UNIVERSIDADE DO ALGARVE

Quality of Service and Security in Future Mobile Technologies

Diyar Khairi M S

PhD Thesis in Informatics Engineering

Work done under the supervision of: Prof. Dr. Pedro Guerreiro and
Prof. Dr. Amine Berqia
2016

Statement of Originality

Quality of Service and Security in Future Mobile Technologies

Statement of authorship: The work presented in this thesis is, to the best of my knowledge and belief, original, except as acknowledged in the text. The material has not been submitted, either in whole or in part, for a degree at this or any other university.

Candidate:

_____

(Diyar Khairi M S)

Abstract

Future networks will comprise a wide variety of wireless networks. Users will expect to be always connected from any location, and, as users move, connections will be switched to available networks using vertical handover techniques.

The current approach of the operators is a centralized network, and the mobility management is done at the infrastructure level. The decentralized mobility management is another approach developed in many researches, however, not widely deployed. We are interested in this type of decentralized mobility management, especially in a highly dynamic environment when the network topology changes frequently.

We choose a particular case study, Vehicular Ad-hoc Networks (VANETs), which are a new emerging network technology derived from ad-hoc networks and are an example of future networks. In the field of Intelligent Transportation Systems (ITS), communications without a wire between vehicles (V2V) appear as an accident prevention solution offering a wider vision than conventional sensors. By linking vehicles to telecommunications network (V2I), new perspectives are offered both passengers and driver with conventional communication applications such as access Internet, e-learning, games or chat. This means that future mobile networks like VANETs will have to integrate communications, mobility, Quality of Service (QoS) and security.

We mainly interested in three issues: mobility, QoS and security. These three issues are intrinsic to vehicles on motorway networks. We need to simultaneously manage QoS and security while taking into account users mobility. In this thesis, we propose to contribute on how to improve security without degrading the quality of service QoS in a highly mobile environment as VANETs networks. To answer this research question, we use simulations and experiments. Simulation using Network Simulator 2 (NS2) will be used to show that security schemes have significant impacts on the throughput QoS, and our proposed schemes can substantially improve the effective secure throughput with cooperative communications.

Keywords: VANETs, QoS, Security, Mobility, Intelligent Transportation Systems (ITS).

Resumo

As redes futuras serão constituídas por uma grande variedade de redes sem fios. Os utilizadores quererão estar ligados em permanência, seja qual for a sua localização. Para isso, quando os utilizadores se deslocam de um ponto para outro, terão de se religar automaticamente a outras redes, usando técnicas de handover vertical.

Atualmente, a abordagem predominante baseia-se na utilização de uma rede centralizada, em que a mobilidade é realizada ao nível da infraestrutura. Uma outra abordagem, preferida por muitos investigadores, é a gestão descentralizada da mobilidade, a qual, no entanto, não é ainda muito utilizada. O nosso interesse reside precisamente neste tipo de gestão descentralizada, especialmente em ambientes muito dinâmicos em que a topologia da rede muda frequentemente.

Escolhemos neste trabalho as redes veiculares ad hoc, em inglês, *vehicular ad hoc networks* (VANETs). Estas redes representam uma nova tecnologia, derivada das redes ad hoc, e representam um exemplo de redes futuras. No domínio dos sistemas de transporte inteligentes, as comunicações sem fio entre veículos constituem um mecanismo de prevenção de acidentes rodoviários, com a vantagem de permitirem um perímetro de visão mais alargado do que o fornecido pelos sensores convencionais. Ao ligar veículos às redes de telecomunicações, abrem-se nova perspetivas, para os passageiros e para os condutores, por via do acesso a aplicações convencionais, tais como a Internet, o ensino a distância, os jogos online, as redes sociais, por exemplo. Isto implica que as redes mòveis do futuro, e as VANETs em particular, terão de conjugar as comunicações com a mobilidade, a qualidade do serviço e a segurança.

Interessam-nos sobretudo estas três questões: mobilidade, qualidade de serviço e segurança. Todas elas são intrínsecas aos veículos que circulam em estradas equipadas com redes de comunicações. O problema principal é gerir a qualidade de serviço e a segurança tendo em atenção que os utilizadores estão em movimento. Nesta tese, propomo-nos contribuir para aumentar a segurança sem comprometer a qualidade de serviço, em redes altamente mòveis, tais como as VANETs. A esta questão de investigação, damos resposta por meio de simulações e de experiências. Em particular, realizaremos simulações usando o software Network Simulator 2 para mostrar que os esquemas de

garantia de segurana têm um impacto significativo no desempenho da rede. Complementarmente, mostramos que os esquemas alternativos por nós propostos, baseados em comunicações cooperativas, são capazes de melhorar o desempenho esperado, sem colocar em risco a segurança.

Palavras-chave: VANETs, QoS, mobilidade, sistemas de transporte inteligentes.

Acknowledgements

I would like to express my special appreciation and thanks to my advisors and supervisors Professor Dr. Amine Berqia and Professor Dr. Pedro Guerreiro, you have been tremendous mentors for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career have been invaluable.

I like to have a great special thank for the lovely and beauties country I have ever seen PORTUGAL for all the hospitality and lovely years I spend over there.

I would also like to thank my committee members, for serving as committee members even at hardship. I also want to thank you for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

To all my friends, thank you for your understanding and encouragement in my many, many moments of crisis. Your friendship and your existence makes my life a wonderful experience. I cannot list all the names here, but you are always on my mind.

I feel very special because there is always an angel voice inside my mind giving me strength to reach for the stars and chase my dreams and being there for me throughout the entire PhD program and my life.

A special thanks to my family. Your prayer for me was what sustained me thus far. God bless you all.

Thank my God for letting me through all the difficulties. I have experienced your guidance day by day. You are the one who let me finish my degree. I will keep on trusting you for my future. Thank you, Allah.

Contents

Statement of Originality i

Abstract ii

Resumo iii

Acknowledgements v

Nomenclature xii

I Introduction 1

1 Introduction 2

1.1 Background 2
1.2 Problem statement 7
1.3 Research Question 9
1.4 Thesis Outline 9

II Background on MANETs and VANETs 11

2 Background on MANETs and VANETs 12

2.1 Introduction 12
2.2 Introduction to wireless networks 13
2.3 Mobile Wireless Ad-hoc Networks (MANETs) 15
2.3.1 The evolution of MANETs 16
2.3.2 The Characteristics of MANET 16
2.3.3 Advantages of mobile ad hoc networks 17
2.3.4 Applications of mobile ad hoc networks 18
2.4 Vehicular ad hoc networks (VANETs) 20
2.4.1 Vehicle to Vehicle communication V2V 22
2.4.2 Vehicle communication with use of infrastructure V2I 23
2.4.3 Hybrid communication 24

2.5 Conclusion 24

III Standards of communication and challenges in VANETs 25

3 Standards of communication and challenges in VANETs 26

3.1 Standards of Communication in VANETs 26

3.1.1 Protocols WAVE and IEEE 802.11p 27

3.1.2 Access Techniques at the MAC level channel 28

3.2 Challenges in VANETs 30

3.2.1 Quality of Service In VANETs 30

3.2.2 Security In VANETs 34

3.3 Conclusion 38

IV Improving QoS in MANETs
***"Improving tcp performance in manet by exploiting mac layer algorithms. IRACST-International Journal of Research in Management & Technology (IJRMT), 2011. Published"* 39**

4 Improving QoS in MANETs 40

4.1 Introduction 40

4.2 Interactions between MAC and TCP 41

4.2.1 MAC 802.11 and TCP Protocols in MANET 41

4.2.2 Related Works 42

4.2.3 IB-MAC Improvement of the backoff algorithm 45

4.2.4 Evaluation of IB-MAC and its impact on TCP performance . . . 48

4.3 Conclusion 54

V Improving TCP Performance on WAVE Networks
***"Improving TCP Performance on WAVE Networks, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, 2015, Published"* 55**

5 Improving TCP Performance on WAVE Networks 56

5.1 Introduction 56

5.2 Improving TCP Performance 59

5.2.1 Enhanced ETT scheme 59

5.2.2 E-ETT Performance Evaluation 60

5.2.3 Security cost for WAVE 64

5.3 Conclusion 67

VI NEtwork MObility (NEMO)
"Design and implementation of a secure nemo. International Journal of Computer Science and Information Security, ISSN 1947-5500, 2012. Published" **68**

6 A Deploy ability Analysis of NEMO in VANETs and Application 69
6.1 NEtwork MObility (NEMO) 69
6.2 Issues for QoS and security in NEMO-based VANET 72
6.3 Design and Implementation of a Secure NeMo 72
6.3.1 System Architecture 73
6.3.2 Experimental Setup 74
6.4 V-Learning: VANETs for Social and Mobile Learning 77
6.5 Conclusion 82

VII Conclusion and Perspectives 83

7 Conclusion and perspectives 84
7.1 Conclusion 84
7.2 Perspectives 85

A Networks Simulator NS A-1
A.1 Introduction A-1
A.2 NS2 Architecture A-2
A.3 Simulation A-5
A.3.1 Tcl script A-5
A.3.2 Network stack and node A-6

References 13

List of Publications 22

List of Figures

2.1 Example of Infrastructure and Infrastructure-less wireless networks [69]. 14
2.2 Using Ad-hoc to extend coverage. 18
2.3 Wireless networks hierarchy 21
2.4 Design of a modern vehicles network architecture [92]. 22
2.5 V2V Communication. 22
2.6 V2I Communication. 23
2.7 Hybrid communication. 24

4.1 Throughput variation without Mobility (chain topology). 50
4.2 End-To-End Delay variation without mobility (chain topology). 51
4.3 Throughput variation with weak mobility (speed W=5 m/s). 52
4.4 End-To-End Delay variation with weak mobility (speed W = 5 m/s). . . 52
4.5 Throughput variation with strong mobility (speed W=25 m/s). 53
4.6 End-To-End Delay variation with strong mobility (speed W = 25 m/s). . 54

