System). These organizations known as Intelligent Transportation Societies are active in several parts of the world, striving to promote R&D and ITS deployment.

In order to make IT systems a reality in the near future several standardization organizations are developing several communications standards and architectures that will be used to support ITS. Due to space limitation we only present some of the ITS organizations and standardization efforts in existence.

5.4.1 ITS Organizations and Intiatives

- ***ITS JAPAN:*** ITS Japan [20] consists of several public and private partners such as government ministries, academia, industry and private corporations. Its role is the promotion of R&D and deployment of ITS systems. It plays an important role as liaison between ITS-related public and private organizations and academia. Additionally it supports any ITS-relevant standardization activities.

- ***ITS AMERICA:*** ITS America [21] works with many public and private partners among other the U.S Department of Transportation and General Motors in order to promote collaboration and research in the vehicular communications area in order to accelerate the deployment of IT systems and improve the safety, security and efficiency on the surface's transportation system.

- ***ITS EUROPE:*** ITS Europe [22] also known as ERTICO connects public and private partners towards a common goal. Most of the R&D projects in Europe are managed by ERTICO while providing the necessary tools to get tangible results from those projects. The large-scale deployment of IT systems is also among the goals of the ERTICO, providing open and interoperable systems. Lastly it also provides information and guiding policy to ITS stakeholders to assist in its rapid and large-scale deployment.

5.4.2 Worldwide Standarization Efforts

- ***C2C-CC:*** The Car-2-Car Communication Consortium [10] was initiated by European car manufacturer's including BMW, Audi, Fiat, etc. Its main objective is the creation of an open European industry standard for CAR-2-X communication based on wireless LAN technology, to support efforts to achieve interoperability, to push for harmonization of worldwide standards, and to develop deployment strategies. The major focus of the consortium is road safety and traffic efficiency applications.

- ***ETSI:*** ETSI [10] is a European standardization organization, responsible for telecommunication standards in Europe. Concerning vehicular communications, an ITS committee has been founded under ETSI to assist in all levels of ITS deployment, such as application development, security and network issues etc.

- ***VIIC (U.S.A):*** Vehicle Infrastructure Integration Consortium [7] has as its objective the deployment of an enabling communications infrastructure that supports vehicle-to-infrastructure as well as vehicle-to-vehicle communications for a wide variety of applications.

- ***CALM:*** C.A.L.M [10;23] which stands for Communication Access for Land Mobiles is an initiative started by ISO TC 204/Working Group 16 that aims to develop a family of international standards. This family of standards specifies a common architecture, network protocols and communication interface definitions for wired and wireless communications using various access technologies including cellular 2nd generation, cellular 3rd generation, satellite, infra-red, 5 GHz micro-wave, 60 GHz millimeter-wave, and mobile wireless broadband. These and other access technologies that can be incorporated are designed to provide broadcast, unicast and multicast communications between mobile stations, between mobile and fixed stations and between fixed stations in the "Intelligent Transport Systems" (ITS) sector.

5.5 Concluding remarks

In the future, with the help of wireless communications, each automotive vehicle will be a unique node on the global communications network. This vehicular communications network will effectively support interactions within the automobile and with the surrounding environment, fixed or mobile. Many potential applications and services that will be supported include safety, security, real-time traffic monitoring, health and status of the vehicles, user services, passenger entertainment, and more efficient use of the transportation and telecommunications infrastructure. The current paper investigated the security issues that may rise in vehicular communications, but also presented a detailed taxonomy of the initiatives, R&D projects and organizations worldwide that strive to solve many open issues in vehicular communications connected directly or indirectly to security provision. However there are some important challenges facing this emerging environment, which are the maturity of the technology, the value of the services performed, the business models and rationale for creating such networks in the first place, and the complex regulatory regime and standards that must be established. Car makers, government policy, business models and international standards activities, that are a major research interest of this paper, will play essential roles for the success of automotive telematics applications and services. Significant R&D effort remains to be done to bring alive the vision of future intelligent vehicular applications, which will be supported by vehicular communications.