5.1 Protocols stack of an IEEE 802.11p/1609 network. 57
5.2 Four channels switching schemes [17]. 58
5.3 Bandwidth wastage problem. 59
5.4 E-ETT Scheme. 60
5.5 TCP throughputs over different frame durations. 63
5.6 Aggregate TCP throughput over different frame durations. 63
5.7 Aggregate TCP throughput for multiple nodes. 64
5.8 TCP throughputs over different frame durations with authentication. . . 65
5.9 Aggregate TCP throughputs over different frame durations. 66
5.10 Aggregate TCP throughputs for multiple nodes. 66

6.1 System view. 74
6.2 System Architecture. 74
6.3 Nested NEMO. 79
6.4 V-learning Platform. 81
6.5 The difference in power consumed between TCP and UDP. 81
6.6 The difference in power consumed between 3G-WiFi and VANET-NEMO. 82

7.1 Li-Fi for V2V communications. 86

A.1 NS2 Basic architecture. [1] A-4
A.2 Basic node architecture. [2] A-7

List of Tables

2.1 Comparison between characteristics of MANETs and VANETs. 12

4.1 IEEE 802.11b Basic parameters 48

5.1 Simulations parameters 60
5.2 IEEE 802.11p Parameters in TCL file 61
5.3 MAC layer Parameters in TCL file 61
5.4 Physical layer Parameters in TCL file 62

6.1 UMIP configuration 75
6.2 radvd software configuration 76

Nomenclature

ABE Available Bandwidth Estimator
AC Access Class
ACO Ant Colony Optimization
AMLA Authentication with Multiple Levels of Anonymity
AODV Ad hoc On Demand Distance Vector
AP Access Point
BER Bit Error Rate
BS Base Station
C2CCC Car2Car Communication Consortium
CL-AKA Certificate-less and key agreement
CNST Channel Neighbour State Table
CoA Care-of Address
CoP Care-of Prefix
CoPP Care-of Prefix Pool
CSMA Carrier Sense Multiple Access
CSMA/CA Carrier Sense Multiple Access with Collision Avoidance
CTS Clear To Send
CF Contention Window
DAD Duplication Address Detection
DARPA Defence Advanced Research Projects Agency
DCF Distributed Coordination Function
DIFS DCF Inter-Frame Space
DoS Denial of Service
DSDV Destination-Sequenced Distance-Vector
DSRC Dedicated Short Range Communications
ECC Elliptic Curve Cryptography
ECN Explicit Congestion Notification
EDCA Enhanced Distributed Channel Access
EIFS Extended Inter-Frame Space
ELFN Explicit Link Failure Notification
ESA European Space Agency
ETSI European Telecommunications Standards Institute

E-ETT Enhanced Estimated Transmission Time
ETT Estimated Transmission Time
FAA Federal Aviation Administration
FIFO First in First out
FP Fake Point
GPS Global Position System
GPSR Greedy Perimeter Stateless Routing
HA Home Agent
HMM Hidden Markov Model
IBE Identity-Based Encryption
ICT Information and Communication Technologies
IETF Internet Engineering Task Force
IFS Inter Frame Spaces
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
ITS Intelligent Transportation Systems
IVC Inter-Vehicle Communication
LBNL Lawrence Berkeley National Laboratory
LDA Loss Differentiation Algorithm
Li-Fi Light Fidelity
LOS Line Of Sight
LREQ Location Request
LTE Long Term Evolution
LTT Location/Time Table
FCC Federal Communication Commission
MAC Medium Access Control
MANETs Mobile Ad-hoc Networks
MIP Mobile IP
MNNs Mobile Network Nodes
MNP Mobile Network Prefix
MPR Multi Point Relay
MQOG Multichannel QoS Cognitive MAC
MR Mobile Router
NAM Network AniMator
NAR New Access Router
NEMO BS NEMO Basic Support
NEMO Network Mobility
NPS Network Policy Services
NRT Non Real-Time

NS2 Network Simulator 2
OBU On Board Unit
OFDM Orthogonal Frequency Division Multiplexing
OLSR Optimized link State Routing
OM Ordinary Member
OTCL Objective Tool Command Language
PAN Personal Area Networks
PCF Point Coordination Function
PDAs Personal Digital Assistants
PKI Public Key Infrastructure
QoS Quality of Service
RA Router Advertisements
RF Radio Frequency
RFN Route Failure Notification
RGB Red-Green-Blue
RL Retry Limit
RREQ Route Request message
RSSs Received Signal Strength
RSU Road Side Unit
RT Real-Time
RTS Ready To Send
RTT Round-trip Time
SMSS Symmetric-Masquerade Security Scheme
SSP Security Service Provider
TCP Transmission Control Protocol
TCP-BuS TCP Buffering capability and Sequence information
TDMA Time Division Multiple Access
USC/ISI University of Southern California Information Sciences Institute
V2I Vehicle to Infrastructure
V2V Vehicle-to-Vehicle
VANETs Vehicular Ad-hoc Networks
VINT Virtual Inter Network Testbe
VLC Visible Lighting Communications
WAVE Wireless Access in Vehicular Environment
WBSS WAVE Basic Service Set
WCCP Wireless Congestion Control Protocol
WEP Wired Equipment Privacy
WG Working Group
Wi-Fi Wireless Fidelity

WPA Wi-Fi Protected Access
WPA2 Wi-Fi Protected Access II
WSMP WAVE Short Message Protocol

Part I

Introduction

CHAPTER 1

Introduction

1.1 Background

Future networks will comprise a wide variety of wireless networks. Users will expect to be always connected from any location, and, as users move, connections will be switched to available networks using vertical handover techniques.

In general, different networks have different Qualities-of-Service (QoS). Hence, a QoS framework is needed to help applications and services deal with this new environment. In addition, since these networks must work together, future mobile systems will have an open architecture, unlike the current closed architecture that is common nowadays. Therefore, new mechanisms will be needed to protect users, servers and network infrastructure. This means that future mobile networks will have to integrate communications, mobility, quality of service and security.

In this thesis, we focused on one type of network that has been designated as a technology that can bring several advantages in the near future and will serve as support for multiple applications.

For many years, governments, automakers and industrial consortia , fixed reduction of road accidents as a major priority. To achieve this challenge, an innovative idea was to make vehicles smarter. The vehicles already generate and analyse a large amount of data. With wireless communications, the vehicle environment and the ”field of vision” of the driver are increased. Thus, through vehicles listening to their environment, over 75 potential applications have been identified, including 34 in vocation of security (the remaining 41 being for the optimization of traffic and comfort users).

With the advent of wireless technologies such as 4G, WiFi, or Bluetooth, Wireless communications have become ubiquitous and inexpensive. Therefore, in order to deploy these applications, a network type emerged: vehicular wireless network. One of the main com-

ponents of such network is the inter-vehicle communication; it allows service availability in case of non-existent infrastructure. The network is then called a Vehicular Ad-hoc Network, VANET.

VANETs are autonomous systems consisting of some mobile nodes communicating between themselves by wireless communication on a peer to peer basis. They are self-organized, self-configured and self-controlled infrastructure-less networks. Nodes communicate with each other not following any predetermined plan and not using any base station. These networks are therefore particularly useful to those who need to communicate in situations where no fixed wired infrastructures are available.

Intra-vehicle communication brings essential changes to telecommunications and data networking. Toyota and Microsoft have declared a 12 million dollar joint investment on including Microsoft's Azure cloud platform in upcoming Toyota vehicles for better telematics [3]. Vehicular Ad-hoc Networks (VANETs) are a new emerging network technology derived from ad hoc networks; vehicles are free to move and organize themselves arbitrarily, whilst they can exchange information between themselves and Road Side Units (RSUs). This promising technology for future smart vehicle systems and ITS has the potential to increase road safety.

VANETs can also be used to enhance passenger comfort by providing services such as exchanging traffic information, weather information, interactive communication and offering internet access. Compared to the limited resources available in traditional ad hoc networks, vehicles can store and process large amounts of information. These data will be obtained via the vehicles sensors and may also include drivers personal information. Both traveling vehicles drivers and passengers today can have access to the sensor data (dash-board), location information (GPS), traffic information, etc.

The design and implementation of protocols and applications in VANETs will face the many traditionally known challenges in wireless communications (mobility, connectivity, security, etc.). In addition, the applications require in most cases a reliable communications, a minimum quality of service and sometimes even real-time communications. However, this comes in contrast to the highly dynamic nature of vehicular networks (topology change, variable distance between vehicles, frequent loss connectivity, unreliable communications, delay, etc.).

IP protocol is increasingly presented as a solution for the problems encountered by mobile users to access the internet. Using IP (v4 or v6) protocol, mobile nodes would not be reachable because their point of attachment and their IP address have changed. This

results in the connectivity breakage and then, an increase of packet loss. In order to avoid these problems, a protocol that allows nodes to remain reachable while moving around in the IP networks was developed [84], this protocol is known as Mobile IP (MIP).

To allow nodes to remain reachable, even if they change their points of attachment to Internet, Mobile IP uses a Mobile Router (MR). The MR allows local mobile nodes and visiting nodes to connect to Internet. The MR reduces transmission power because nodes do not need to connect individually to the network. Furthermore, the MR reduces handoffs because it handles link layer handoffs. MR reduces the bandwidth consumption and location update delays. When a network changes its point of attachment to the Internet, all mobile and fixed nodes inundate their Home Agent (HA) with registration messages, but with the use of an MR, one registration message is sent to HA to register the whole network.