Thesis Conclusion

This thesis presented and examined several aspects of a state-of-the-art field in vehicular networks and communications. Two papers were authored during the preparation of the current thesis that aim to shed light in some of the most challenging tasks in Vehicular Ad-hoc Networks. We summarized several simple and complex concepts of the Vehicular Ad-hoc Networks and examined how roadside support enhances or downgrades the performance of the network. We also studied a major drive towards the development and deployment of vehicular communications, which is Intelligent Transportation Systems, whose main focus is driver and passenger safety, but also in the recent years driving assistance and comfort provision. That which was illustrated while authoring this thesis is that vehicular networks have great benefits to offer in both road conditions and safety as well as to the socio-economic growth of societies.

Bibliography and References

(Sorted per Chapter and Order of Appearance)

CHAPTER -1-

[1] Andrea Tonnesen. Mobile Ad-hoc Networks. www.olsr.org/docs/wos3-olsr.pdf.

[2] Olariu Stephan, Weigle C. Michele (Eds.), (2009), "Vehicular Networks From Theory to Practice", CRC Press.

[3] Hassnaa Moustafa, Yan Zhang (Eds.), (2009), "Vehicular Networks Techniques, Standards and Applications", CRC Press.

[4] Yue Liu, Jun Bi, Ju Yang, "Research on Vehicular Ad Hoc Networks", Chinese Control and Decision Conference (CCDC), 2009. Page(s): 4430 – 4435.

[5] R. Uzcategui and G. Acosta-Marum, "Wave: a tutorial", IEEE Communications Magazine, vol. 47, no. 5, pp. 106–133, 2009.

[6] Morgan, Y.L, "Notes on DSRC & WAVE Standards Suite: Its Architecture, Design, and Characteristics", *Communications Surveys & Tutorials, IEEE*, vol.12, no.4, pp.504-518, Fourth Quarter 2010

[7] Anand R. Prasad, Neeli R. Prasad, "802.11 WLANs and IP Networking: Security, QoS and Mobility", Artech House, April 2005.

[8] G. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X.P. Costa, B. Walke, "The IEEE 802.11 universe", IEEE Communications Magazine, vol.48, no.1, pp.62-70, January 2010.

[9] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments", IEEE Vehicular Technology Conference, (VTC Spring 2008), pp. 2036–2040, May 2008.

[10] M. Gast, "802.11 Wireless Networks: The Definitive Guide, Second Edition", Sebastopol: O'Reilly Media, Inc., 2005.

[11] IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std

802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009) , pp.1-51, July 15 2010.

[12] Wiesbeck Werner, Reichardt Lars, (2010), "C2X Communications Overview", *URSI International Symposium on Electromagnetic Theory*, pp. 868-871.

[13] IEEE Standards Association, IEEE P1609.1—Standard for Wireless Access in Vehicular Environments (WAVE)—Resource Manager, IEEE P1609.2—Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages, IEEE P1609.3—Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services, IEEE P1609.4— Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operations, adopted for trial-use in 2007, IEEE Operations Center, 445 Hoes Lane, Piscataway, NJ, 2007.

[14] http://wireless.fcc.gov/services/its/dsrc , (last accessed 2/5/2011), The FCC DSRC (Dedicated Short Range Communications).

[15] http://www.standards.its.dot.gov (last accessed 15/5/2011) , SAE J2735 ITS Standard.

[16] K.-Y. Ho, P.-C. Kang, C.-H. Hsu, and C.-H. Lin, "Implementation of WAVE/DSRC devices for vehicular communications", in Computer Communication Control and Automation (3CA), 2010 International Symposium on, vol. 2, May 2010.

CHAPTER -2-

ƀ

CHAPTER -3-

Overview and Background of VANETs

Hassnaa Moustafa, Yan Zhang (Eds.), (2009), Vehicular Networks Techniques, Standards and Applications, CRC Press.

"IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std

802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009) , pp.1-51, July 15 2010.

Wiesbeck Werner, Reichardt Lars, (2010), C2X Communications Overview, *URSI International Symposium on Electromagnetic Theory*, pp. 868-871.

Kamini, Rakesh Kumar, (2010, September), VANET Parameters and Applications: A Review, *Global Journal of Computer Science and Technology*, 10, Issue 7, pp. 72-77.

IEEE Standards Association, IEEE P1609.1—Standard for Wireless Access in Vehicular Environments (WAVE)—Resource Manager, IEEE P1609.2—Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages, IEEE P1609.3—Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services, IEEE P1609.4— Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operations, adopted for trial-use in 2007, IEEE Operations Center, 445 Hoes Lane, Piscataway, NJ, 2007.

Olariu Stephan, Weigle C. Michele (Eds.), (2009), Vehicular Networks From Theory to Practise, CRC Press.

Motsinger Caitlin, Hubbing Todd., (2007), A review of vehicle-to-vehicle and vehicle-to-infrastructure initiatives (Tech Rep No. 3). USA, South Carolina, Clemson: University of Clemson, Vehicular Electronics Laboratory.

Stampoulis A., and Chai Z., (2007), Survey of Security in Vehicular Networks (Technical Report), Project CPSC 534

H.T.Cheng, Hangguan Shan**,** Weihua Zhuang, (In Press), Infotainment and road safety service support in vehicular networking: From a communication perspective, *Mechanical Systems and Signal Processing Journal*.

Yue Liu, Jun Bi, Ju Yang, (2009), Research on Vehicular Ad Hoc Networks, *Control and Decision Conference, CCDC '09*, pp. 4430-4435.

Security

F. Dötzer, (2005), Privacy issues in vehicular ad hoc networks, *in Proceedings of the Workshop on Privacy Enhancing Technologies (PET)*, ACM Press.

P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya. (2007), Architecture for secure and private vehicular communications, *ITST '07, 7th International Conference on ITS Telecommunications*, pp. 1-6.

K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki., (2005), CARAVAN: providing location privacy for VANET, *In Workshop on Embedded Security in Cars*.

P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux,, (2008, November), Secure vehicular communication systems: Design and architecture, *IEEE Communications, 46*, pp. 100-109.

G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy., (2007), Efficient and robust pseudonymous authentication in VANET, *Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 19–28.

P. Wohlmacher, (2000), Digital Certificates: A Survey of Revocation Methods, *ACM Workshop*, pp. 111–114.

M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux., (2007, October), Eviction of Misbehaving and Faulty Nodes in Vehicular Networks, *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, 25(8), pp. 1557–1568.

Jinhua Guo; Baugh, J.P.; Shengquan Wang, (2007, May), "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework", *Mobile Networking for Vehicular Environments Conference*, pp.103-108, IEEE.

Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) *CRYPTO 2004. LNCS*, 3152, pp. 41–55. Springer, Heidelberg (2004).

Xiaoting Sun, Xiaodong Lin, Pin-Han Ho, (2007), Secure Vehicular Communications Based on Group Signature and ID-Based Signature Scheme*, IEEE International Conference on Communications* pp.1539-1545, IEEE.

Dhurandher, S.K., Obaidat, M.S., Jaiswal, A., Tiwari, A., Tyagi, A., (2010), Securing vehicular networks: A reputation and plausibility checks-based approach, *GLOBECOM Workshops*, pp.1550-1554.

Serna, J., Luna, J., Medina, M., (2008), Geolocation-Based Trust for Vanet's Privacy, *Fourth International Conference on Information Assurance and Security*, pp.287-290.

Wex, P., Breuer, J., Held, A., Leinmuller, T., Delgrossi, L., (2008), Trust Issues for Vehicular Ad Hoc Networks, *Vehicular Technology Conference*, pp.2800-2804, IEEE.

Felix Gomez Marmol, Gregorio Martinez Perez, (In Press), TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, *Network and Computer Applications Journal*.

A. Perrig, R. Canetti, J. Tygar, and D. Song, (2002), The TESLA broadcast authentication protocol, *RSA CryptoBytes Newsletter*, 5, pp. 2–13.

A. Studer, F. Bai, B. Bellur, and A. Perrig, (2008), Flexible, extensible, and efficient VANET authentication, *In Proceedings of 6th Annual Conference on Embedded Security in Cars*.

Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, (2008), RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks*, IEEE International Conference on Communications*, pp.1451-1457, IEEE.

Studer, A., Shi, E., Fan Bai, Perrig, A., (2009), TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs, *In Proceedings of 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp.1-9, IEEE.

Wasef, A., Xuemin Shen, (2009), MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks, *In Proceedings of Global Telecommunications Conference*, pp.1-6, IEEE.

Wasef, A., Xuemin Shen., (2009), ASIC: Aggregate Signatures and Certificates Verification Scheme for Vehicular Networks", *In Proceedings of Global Telecommunications Conference*, pp.1-6, IEEE.