The HA is a router that delivers packets to a mobile node when it is away from its home network and maintains current location information for the mobile node. When away from its home network, a mobile node is associated with a Care-of Address (CoA) that reflects its current point of attachment. This allows nodes to keep their home IP addresses and to receive packets sent to them, even when they are away from the home network. The mechanisms of MIP make the movement of nodes transparent to transport layer and higher layer protocols and applications.

Mobile IP may be used in IPv4, but the restricted scale of addresses makes communication management of mobile terminals more complicated than necessary. IPv6 is preferable due to its great number of available addresses that allow attribution of temporary addresses to the moving stations. In [61], MIPv6 was defined as a protocol allowing mobile nodes to move from a link to another while keeping their home address unchanged. The use of IPv6 routing header by MIPv6 results in a less overhead, and improves the use of the resources of the communication medium.

However, MIPv6 is unable to support network mobility. Not all devices in a mobile network, for example, the sensors in an aircraft, may be sophisticated enough to run the complex mobility support protocols. In addition, once a device has attached to the MR on a mobile network, it may not see any link-level handoffs even as the network moves. Thus the host mobility protocols such as MIP and MIPv6 do not get triggers indicating link-level handoffs and as a result will not initiate handover. This paved the way to the development of a Mobility management mechanism that consists of Network mobility basic support. Till now, only nodes mobility is considered. However, different scenarios of entire moving networks exist (WLANs on trains, planes, ships etc.). In order to support

1.1 Background

Network Mobility (NEMO), NEMO Basic Support (NEMO BS) [38] was developed to cope with the aforementioned drawbacks of the MIPv6 protocol. Is fact, NEMO BS is an extension of MIPv6. It allows terminals within a mobile network to globally and continuously be connected to the Internet. The NEMO BS is designed so that network mobility is transparent to the node inside the mobile network, as only MR and HA have to be aware of the network changes. The Mobile Network Nodes (MNNs) continue to be connected via the MR using the same address configured using the Mobile Network Prefix (MNP).

If the mobility of each moving node has to be managed independently, this would create in an important amount of control messages, rapidly overloading the wireless link. Since all the devices on a vehicle are moving in along the same trajectory and with the same speed, managing the mobility of these nodes jointly decreases deeply the amount of generated traffic in the wireless link, thus optimizing the use of available bandwidth. Therefore, NEMO BS is suitable to manage devices mobility in vehicular networks due to their highly mobile nature. The main goals of the mobility management protocol NEMO BS are providing continuous communications without service disruption caused by mobility events; and allowing reachability to onboard nodes regardless of their location, all this without incurring in a significant increase in the overhead traffic. As such NEMO BS is suitable to manage devices mobility in vehicular networks.

If a vehicle is connected to the internet, then it can be assisted remotely, and its passengers can take advantage of the usual communication services, just like if they were at home or the office. However, then, it is necessary to secure data communication services and network mobility management exchanges from attacks that can cause the break down of ongoing communication. In fact, a disconnection due to security attacks can isolate the mobile network and result in the interruption of the remote the assistance of vehicles by the provided ITS, with serious consequences.

In NEMO, the MR needs to allow subscribers from different domains to get Internet connectivity through it. In such settings where static trust relationships are lacking, a variety of several security threats arises. Security and performance are critical aspects of NEMO. Mobile networks travel on foreign, and possibly untrusted, networks when away from home. Because MNNs are unaware of mobility, it is important that NEMO provides security while a network is away. Also, performance is important in accomplishing the goal of NEMO to provide seamless mobility to unaware IP devices. In the NEMO BS protocol we advocate the use of IPsec to protect signaling messages. Security mechanisms for network mobility are at a preliminary stage, and much work needs to be done for mobile networks to be deployed in a secure setting.

Delay and packet losses constitute another issue for mobility management in VANETs. When an MR does a handover and changes its point of attachment it needs to activate MIPv6 and the NEMO handover procedures. Upon detection of a movement, the MR obtains a care-of address from the foreign network and then indicates to it is HA that it is playing the role of an MR. This handover process results in increased latency due to the multiple levels of indirection involved. The chances of packet loss are also more significant as a result of an increase in latency. Research is required to adapt mechanisms such as fast handover to support mobile networks.

In [88], Sanaa Taha and Xuemin Shen proposed a location privacy solution that consisted on the fake point to protect the privacy of the vehicles in NEMO-based VANETs. The proposed scheme involves fake-point- and cluster-based sub-schemes, and its goal is to confuse the attackers by increasing the estimation errors of their Received Signal Strength RSSs measurements and, hence, preserving mobile network nodes MNNs' location privacy. Using correctness, accuracy, and certainty metrics, we show that the fake point-cluster-based scheme achieves higher MNN's location privacy when the number of network grid points in the hotspot decreases. The fake point mechanism allows a high-level privacy for MNNs. The main idea of this protocol consists on choosing a location inside the hotspot that is called Fake Point (FP). This FP is considered by the MNNs while calculating their transmission power.

If an attackers device is located inside the FP, it measures the RSS value as being the same for all the MNNs. This makes a deviation in the attackers estimation of the MNNs distance. Hence, the privacy of the location of the mobile nodes is kept. This information allows the MNNs to calculate their distance to the AP according to the RSS, join the NEMO hotspot and check the authenticity of the AP in the hotspot. After that, the AP sends the grid points list containing the locations inside the hotspot to the MNNs. Then, the MNN selects a point in the list and calculate its transmission power to this point as it will send its data to the AP via this node. Instead of sending data to this selected FP in grid-point list, a MNN sends it to its AP to confuse attacker devices which may be located in this fake point.

In [98], a handover mechanism based on Care-of Prefix Pool (CoPP) is proposed. Vehicles move so fast that they always cause the handover delay problem in the VANET. This problem will lower down the throughput of the network and make the mobile devices' connection to the Internet ineffective. To solve this problem, we propose a handover mechanism based on CoPP in VANET with NEMO. The vehicle adopting the handover mechanism can acquire unique Care-of Prefix (CoP) from the new Base Station (BS) with CoPP. The proposed solution leaves out the Duplication Address Detection (DAD) phase,

and then they can significantly reduce the handover delay.

In [87], Sanaa Taha and Xuemin Shenhave proposed a link-layer authentication and key agreement scheme. This protocol uses the Certificate-less and key agreement (CL-AKA) scheme to secure public hotspots in NEMO-based VANET. Based on certificate-less public key cryptography, a link-layer authentication and key agreement scheme, CL-AKA, is proposed. CL-AKA achieves mutual authentication between an MNN and MR as well as creates a secure shared key between them. Unlike existing Wi-Fi security schemes, CL-AKA uses only one certificate verification to verify an MR to an MNN while implicitly verifying this MNN to the MR. Therefore, the proposed CL-AKA scheme has less communication overhead than that by captive portal and higher security level than that by dummy authentication scheme.

The weak point of those works is that they do not manage simultaneously QoS and security.

1.2 Problem statement

The quality of service and security are the main challenges in VANETs applications since they are directly related to the safety of people, for example, drivers in a highway. In this thesis, we surveyed the most important requirements of VANETs applications that consist on the Quality of Services, security and privacy aspects. Wireless environment characteristics, such as dynamic topology changes due to the high speed (more than 50km/h) of vehicles, have an impact on QoS and security.

Several works have been conducted in the literature. After reviewing the architecture, the applications, characteristics and challenges, we present some of the shortcomings of QoS and security in vehicular environments. As VANETs are foreseen to provide ubiquitous services for users by keeping them connected to the internet for safety and entertainment needs, NEMO was proposed as a promising solution to cope with users disconnections due to the high speed of vehicles. Thus, we expose the main idea of NEMO, which is still evolving. Then, we survey some recent solutions proposed to improve the different parameters in order to provide efficient and secure communications in vehicular environments.

Security is not a separate issue but linked to the control and management of QoS network and services. Security is an important issue in any communication system. As VANETs are composed of number of communicating autonomous entities moving at high speed, the randomness of the connectivity between the vehicles and their relative geographic po-

sitions raises concerns about users and data security. The most desired security attributes as criteria to measure security for all VANET applications are authenticity, privacy, availability, confidentiality and non-repudiation. Attacks in VANETs hinder vehicles communications by deteriorating or interrupting their functions. To meet aforementioned security requirements, several approaches were proposed by researchers which aim to prevent or diminish the consequences of attacks.

A key challenge of securing VANETs is to provide sender authentication in broadcast communication scenarios. To authenticate users or messages in VANETs, we have used the identification. A vehicle is identified by being registered to the VANET; a vehicle must provide a registration number to a certified authority or trusted authority. This authority is responsible for providing an authenticated recognition to each vehicle in the network. Vehicle credentials provided to Certified Authorities allow the localization of vehicles by geographic localization services like GPS. This information may be used by adversaries to track the vehicle or get personal information about drivers. In order to preserve privacy, it is necessary to use cryptography and digital signatures. Therefore, the cryptographic techniques and digital signatures used in VANETs must have low traffic and processing overheads while generating and exchanging public keys.

A malicious entity within the VANET may broadcast false information. This attack is known as a Sybil attack. In a Sybil attack, a vehicle sends multiple copies of messages to other vehicles and each message contains a different fabricated identity. The problem arises when the malicious vehicle can pretend as to be multiple vehicles and reinforce false data. A Sybil node may create an illusion of traffic congestion. There are several techniques to avoid Sybil attacks in VANETs such as statistical and probability, signal strength and session keys [94]. Spoofing is an attempt by a node to send modified version of the message and claims that the message comes from the originator for the unknown purpose. Itś another category of attacks on the data integrity.

Keeping a reasonable balance between the security and privacy is one of the main challenges in VANET. On the one hand, the receivers want to be sure that they can trust the source of information. On the other hand, the availability of such trust may contradict the privacy requirements of the sender. After registration, information provided by the vehicle may be used by a malicious entity in order to localize the vehicle and track it. The privacy issues are concerned with protecting and disclosing drivers personal information such as name, location, etc.