G. Yan, S. Olariu, and M. C. Weigle, (2008, July), Providing VANET Security through Active Position Detection, *Computer Communications: Special Issue on Mobility Protocols for ITS/VANET*, 31, pp. 2883-2897.

Leping Huang; Matsuura, K., Yamane, H., Sezaki, K., (2005), Enhancing wireless location privacy using silent period, *Wireless Communications and Networking Conference*, pp. 1187-1192, IEEE.

D. Boneh and X. Boyen., (2004, May), Short signatures without random oracles, In C. Cachin and J. Camenisch, (Eds.), *Eurocrypt 2004 Conference*, pp. 56–73.

Langley, C., Lucas, R., Huirong Fu, (2008), Key management in vehicular ad-hoc networks, *In Proceedings of International Conference on Electro/Information Technology*, pp.223-226, IEEE.

Soyoung Park, Aslam, B., Turgut, D., Zou, C.C., (2009), Defense against Sybil attack in vehicular ad hoc network based on roadside unit support, *Military Communications Conference*, pp.1-7, IEEE.

Hubaux, J.P., Capkun, S., Jun Luo, (2004, May), The security and privacy of smart vehicles, *IEEE Security & Privacy*, 2, pp.49-55.

J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, J-P. Hubaux, (2007), Mix-Zones for Location Privacy in Vehicular Networks, *1st International Workshop on Wireless Networking for Intelligent Transportation Systems*.

Cencioni, P. Di Pietro, R., (2007), VIPER: A vehicle-to-infrastructure communication privacy enforcement protocol*, IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems*, pp.1-6, IEEE.

Haas, Jason J., Hu, Yih-Chun, Laberteaux, Kenneth P., (2010), The Impact of Key Assignment on VANET Privacy, *In Proceedings of 1st International Workshop on Security and Communication Networks*, 3, pp. 233-249, John Wiley & Sons, Ltd.

Rawat, D.B. Treeumnuk, D. Popescu, D.C. Abuelela, M. Olariu, S., (2008), Challenges and perspectives in the implementation of NOTICE architecture for vehicular communications, *In Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp.707-711, IEEE.

Nai-Wei Lo, Hsiao-Chien Tsai, (2007), Illusion Attack on VANET Applications - A Message Plausibility Problem, *in Proceedings of the 2nd IEEE Workshop on Automotive Networking and Applications (AutoNet '07)*, pp.1-8, 26-30, IEEE.

Quality of Service

Saleet, H., Langar, R., Basir, O., Boutaba, R., (2009), Adaptive Message Routing with QoS Support in Vehicular Ad Hoc Networks, *Global Telecommunications Conference*, pp.1-6, IEEE.

Ksentini, A., Tounsi, H., Frikha, M., (2010), A proxy-based framework for QoS-enabled Internet access in VANETS, *Second International Conference on Communications and Networking*, pp.1-8.

Sun, W., Yamaguchi, H., Yukimasa, K., Kusumoto, S., (2006), GVGrid: A QoS Routing Protocol for Vehicular Ad Hoc Networks, *14th IEEE International Workshop on Quality of Service*, pp.130-139, IEEE.

Y. Zhang, J. Zhao, and G. Cao, (2007), On scheduling vehicle-roadside data access, *ACM International Workshop on VehiculAr Inter-NETworking ACM VANET*, pp. 10–19, ACM Press.

Korkmaz, G., Ekici, E., Ozguner, F., (2006), Internet access protocol providing QoS in vehicular networks with infrastructure support, *Intelligent Transportation Systems Conference ITSC*, pp.1412-1417, IEEE.

Alcaraz, J., Vales-Alonso, J., Garcia-Haro, J., (2009), Control-based scheduling with QoS support for vehicle to infrastructure communications, *Wireless Communications*, 16, pp.32-39, IEEE.

Ramirez CL, Veiga MF, (2007), QoS in vehicular and intelligent transport networks using multicast routing, *IEEE international symposium on industrial electronics*, pp. 2556–2561, IEEE.

Saleet, H., Langar, R., Naik, S., Boutaba, R., Nayak, A., Goel, N., (2010), QoS Support in Delay Tolerant Vehicular Ad Hoc Networks, *IEEE Global Telecommunications Conference*, pp.1-6, 6-10, IEEE.