As VANETs consist on vehicles moving at high speed, the development of secure routing protocols is necessary to ensure that messages reach the destinations. The efficacy

of VANET communication depends on providing critical data within the relevant time to give users enough time to take into consideration the critical data. As vehicles use the scarce resource radio channel to communicate, VANETs are prone to attacks on network availability. Two possible threats to availability are for example Denial of Service (DoS) and jamming attacks. Another availability problem may be caused by selfish nodes that do not provide their services for the benefit of other nodes to save their own resources like battery power [34].

1.3 Research Question

Managing the access to secret information sent between nodes in the VANET is currently not possible. To our knowledge, none of the related work addressed the issue of controlling the information flow in VANETs. However, securing a service can cause degradation of the QoS, and the mobility of a user can change the service needs in terms of QoS and security. Thus, we need to simultaneously manage QoS and security while taking into account users mobility.

In this thesis, we propose to contribute on how to improve QoS and respect security for future networks.

To answer this research question, we use simulations and experiments. Simulation using NS2 (Network Simulator 2, see Appendix A) will be used to show that security schemes have significant impacts on the throughput QoS, and our proposed scheme can substantially improve the effective secure throughput with cooperative communications.

1.4 Thesis Outline

The thesis is structured as follows:

- Chapter 2 presents an introduction of the wireless ad hoc networks and Mobile Ad-hoc Networks (MANETs), it also describes the characteristics, challenges, vulnerabilities of mobile ad hoc networks, and then it illustrates the various advantages of MANET and enumerates the applications of MANET. This chapter also presents an introduction of the VANETs, history and background; also it describes their characteristics.
- Chapter 3 introduces VANETs standards protocols and challenges. It also defines the security concepts and requirements; it presents an overview of the network security and describes the related work in privacy and confidentiality issues in VANETs.

- Chapter 4 presents the first contribution of the thesis: a new technique to improve the Transmission Control Protocol (TCP) performance in MANET by exploiting the Backoff algorithm of Medium Access Control (MAC) protocol. This improvement is the Improvement of Backoff algorithm of MAC protocol (IB-MAC). It proposes a new Backoff algorithm based on a dynamic adaptation of its maximal limit according to the number of nodes and their mobility. The results are satisfactory and show that our algorithm can outperform not only MAC standard, but also similar techniques that have been proposed in the literature like MAC-LDA and MAC-WCCP.

- Chapter 5 presents the second contribution of the thesis. We evaluate the performance of TCP over IEEE 802.11p/1609.x with various networks configurations. We overcome the bandwidth wastage problem caused by channel switching in the standards IEEE 802.11p m/1609.x. We propose a scheme that we called E-ETT and we show that our scheme has better performance compared with the scheme used by IEEE802.11p. We also introduced security to study the additional cost and the impact on the performance. Overall, our scheme improves the performance by about 5% in the presence or not of the security aspect.

- Chapter 6 presents the third contribution of the thesis: a deploy ability analysis of NEMO in VANETs and an example of application. We discuss how cooperation between VANET and NEMO can bring several benefits. In fact, our results show that VANET network performance is improved. We introduce our proposed architecture that has been designed to give access in social and mobile learning context. We focus on the problem of learners devices energy consumption. The results show that VANET-NEMO approach provides more energy saving than a 3G-Wifi approach.

- Chapter 7 includes a conclusion of our research and introduces VLC Visible Light Communication technology as the future of VANETS.

Part II

Background on MANETs and VANETs

CHAPTER 2

Background on MANETs and VANETs

2.1 Introduction

This chapter presents a review of wireless ad-hoc networks and MANETs. It also describes the characteristics, challenges, vulnerabilities of mobile ad hoc networks, and then it illustrates the various advantages of MANET and enumerates the applications of MANET. It also presents an introduction to the VANETs, history and background, characteristics, challenges and vulnerabilities. Finally, this chapter provides a comparison between characteristics of MANETs and VANETs as described in the Table 2.1.

Characteristic	MANET	VANET
Topology	Dynamic	Dynamic (more than MANET)
Mobility Prediction	No	Yes
Muti-hop	Yes	Yes
Limited Device Security	Yes	No
Limited Physical Security	Yes	Yes
Short Range Connectivity	Yes	Yes
Infrastructure less	Yes	Yes

Table 2.1: Comparison between characteristics of MANETs and VANETs.

Although VANETs are interesting for many on-road applications, they nevertheless have several challenges, as shown in Section 3.2. Each of these challenges can be considered as a separate research area needing intensive investigation. Researchers investigated the security issues in both MANETs and VANETs and they proposed many solutions; the next chapter will investigate these issues by discussing the security requirements, security attacks, and security mechanisms used in the literature to make a secure communication between the entities. Recently ad-hoc networks received extensive attention in both industrial and military applications, because of the striking property of creating a network while moving from one place to another and not requiring any pre-designed infrastructure.

These unique characteristics in MANETs present appreciable challenges; therefor Section 2.3.2 describes the vulnerabilities and challenges of MANET: lack of secure boundaries, restricted power supply, unreliability, lack of centralized management facilities, threats from compromised nodes, and scalability. Section 2.3.3 mentions the advantages of MANETs.

There are many applications of MANETs; therefore Section 2.3.4 presents these applications: home networks, enterprise networks, military applications, emergency response networks, sensor networks, and VANETs. Section 2.4 presents an introduction to VANETs and describes the modern vehicles components.

2.2 Introduction to wireless networks

In the past few decades wireless networks have become increasingly popular, due to the wide availability and rapid introduction of wireless transceivers into a variety of computing devices such as PDAs, laptop and desktop computers. Wireless communication brings essential changes to telecommunications and data networking. Air is used as the transmission medium, allowing great flexibility; networks can be deployed quickly where cabling is difficult. Good performance and low prices encourage progressively more home users and companies to choose these new kinds of networks. Wireless communications could replace wired communications in many situations. Traveling users today have access to the Internet at many places like their offices, homes, and even at public places like airports, conferences, shopping centers, hotels, and libraries.

Wireless LAN networks can be classified into two categories. The first and most common infrastructure are networks with fixed and wired gateways (a wireless network built on-top of a wired network). In this kind of network mobile nodes connect to a network via an Access Point (AP) within its coverage range in a single hop communication technique. The second type of wireless network is the infrastructure-less mobile network, commonly known as MANET.

One advantage of wireless is the ability to transmit data among users in a common area while remaining mobile. However, the distance between participants is limited by the range of transmitters or their proximity to wireless access points. On the other hand, MANETs solve this problem by allowing out of range nodes to route data through intermediate nodes.

In figure 2.1, node 1 can communicate directly with nodes 2 and 4. To reach other destinations, for example, the node 3, it must be based on intermediate nodes that will

relay its messages in this case node 2 for example. Unlike the infrastructure wireless network where the maintenance of connectivity is provided by specific equipment, in infrastructure-less wireless networks each node must calculate and maintain routes to reach all destinations. Furthermore, not only each node uses intermediate nodes to reach the intended destination, but it also must in retransmit the traffic of its neighbors.

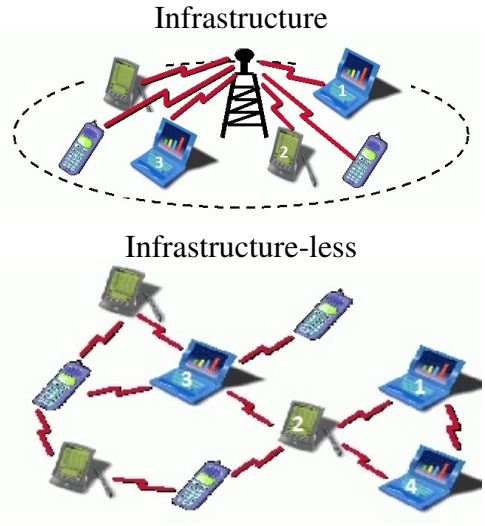

Figure 2.1: Example of Infrastructure and Infrastructure-less wireless networks [69].

2.3 Mobile Wireless Ad-hoc Networks (MANETs)

MANETs are complex distributed systems that, composed of wireless mobile or static nodes. In such networks, the wireless medium must have the access provided by the MAC protocol efficiently to reduce interference.

A network consists of terminals and routers. A router allows routing the packets. In contrast, an ad-hoc network contains no dedicated routers: any node can be terminal and router [76].

Therefore, two nodes of an ad-hoc network can communicate without the infrastructure set-up as in a conventional network. In addition, an ad-hoc network is mainly used in the context of mobility while routing protocols used in a traditional network are not adapted to a topology change.

In an ad-hoc network, two nodes on a network exchange data using nodes called relay nodes (or intermediate nodes). For this, the exchange initiator node, called the source node, transmits packets to its neighbours. If the node is not the destination of the packet, a relay node transmits the packet to its neighbours, and neighbouring transmits to their neighbours until the packet reaches the destination.

When a node receives a packet, a routing protocol takes the decision. If the node is the packet destination, the packet is sent to the application layer. If it is a relay node to the destination of the packet, then it forwards the packet. Otherwise, the packet is ignored.

In MANET, nodes move and thus the topology changes frequently. A suitable protocol must be used and must support node mobility.

Each node runs this protocol to calculate the next relay node. Under this protocol, the nodes exchange signaling messages between them to be aware of the topology by creating a graph of the network or to create a path to the destination.

Mobile ad hoc networks are autonomous systems that consist of some mobile nodes that communicate between each other using wireless connection. They have the ability to configure themselves, to self-organize, and to control their infrastructure. This kind of network can easily deploy anywhere and at anytime because there is no central administration.

MANETs are a case of wireless ad hoc networks, progressively more popular and success-

ful in the market place of wireless technology. Examples include Bluetooth and Wireless Local Area Networks (WLANs). These networks are very useful particularly in where no wired infrastructures are available.