Antonio Iera, Antonella Molinaro, Sergio Polito, Ruggeri G., (2008), A Multi-Layer Cooperation Framework for QoS-Aware Internet Access in Vanets, *Ubiquitous computing and communication journal*, Special issue of UbiRoads, pp. 10-19.

Routing

Ferreira, N. Meireles, T. Fonseca, J.A., (2009), An RSU coordination scheme for WAVE safety services support, *IEEE Conference on Emerging Technologies & Factory Automation*, pp.1-4, IEEE.

Brahmi, N. Boukhatem, L. Boukhatem, N. Boussedjra, M. Nuy, N. Dau Labiod, H. Mouzna, J. , (2010), End-to-end routing through a hybrid ad hoc architecture for V2V and V2I communications, *The 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop*, pp.1-8.

Borsetti, D. Gozalvez, J., (2010), Infrastructure-assisted geo-routing for cooperative vehicular networks, *Vehicular Networking Conference*, pp.255-262, IEEE.

Shen Wan, Jian Tang, Wolff, R.S., (2008), Reliable Routing for Roadside to Vehicle Communications in Rural Areas, *IEEE International Conference on Communications*, pp.3017-3021, IEEE.

Gupta, A. Chaudhary, V. Kumar, V. Nishad, B. Tapaswi, S., (2010), VD4: Vehicular Density-Dependent Data Delivery Model in Vehicular Ad Hoc Networks, *Sixth Advanced International Conference on Telecommunications*, pp.286-291.

Yanlin Peng, Abichar, Z. Chang, J.M., (2006) Roadside-Aided Routing (RAR) in Vehicular Networks, *IEEE International Conference on Communications*, pp.3602-3607, IEEE.

Rongxi He, Rutagemwa, H. Xuemin Shen, (2008), Differentiated Reliable Routing in Hybrid Vehicular Ad Hoc Networks, *IEEE International Conference on Communications*, pp.2353-2358, IEEE.

Toor, Y. Muhlethaler, P. Laouiti, A., (2008), Vehicle Ad Hoc networks: applications and related technical issues, *Communications Surveys & Tutorials, IEEE*, 10, pp.74-88, IEEE.

P. Papadimitratos, V. Gligor, and J.-P. Hubaux, (2006), Securing vehicular communications - assumptions, requirements, and principles, *in Proccedings of Workshop on Embedded Security in Cars*.

Vishal Kumar & Narottam Chand, (2010), Data Scheduling in VANETs : A Review, *International Journal of Computer Science & Communication*, 1(2), 399-403.

Nadeem Tamer, Shankar Pravin, Iftode Liviu, (2006), A Comparative Study of Data Dissemination Models for VANETs, *Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pp.1-10.

Nekovee, M. (2005) Sensor networks on the road: the promises and challenges of vehicular adhoc networks and vehicular grids, *In Proceedings of the Workshop on Ubiquitous Computing and e-Research*, Edinburgh, UK.

Blum, J., Eskandarian, A. & Hoffmman, L., (2004), Challenges of inter-vehicle ad-hoc networks, *IEEE Trans. Intelligent Transportations Systems*, 5(4), pp. 347-351.

Tsugawa, S. (2005), Issues and recent trends in vehicle safety communication systems, IATSS Research, *Journal of International Association of traffic and safety sciences*, 29(1), pp. 7-15.

International Organization for Standardization, Intelligent Transport System-Continuous Air Interface Long and Medium—Medium Service Access Point, Draft International Standard ISO/DIS 21218, 2007.

Japan Ministry of Land, Infrastructure and Transport, Road Bureau, Smartway 2007 Public Road Test, available at http://www.its.go.jp/ITS/topindex/topindex_sw2007.html, 2007.

Xin Wang, Georgios B. Giannakis, Antonio G. Marques, (2007), A Unified Approach to QoS Guaranteed Scheduling for Channel-Adaptive Wireless Networks, *Proceedings of the IEEE journal*, 95(12), pp. 2410-2431, IEEE.

Sichitiu M.L., Kihl M., (2008), Inter-vehicle communication systems: a survey, *Communications Surveys & Tutorials*, 10(2), pp.88-105, IEEE.

CHAPTER -4-

[1] Olariu Stephan, Weigle C. Michele (Eds.), (2009), Vehicular Networks From Theory to Practise, CRC Press.

[2] Dimitrakopoulos G., Demestichas, P., “Intelligent Transportation Systems”, IEEE Vehicular Technology Magazine, vol.5, no.1, pp.77-84, March 2010.