2.3.1 The evolution of MANETs

Since 1970s, in the American military DARPA project, we saw the birth of the first networks using the radio medium. These networks already had a distributed architecture, shared the broadcast channel by repeating packets to expand the global coverage area.

In 1983, the Survivable Radio Networks (SURAN) were developed by DARPA [28]. The aim was to overcome the limitations as number of nodes by networks, security or energy. But research on these networks remained exclusively military. Only in the late of 90s, civil research seized issues related to these networks. So, the IEEE 802.11 community adopted the term Ad Hoc Networks, and the idea of having a collection of nodes was proposed. Researchers began, therefore, to think of a way to deploy in other areas as radio broadcasting.

MANET (Mobile Ad hoc Networks) is the name of the IETF (Internet Engineering Task Force) working group is responsible for standardizing based on IP technology, routing protocols for Ad-Hoc networks, whether mobile or not. Since the birth of the MANET group, the name of the group has been used as a common name for a Mobile Ad-Hoc network. A MANET is a special case of wireless network where each node can directly join its neighbours using its radio interface and has the ability to contact any other node within the network using the intermediate nodes. They are responsible for relaying messages and offer a standalone network, designed and supported by all participants.

2.3.2 The Characteristics of MANET

MANETs have many constraints in their characteristics. For MANETs to be usable for the support of multimedia streams and real-time, it is necessary to provide solutions to some of its limitations. Chapter 5 is our contribution in this direction. MANET has special characteristics [74] compared to other wireless networks. MANETs have many characteristics that make them distinguishable from other wireless and wired networks which are in detail:

- **Constrained Resources:** : Most MANET devices are small handheld devices like Personal Digital Assistants (PDAs), laptops and cell phones. These devices have limitations because of their restricted battery-capacity, small processing power and

storage facilities. Energy consumption is an important criterion when designing the MANET.

- **Infrastructure-less(Autonomous):** MANETs are based on the teamwork between independent peer-to-peer nodes that communicate with each other. Without any preplanned arrangement or base station, all nodes have the same role in the network. There are no pre-set roles like router, server or gateways for the nodes participating in the network.

- **Low and Variable Bandwidth:** Wireless links that connect the MANET nodes have lower bandwidth than wired links. The effects of interference, congestion and noise are more significant.

- **Dynamic Topology:** MANET nodes can move arbitrarily; thus the nodes can dynamically enter and leave the network, continually change their links and topologies. This leads to frequent changes in the routing information.

- **Multi-hop communications:** The communication in MANET between any two nodes is performed by numerous intermediary nodes whose functions are to relay data-packets from one point to another.

- **Limited Device Security:** MANETs devices are usually small and can be transported from one place to another. Unfortunately, as a result, these devices can be easily lost, stolen or damaged.

- **Limited Physical Layer Security:** MANETs are in general more vulnerable to physical layers attacks than wired networks; the possibility of spoofing, eavesdropping, jamming and denial of service (DoS) attacks should be carefully considered. However, the self-administration nature of MANET makes them more robust against single failure points.

- **Short Range Connectivity:** MANETs rely on radio frequency (RF) technology to connect, which is considered to be short range communication. For this reason, the nodes that want to communicate directly need to be in the close range of each other.

2.3.3 Advantages of mobile ad hoc networks

MANETs have particular advantages over the conventional networks. Some of these advantages are:

- Increasing mobility and flexibility, as MANETs can be initiated and terminated in a very short time.

- More robust than traditional wireless networks, as MANETs do not rely on the centralized base station.
- More economical than traditional networks, as MANETs eliminate the cost deployment of infrastructure.
- Reducing the power consumption of devices by using multi-hop sending mechanism; all nodes can be relay stations receiving and sending packets to the goal destination, rather than sending data packets over one long hop.
- Ad hoc networks can be used to enlarge the coverage area of an access point. By this method, a few users are connected to a single access point providing connections to another outside of range users. Figure 2.2 shows how the Ad hoc fashion can do this.

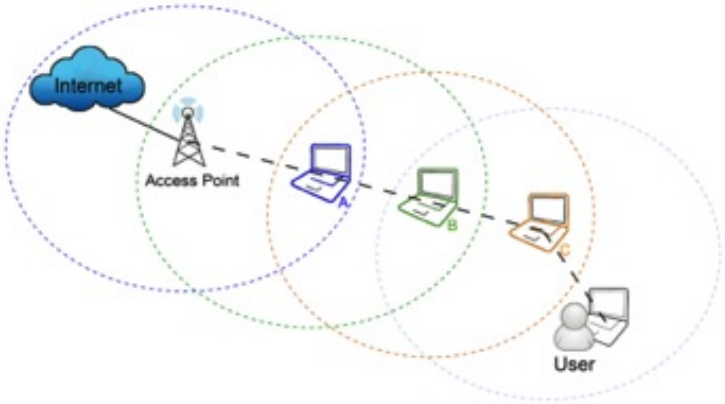

Figure 2.2: Using Ad-hoc to extend coverage.

2.3.4 Applications of mobile ad hoc networks

There are many applications of mobile ad hoc networks; these have been listed in [25]. We classify those application in two groups: military and civil.

- **Military Applications:** The soldiers were among the first to use mobile ad hoc networks as part of their tactical networks to improve the quality and duration communications during operations. The use of mobile ad hoc networks had proved interesting because they are based on an pre-existing infrastructure but allow their nodes to relay themselves communications to overcome the physical limit of radio propagation.

  In 1997, the US military has set up the IT (internet Tactical), which allowed the largest implementation of large scale wireless network, wireless multi-hop packet switched radio. Indeed, the platform Force XXI Battlefield Command Brigade and

Below, or FBCB2 [77] based on MANET was put in place to allow soldiers to locate Allied and enemy forces on the battlefield.

- **Civil Applications:** There are diverse and varied civil applications based on MANETs. We classify into two groups: commercial and non-commercial:

  1- Commercial: These services include e-commerce, access to files stored on a centralized system, call transfer or the particulars of services nearby a given location. Some others like access by commercial agents to a common central database will be more effective and strengthened. New services will emerge as well as guidance while driving to prevent accidents.

  Commercial applications based MANETs are mainly designed as part of the role they play in extending other wired or wireless networks. Also, RFC 2501 [74] described MANETs in these terms (stub networks). This will have its meaning in the future mobile technologies like VANETs. It is a subclass of MANETs, where the mobile nodes are vehicles; today vehicles are becoming ”computer networks on wheels”, these vehicles are free to move and organize themselves arbitrarily, which they can exchange information between themselves and RSUs, in order to increase safety in the roads by warning the drivers about ongoing hazard situations, and increasing the responsiveness of their surroundings and make them more vigilant.

  In another aspect Inter-Vehicle Communication (IVC) can be used to enhance passenger comfort and enrich the traffic system, by exchanging traffic information, weather information, petrol station, restaurants location and price information, and providing the interactive communication like offering access to the Internet.

  Road traffic management applications are designed to optimized the traffic and prevent congestion through communication between vehicles, then they become sensor's traffic.

  2- Non-Commercial: rescue operations in case of emergencies to quickly deploy a network on land where infrastructure is lacking or damaged due to natural disaster, fire or attack by an enemy. In Europe, the E-SPONDER program was launched in July 2010. Its objective is to develop a comprehensive system for crisis management assistance on 3 levels: central permanent command, postmobile command and unity of first responders. The latter will deploy a MANET network [4].

  Moreover, MANETs could be used to set up a wireless LAN at home or at work

to share like a printer or a backup drive, share files as multimedia files or customer records, share expensive applications whose implementation is tedious, etc. Internet access can also be extended and for working outside in the garden, by the pool or on a terrace.

In the field of education, MANETs also offers a perspective. Virtual classrooms can indeed be by networking several rooms. Collaborative work on a set of data from multiple terminals MANET and synchronizing with a remote database becomes practical.

For the leisure, network gaming win to use MANETs enjoying their exibility to play anywhere like in a park and anytime as during waiting times.

2.4 Vehicular ad hoc networks (VANETs)

Conventional Traffic management systems are based on a centralized infrastructure where cameras and sensors installed on the road collect information on the density and conditions of the traffic. This information is transmitted to a central unit to process and make adequate decisions. Such systems exhibit a relatively large cost of deployment and are characterized by a reaction time of the order of one minute for the processing and transfer of information. In a context where the deadline for transmission of information is vital and is of major importance in this type of systems, this delay is unacceptable..

In addition, the equipment set up on the road requires periodic and expensive maintenance. Therefore, in order to deploy such a system-wide scale, a significant investment in communication infrastructure and sensors is necessary. However, with the fast growing of wireless communication technologies tracking systems and information collection by sensors, a new architecture decentralized (or semi-centralized) based on vehicle-to-vehicle communications (V2V, Vehicle to Vehicle) was developed in recent years attracting great interest from the scientific community, car manufacturers and telecom operators.

This type of architecture is based on a system distributed, autonomous, and is formed by the vehicles themselves without the help of a fixed infrastructure relaying data and messages.

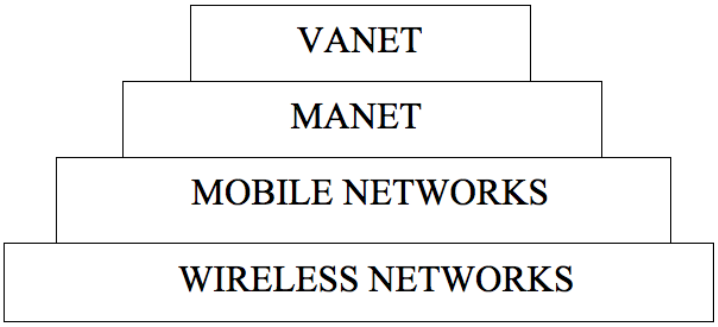

Figure 2.3: Wireless networks hierarchy .

A VANET network is a feature of MANET networks where mobile nodes are vehicles (smart) equipped with computers, network cards and sensors. Like any other ad hoc network, vehicles can communicate with each other (to exchange traffic information for example) or with base stations placed along the roads (to request information or access to the Internet).

The figure 2.3 shows the hierarchy of wireless networks where it diagrams the inclusion of VANET in MANET, MANET networks in the Mobile and mobile networks in wireless networks.

The introduction of intelligence in the field of cars (see Figure 2.4) is aimed at improving the lives of passengers and drivers. The applications are countless and range from safety and comfort through entertainment and services. All these concepts are the object of interest of what is commonly called ”Intelligent Transport Systems (ITS).” The idea is to introduce a certain level of intelligence in vehicles by equipping them with sensors, actuators and processors. At this level, it is called local board intelligence (only a local vision and the surrounding environment is established). Vehicular networks include two classes of applications, applications that build an ITS and those related to comfort or to warn the driver and any passengers.

Vehicular networks are the basis of exchanges for intelligent transport systems. From an architectural point of view, communication in a VANET can be either: i) Vehicle-to-Vehicle (V2V); ii) Vehicle to Infrastructure (V2I); iii) Hybrid communication.

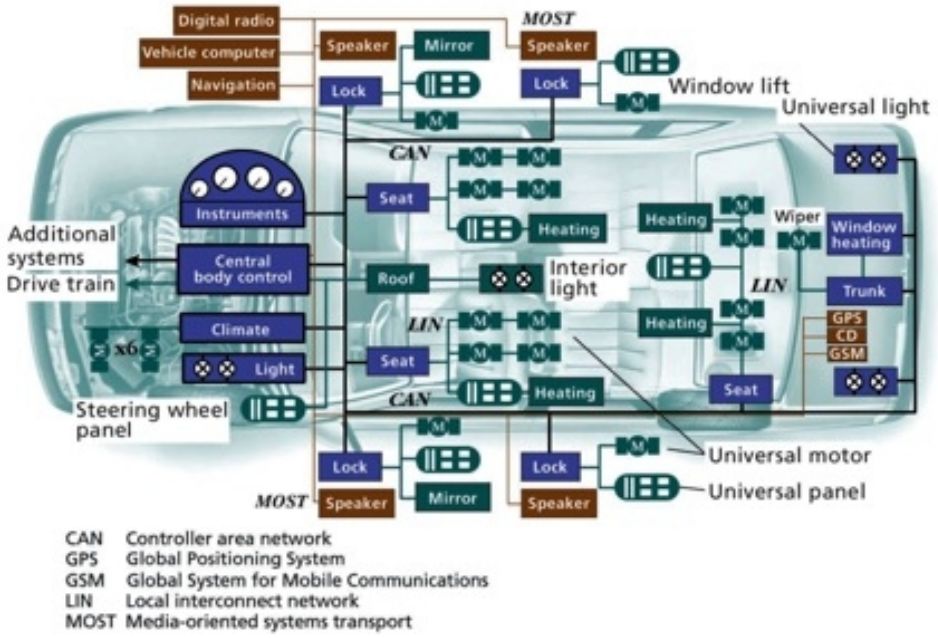

Figure 2.4: Design of a modern vehicles network architecture [92].

2.4.1 Vehicle to Vehicle communication V2V

In this category, a vehicle network is seen as a special case of MANET where energy constraints and memory capacity are relaxed and where the mobility model is not random but predictable with great mobility. This architecture can be used in the dissemination of alerts scenario (emergency braking, collision, slowdown, etc.) or to the cooperative behavior.

No infrastructure is used, no installation is needed on the roads and all vehicles are equipped to communicate directly with each other anywhere, whether on highways, mountain roads or urban roads, which can provide a less expensive and more flexible communication.

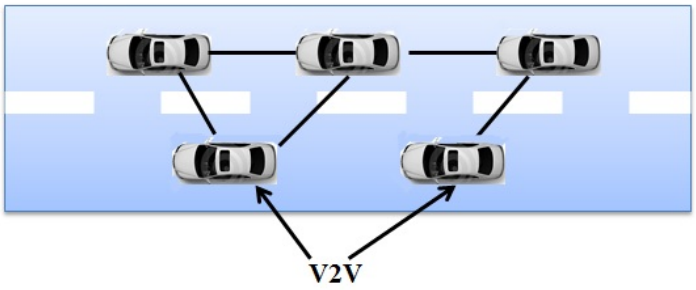

Figure 2.5: V2V Communication.

This approach suffers from certain drawbacks:

- The time of communication is high, given that the communication is done using multi-jumps.
- The Frequent disconnections due to the fact that vehicles are mobile.
- Network security is very limited.

2.4.2 Vehicle communication with use of infrastructure V2I

In this category, we do not just focus on simple inter-vehicle communication systems but also on those using base stations or points of RSUs (name proposed by the consortium C2C-CC). This approach is based on the client / server model where vehicles are clients and stations installed along the road are the servers. These servers are connected to each other via a wired or wireless interface. All communication must go through them. They can also offer users more services on trafficking, internet, exchange car-to-home communication data and even car to the garage for the remote diagnosis.

The major drawback of this approach is that the installation of the stations along the roads is a costly and time consuming not to mention the costs of maintenance of the stations.

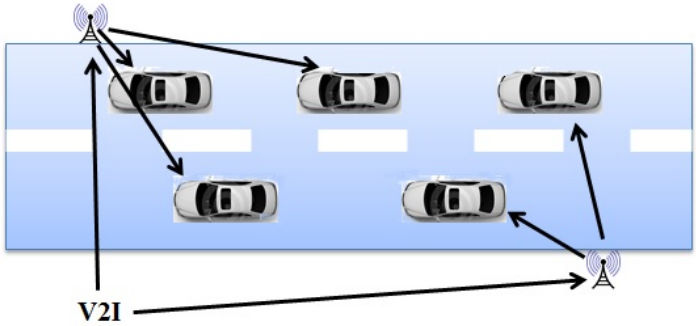

Figure 2.6: V2I Communication.

2.4.3 Hybrid communication

The combination of these two types of communication architecture provides an interesting hybrid architecture. Indeed, the increase of infrastructure is limited, the use of vehicles as relays can extend this distance. Nevertheless, the inter-vehicular communications suffer from routing problems on long distance transmission. In such situations, access to infrastructure can improve network performance. In order to avoid multiple base stations at every street corner, the use of vehicles as intermediate hops takes all its importance.

A special case of the hybrid architecture is the VSN network (Vehicular Sensor Network). Indeed, this type of network emerges as new vehicle network architecture because cars are provided with more sensors of all categories (cameras, pollution sensors, rain sensors, tire condition sensors, ESP, ABS, satellite geolocation, etc.). Information delivered by these devices may be useful for obtaining statements on road traffic (congestion, delays, average traffic speed, etc.) on available parking spaces, for more general information such as average fuel consumption and the rate of pollution, or for monitoring applications (through cameras on the vehicles).

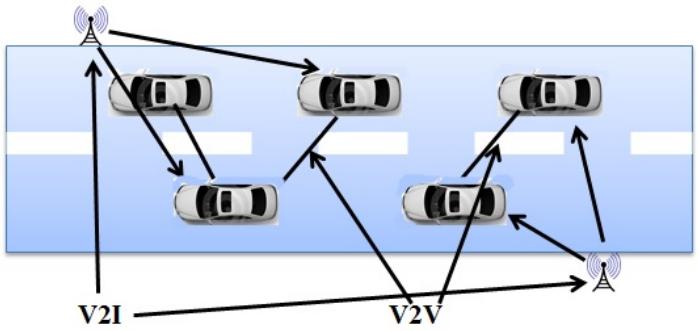

Figure 2.7: Hybrid communication.

2.5 Conclusion

This chapter presented an introduction of wireless networks and its two types: infrastructure and infrastructure-less. It also presented an introduction to the VANETs, history and background, characteristics, challenges and vulnerabilities. Finally, this chapter provides a comparison between characteristics of MANETs and VANETs.

In the next chapter, we will focus on VANETs and we will present standards of communication for this kind of networks.

Part III

Standards of communication and challenges in VANETs

CHAPTER 3

Standards of communication and challenges in VANETs

Unlike traditional wireless networks where energy represents a constraint-limiting factor, important entities of vehicular networks have sufficient energy capacity that they derive from the vehicle fuel system. Even when the vehicule stops, embedded platforms may give more benefit's from massive computing capabilities and multiple communication interfaces.

If communication environments from traditional wireless networks generally consist of completely unobstructed open spaces and indoor or enclosed spaces, vehicular networks require consideration of greater environmental diversity. Due to the mobility of vehicles, it is possible to move from an urban environment to a motorway environment with radically different features. It is also necessary take into account volatile climate and topological constraints. This communication environment leads to complex waves propagation models.

Vehicular networks are also distinguished from conventional wireless networks by a mobility model where one of the most obvious and important parameters is the speed of nodes. This mobility constraint dramatically reduces the time during which nodes can communicate. These conditions are likely to pose significan connectivity problems coupled with worsening of the instability of the radio propagation.

3.1 Standards of Communication in VANETs

The IEEE has extended its family of 802.11 protocols by adding 802.11p [19], drawing it from the ASTM E2213-03 standard [86], itself based on the 802.11a [15]. This protocol changes the physical layer and the MAC layer to adapt to vehicles networks in accordance with the DSRC (Dedicated Short Range Communication) band 2. In addition, the IEEE 1609 family defined protocols, called WAVE for Wireless Access in Vehicular Environment [19].