[3] Motsinger Caitlin, Hubbing Todd., (2007), “A review of vehicle-to-vehicle and vehicle-to-infrastructure initiatives (Tech Rep No. 3)” USA, South Carolina, Clemson: University of Clemson, Vehicular Electronics Laboratory.

[4] Kamarudin, A., Riza Atiq A., Rozmi, I., “Intelligent Transports System for motorcycle safety and issues”, European Journal of Scientific Research, 28 (4) 600-611, 2009.

[5] Papadimitratos, P.; La Fortelle, A.; Evenssen, K.; Brignolo, R.; Cosenza, S.; “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation”, IEEE Communications Magazine, IEEE , vol.47, no.11, pp.84-95, November 2009.

CHAPTER -5-

[1] Raya, M. and Hubaux, J., "The Security of Vehicular Ad Hoc Networks", in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), Alexandria, VA, pp 1 – 11.

[2] Stampoulis, A. & Chai, Z., A Survey of Security in Vehicular Networks, http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf.

[3] Jiang, D. & Delgrossi, L., "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments", in Proceedings of 67th IEEE Vehicular Technology Conference on Vehicular Technology, May 2008, pp. 2036-2040.

[4] Sevecom, Mission and Objectives. (n.d.). Available at: http://www.sevecom.org/Pages/Objectives.html

[5] Network on Wheels. (n.d.). About. Available at: http://www.network□]on□]wheels.de/about.html

[6] SAFESPOT: Factsheet. Retrieved April, 15, 2011, Available at: http://ec.europa.eu/information_society/activities/esafety/doc/rtd_projects/fact_sheets/call_4/safespot.pdf

[7] VII Consortium, "Final Report: Vehicle Infrastructure Integration Proof of Concept Proof of Concept Results and Findings Summary – Vehicle", May 2009.

[8] PReVENT. (n.d.). Available at: www.prevent-ip.org/en

[9] Motsinger Caitlin, Hubbing Todd., (2007), A review of vehicle-to vehicle and vehicle-to-infrastructure initiatives (Tech Rep No. 3). USA, South Carolina, Clemson: University of Clemson, Vehicular Electronics Laboratory.

[10] Olariu Stephan, Weigle C. Michele (Eds.),*Car-2-X Communications in Europe* in *Vehicular Networks: From Theory to Practise*, CRC Press, 2009, 112-143.

[11] Nekovee, M. Sensor networks on the road: the promises and challenges of vehicular adhoc networks and vehicular grids, *In Proceedings of the Workshop on Ubiquitous Computing and e-Research*, Edinburgh, 2005.

[12] "IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," IEEE Std 802.11p-2010

(Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009) , pp.1-51, July 15 2010

[13] IEEE Standards Association, IEEE P1609.1—Standard for Wireless Access in Vehicular Environments (WAVE)—Resource Manager, IEEE P1609.2—Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages, IEEE P1609.3—Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services, IEEE P1609.4— Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operations, adopted for trial-use in 2007, IEEE Operations Center, 445 Hoes Lane, Piscataway, NJ, 2007.

[14] Wu, H., Fujimoto, R., Hunter, M., & Guensler, R. An architecture study of infrastructurebased vehicular networks. In *ACM MSWiM,* Montreal, Canada, 2005, (pp.36-39).

[15] AKTIV. (n.d.) Available at: http://www.aktiv online.org/english/projects.html

[16] About, PRESERVE. (n.d.) Available at: http://www.preserve-project.eu/about

[17] About, OFAV. (n.d.) Retrieved April, 29, 2011 from http://ec.europa.eu/research/fp7/pdf/19072010/ofav_-_erc_story.pdf

[18] About, EVITA. (n.d.) Retrieved April, 29, 2011 from http://evita-project.org/Publications/Seu09.pdf

[19] About, PRECIOSA (n.d.) Available at: http://www.preciosa-project.org/

[20] What is ITS Japan (n.d.) Available at: http://www.its-jp.org/english/what_its_e/

[21] About, ITS America (n.d.) Available at: http://www.itsa.org/aboutus/c3/About_Us.html

[22] About, ITS Europe (n.d.) Available at: http://www.ertico.com/about-ertico/

[23] About C.A.L.M (n.d.) Available at: http://www.isotc204wg16.org/conce