3.1.1 Protocols WAVE and IEEE 802.11p

Since 2003, the IEEE organization has initiated work to define a new standard dedicated to communications in the DSRC band. This standard known as IEEE 802.11p / WAVE (Wireless Access in Vehicular Environments) [59] uses the concept of multi-channel to ensure communications for safety applications and other services ITS. This protocol addresses a lack of homogeneity between car manufacturers and provides sufficient support for the organization of management functions and mode of operation for the vehicular communication. WAVE provides a set of services and interfaces that enable collectively to ensure V2V or V2I communication security.

The WAVE protocol is based on family IEEE1609 protocols to operate in the DSRC band. This protocol stack consists of five standards :

(i) IEEE P1609.0 WAVE Architecture describes the architecture and the services needed in the DSRC / WAVE devices so that they can communicate in a vehicular environment.

(ii) IEEE 2006 1609.1- WAVE Resource Manager for resource management at the three upper layers of the OSI model. It describes management and data services available in the WAVE architecture. It defines the command message format and the appropriate response to these, data storage formats used by applications to communicate between the architecture components and format of status messages and query.

(iii) IEEE 1609.2-2006 WAVE Security Services for Applications and Management Messages for transmission and secure processing messages at the transport layer. It also defines the circumstances of the use of a secure exchange and how these messages should be treated according to the purpose of the exchange.

(iv) IEEE 1609.3-2006 WAVE Networking Services, defines the network layer level of services and transport, including the addressing and routing for secure data exchange support. It also defines the WAVE Short Messages (WSM), providing an alternative to effective specific IPV6 WAVE can be directly supported by applications. In addition, this standard defines the Management Information Base (MIB) for WAVE protocol stack.

(v) IEEE 1609.4-2006 WAVE Multi-Channel Operations, provides an improvement in MAC layer 802.11 to support the WAVE operations; coordination and management of seven channels in the DSRC band and management of queues and priority access to the medium. (vi) IEEE P1609.11 Over-the-Air Data Exchange Protocol for ITS defines the services and the secure message format for secure electronic payment support.

802.11p MAC extensions concern the management of message priority to better manage delay-sensitive applications. At physical layer, IEEE 802.11p use Orthogonal Frequency Division Multiplexing (OFDM) in a manner similar to IEEE802.11a, but with channel 10MHz. In the future, many applications based on the WAVE technology will be safety-oriented. Unfortunately the IEEE 802.11p amendment designed as it is now does not provide enough guaranties for the support of such applications. One reason of this issue is because the MAC layer of the 802.11p amendment cannot provide any time boundary when transmitting a message.

3.1.2 Access Techniques at the MAC level channel

The MAC layer protocols are responsible for maintaining and managing access to the shared channel. These protocols decide which nodes can access the channel at any given time. Security applications express strict constraints in terms of time to alert the driver of an imminent danger.

So an MAC-level access technology must support these constraints in order to allow the realization of such security applications. There are two main strategies for the acquisition of the channel: contention-free access or controlled access protocol. In those techniques, access to the channel is pre-allocated. One of the main constraints is the need for a central entity to coordinate a fair Resources Management.

The other category refers to techniques with contention or random, as the CSMA in which there is a single shared broadcast channel. In this protocol category, collisions can occur and due to collisions, the time of packet transmission can not be guaranteed. In addition, exposed node / hidden node problem makes the guarantee of a reliable transmission difficult. There are a multitude of issues to consider related to VANETs, as priority support, response time, the uncertain reliability, and the problem of the hidden node.

All these issues must be addressed in order to propose a solution meeting the diverse security applications requirements. Several MAC techniques have been proposed to address these problems. RR-Aloha was proposed by FleetNet [93]. It is based on the slotted-aloha protocol and implements a TS reservation technique in a distributed manner. Ad-HOC MAC [20] is a protocol based on a similar time structure; it provides a distributed reservation protocol to ensure reliable transmission on a broadcast channel to a single jump.

One of the major problems of this technique is that the number of nodes communicating within a same communication range must not exceed the number of TS in the time

frame. Another protocol, DRVC (Direct and Relay protocol for Vehicle Communications) has been proposed to expand access beyond the limits of DSRC. Note that in order to attack the hidden node problem, the standard proposes the use of RTS mechanism (Ready To Send) / CTS (Clear To Send). However, the use of such a technique introduces additional time for association and authentication process.

IEEE 802.11 introduced several approaches for access to the medium; PCF (Point Coordination Function) which is applicable only if a central entity such as an access point is available and DCF (Distributed Coordination Function). Another broader approach inherited from the IEEE networks 802.11ea been proposed to introduce a distinction in terms of quality of service, EDCA (Enhanced Distributed Channel Access). DCF uses the principle CSMA / CA which means that the channel is only available if no activity is detected by the physical layer.

An important parameter is the IFS (Inter-Frame Spaces) that characterizes the time that the channel must be observed idly before a station begins transmission. A station must sense the status of the wireless medium before transmitting. In the case where the channel is busy, the transmitter selects a random number of time slots within a certain range between CWmin and CWmax; then begins to decrease this counter until it reaches zero value inorder to initiate the transmission.

The counter is stopped in the case where the channel is sensed busy. If after sending the frame, no acknowledgment is detected, a retransmission is initiated after exponential waiting (Exponential Backoff). Note that the maximum number of retransmission is limited. One fundamental difference between 802.11p compared to standard 802.11, is the ability to communicate outside of BSS (Basic Service Set) to allow communication on a ad hoc basis in a high mobility environment. This communication architecture reduces the functionality of the MAC layer to a minimum.

Only the necessary frame formats are stored and data are transmitted using QoS EDCA format specified by a packet level. EDCA proposed in IEEE 802.11e to introduce a support service quality. The application generating the message associated with the latter an access category depending on the importance and urgency of the information transmitted to it. Each class is identified by an index (ACI), contains its own queue, and is governed by a set of parameters for coordinating access to the channel. These parameters include the AIFSN and minimum and maximum values of the contention window. In other words, these parameters allow introducing a prioritization on the basis of expectations prior to transmission time. It should be noted that internal collisions can occur and in this case, packets with a higher priority are preferred. Note also that all omitted features for a more

or less instant access should be addressed at a higher level of abstraction.

3.2 Challenges in VANETs

The environments considered in the MANET are geographic and are generally limited open spaces. While in VANET, vehicle movements are related to the road infrastructure; highways, intersections, speed limit, etc. By the nature of movements and high mobility in VANET, vehicles can join and leave the network in a short time, this significantly affects connectivity and quality of service.

3.2.1 Quality of Service In VANETs

One of the most challenging tasks in VANETs is QoS parameters. QoS is defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination [23]. In wired networks, the QoS parameters are generally described in terms of delay and throughput. The QoS parameter in vehicular ad hoc networks is difficult to meet because of the network topology changes, scalability, the delay-constrained routing and the impact of density and driving environments on the offered QoS services. We have two kinds of traffic over VANETs:

- Real-Time, RT: such as safety messages and video/ audio signals
- Non-Real-Time, NRT: such as e-maps and road/vehicle traffic/ weather information.

The difference between RT and NRT imposes diverse quality of service (QoS) requirements for VANET designs. QoS is a big challenge when the VANET is under contention-based (e.g. IEEE 802.11 protocol) environments, where the packet delay and data congestion level increase dramatically as the total number of vehicles contending for the common wireless media. Sending and receiving correct data in a fixed duration of time is critical in this type of networks. Safety warning applications require minimum End-To-End delay because if a warning message is received with high delay, that message could be useless for preventing an accident. Rescue vehicles should instantly receive exact coordinates of the location of an accident to reach the scene of the emergency faster. Furthermore, information about traffic and road hazards could be acquired and fed into vehicle navigation systems in real- time to provide alternate driving routes [66].

Diverse solutions were developed to improve QoS in MANETs. These solutions perform either in the network layer, MAC layer or physical layer. However, their utilization in VANETs presents some shortcomings. Among these solutions, we have proactive proactive and reactive routing protocols. Their suitability for vehicular networks was studied

in different articles [56].Due to the instability of the paths in VANETs, proactive routing protocols such DSDV [53] and OLSR [21] may fail. These protocols are based on the exchange of routing tables between neighbor nodes. This becomes worse in case of large scale networks.

Reactive protocols do not use routing tables but use a flooding method for route discovery that initiates more routing overhead and also suffer from the initial route discovery process. Thus, they become unsuitable for security applications in VANET.

AODV [62] is an example of a reactive protocol. AODV floods the network with route request packets which leads to high overhead. The frequent topology changes in VANETs cause an important traffic which consists on control messages. In addition, the main drawback is that AODV needs end-to-end paths for data forwarding, which is difficult to handle because in VANETs end-to-end paths break often due to high speeds of vehicles. Therefore, it is recommended to develop the existing routing protocols to take into consideration the short life of the paths while respecting end-to-end delay, data losses and optimal use of bandwidth.

Furthermore, clustering is an efficient technique to reduce data congestion and support QoS over wireless networks. Lately, extensive research efforts have been dedicated to the design of clustering algorithms to organize nodes in VANETs into sets of clusters. However, due to the dynamic topology of VANET, nodes frequently joining or leaving clusters compromise the stability of the network. The impact of these perturbations becomes worse on network performance if these nodes are cluster heads. Therefore, cluster stability is the key to maintaining a predictable performance and has to consider reducing the clustering overhead, the routing overhead, and the packet losses.

The non-contention-based method Time Division Multiple Access (TDMA) was proposed as an efficient solution in the physical layer for mobile and sensor networks. This method consists in allocating a time slot for each node to send its packets. It is efficient because it provides high reliable communications, and resolves the problem of hidden nodes. However, in VANET, this method suffers from the merging collisions problem [83] that is due to the changing network topology.

In [26], AODV- ABE establishes forwarding paths that satisfy the bandwidth required by the applications. AODV is improved by introducing Available Bandwidth Estimator In ABE, each node estimates its idle time period by sensing the medium. The available bandwidth estimation of a wireless link in ABE uses the idle time periods of the emitter and

the receiver of the link. However, for a communication to take place, emitter and receiver must be both idle. As there is no reason that emitters and receivers are always idle at the same time, ABE includes, in its estimation, the probability that two end nodes of a link be both idle at the same time. To this end, a uniform random distribution of the medium occupancy over an observation period is assumed. The available bandwidth estimation of a wireless link in ABE uses the idle time periods of the emitter and the receiver of the link.

When a new source wants to send a packet to a destination, AODV-ABE floods a Route Request message (RREQ) to that destination by including the required bandwidth in the RREQ. Each intermediate node that receives the RREQ checks if there is enough bandwidth on the link from which it receives the RREQ. If this is the case, the RREQ is forwarded; conversely, the required bandwidth cannot be satisfied and the RREQ is simply discarded. This allows the establishment of a forwarding path that satisfies the required bandwidth when such a path exists. As expected, AODV-ABE only accepts a new flow if the medium has enough capacity to offer the required throughput. AODV-ABE shows more stable throughputs and establishes forwarding paths that are able to guarantee the required bandwidth, so it is suitable for bandwidth demanding services such as video-streaming.

In [27], Multichannel QoS Cognitive MAC (MQOG) which is a new MAC protocol dedicated for VANET environments is developed. MQOG incorporates efficient channel negotiation on the dedicated control channel whereas data is transmitted on the other channel without contention. MQOG assesses the quality of channel prior to transmission employing a dynamic channel allocation and negotiation algorithm to achieve significant increase in channel reliability and throughput. It uses a unique dedicated control channel and multiple service channels for data transfer. MQOG is capable of prioritizing traffic to ensure QoS mitigating interference in high multipath environments and maximize system throughput by introducing a unique multichannel cognitive operation.

This protocol separates the control traffic from the actual data transmission. A Channel Neighbor State Table (CNST) table is used to track communications between neighboring vehicles. The changes of the topology are reported by the neighboring nodes and stored in the CNST table. The underlying communication and intelligence lies on the control channel to dedicate a service channel for data transfer.

Each vehicle is assumed to have two transceivers. The first one is dedicated for control traffic while the cognitive radio is used for data transmission and reception. A dynamic channel allocation algorithm is used where the cognitive radio assesses the available DSRC channel. Then, the noise and interference level is estimated in order to check

the best available channel. If all the messages to be sent are safety messages and there is no channel with acceptable quality, a vehicle waits until the first good path detected becomes free. The safety messages are prioritized to non-safety messages. A handoff mechanism is considered when a high priority frame must be sent. This frame queries the channel used by low priority frames.

In [32], a new QoS aware routing approach was proposed. In this approach, vehicles within the same transmission range and moving toward the same direction form clusters. Each vehicle can either be a cluster head, a gateway and Ordinary Member (OM). Each node in the scheme is in one of three modes: transmitting mode, receiving mode, and CH mode. Ultimately, The CH utilizes a long range transmission power when it wants to exchange information with its neighboring CHs. Whenever a CH wants to communicate with its cluster member, it chooses a short range transmission power to gather/transmit safety messages over data channel using upstream-TDMA/downstream-broadcast method adopted. Much more, the CH allocates the accessible data channels towards the cluster-member nodes for the non-real-time traffic. Therefore, each CH determines the TDMA frame structure based on the number of OMs within the cluster. Subsequently, to broadcast the safety related messages within the cluster, the CH uses its available mini-slots to broadcast the message on CCH from the TDMA frame.

This approach aims to improve channel utilization, data transfer rate and diminish the number of packet drop. The proposed TDMA-based QoS routing and conventional AODV are show lower performance at lower speed mobility. However, our scheme (see chapter 5) is gradually increase to outperform existing protocol at higher speeds. Therefore, the Overall throughput is significantly high with UDP connection as in comparison to TCP.

TDMA based QoS routing is suitable for the rapid topology changes as a result of high mobility speed. Based on the several issues arising in guaranteeing bandwidth in vehicular ad hoc network, enhancement scheme is proposed [78] by utilizing clustering approach using TDMA scheme. LORA-CBF is a reactive routing protocol with cluster-based flooding for inter-vehicle communications.

Firstly, this protocol improves the traditional routing algorithms, based on non-positional algorithms, by making use of location information provided by GPS.

Secondly, it minimizes flooding of its Location Request (LREQ) packets. Member nodes are converted into gateways when they receive messages from more than one cluster head. All the members in the cluster read and process the packet, but do not retransmit the broadcast message. This technique significantly reduces the number of retransmissions

in a flooding or broadcast procedure in dense networks. Therefore, only gateway nodes retransmit packets between clusters (hierarchical organization).

Moreover, gateways only retransmit a packet from one gateway to another in order to minimize unnecessary retransmissions, and only if the gateway belongs to a different cluster head. The protocol does not generate extra control traffic in response to link failures and additions. Thus, it is suitable for networks with high rates of geographical changes. As the protocol keeps only the location information of the [source, destination] pairs in the network, the protocol is particularly suitable for large and dense networks with very high mobility.

3.2.2 Security In VANETs

VANETs are being increasingly important as they are foreseen to deeply influence and improve road safety and driving conditions. Before implementing VANET applications, different security issues such as authenticity, integrity, must be solved because any malicious behavior of users, such as modification and replay attacks with respect to disseminated traffic-related messages, could be fatal to other users.

Security is not a separate issue but linked to the control and management of QoS network and services. Security is an important issue in any communication system. Due to the fact that VANETs are composed of number of communicating autonomous entities moving at high speed, the randomness of the connectivity between the vehicles and their relative geographic positions raises concerns about users and data security. Most desired security attributes as criteria to measure security for all VANET applications are authenticity, privacy, availability confidentiality, and non-repudiation. Attacks in VANETs hinder vehicles communications by deteriorating or interrupting their functions. To meet the aforementioned security requirements, several approaches were proposed by researchers which aim to prevent or diminish the consequences of attacks.

As we saw before, a Sybil node may create an illusion of trafic congestion. There are several techniques proposed to encounter Sybil attack in VANETs such as statistical and probabilities approaches, signal strength and session keys [52]. Another category of attacks on the data integrity is spoofing which consists on node impersonation. Spoofing is an attempt by a node to send modified version of the message and claims that the message comes from the originator for the unknown purpose.

Messages should reach the destination within the relevant time period. As VANETs consist on vehicles moving at high speed, the development of secure routing protocols is

necessary.

The DSRC/WAVE standard, as specified in a range of standards including those generated by the IEEE P1609 working group, enables V2V and V2I wireless communications. This connectivity makes possible a range of applications that rely on communications between road users, including vehicle safety, public safety, and others. As the number of applications using VANETs increases, so do the risk involved. The safety-critical and the safety-critical nature of many WAVE applications makes it vital that services be specified that can be used to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay.

Additionally, the fact that the wireless technology will be deployed in personal vehicles, whose owners have a right to privacy, means that in as much as possible the security services should respect that right and not leak personal, identifying, or linkable information to unauthorized parties. With this in mind, at the time that IEEE P1609 was established to develop the standards for the DSRC wireless network stack, the IEEE 1609.2 was proposed later from IEEE to develop standards for the security techniques that will be used to protect the services that use this network stack. These applications face unique constraints. Many of them, particularly safety applications, are time critical: the processing and bandwidth overhead due to security must be kept to a minimum, to improve responsiveness and decrease the possibility of packet loss.

In [63], authors developed a secure MAC protocol taking account of the DSRC channel structure. This protocol takes into consideration different security parameters and ensures the freshness of the message using a time-stamp, digital signature and trusted certificate. Considered security parameters are message authentication and integrity, message non-repudiation and privacy and anonymity of the senders. The protocol uses a part of IEEE 1609.2 security infrastructure including PKI (Public Key Infrastructure) and ECC (Elliptic Curve Cryptography). Four queues per OBU are reserved to different priority message classes. To each OBU is associated a scheduler which allows higher-priority message before lower priority messages.

A preemptive policy is adopted to schedule high priority messages to get the channel immediately before the transmission of low priority message is completed. In this approach, each OBU is supposed to have a secure database which contains cryptographic keys used for digital signature. These keys change periodically and are certified by the CA which uses these certificates in case of accident or law investigation to prevent non-repudiation. PKI is used for certificates delivered by the CA for each vehicle. For safety messages, the confidentiality is not required, so they are sent in plaintext. Safety messages are signed

with the private key and include the CA's certificate. A time stamp signed with the private key is added to indicate the freshness of the message. The messages are small sized and do not create an overhead in the network. The other vehicles extract the public key of the sender to decrypt the signature and verify the integrity of the message and the time-stamp.

In [40], a Symmetric-Masquerade Security Scheme (SMSS) was proposed. This new approach achieves security requirements of V2V communications while keeping a low system overhead. In a first step, a vehicle entering the coverage of a certain BS, it broadcasts a message containing a public key to apply for a pseudonym and another one as a pre-shared key which is updated periodically. The message includes a time stamp to avoid replay attacks. After that, the BS assigns a local pseudonym to the vehicle. To protect the privacy of each vehicle, only the base station knows their real names and their corresponding pre-shared key. So when vehicles within the coverage of a BS want to communicate, the BS assists the symmetric key exchange between them to verify the integrity of the nodes.

After the symmetric keys are exchanged between the communicating vehicles, a link is established for a short time to allow secure end-to-end communications without the assistance of the BS. When a vehicle leaves the range of a base station, it returns the pseudonym that will be assigned to a future entering vehicle. BSs maintain a table which records the uni- mapping between the pseudonyms and the real identifications of current users. This mechanism allows the BS to identify imposture immediately. This security scheme does not create overhead in the network such as asymmetric schemes where private and public keys are exchanged between communicating entities.

In [64], a secure position-based routing protocol was developed. Authors applied a security mechanism to the protocol Greedy Perimeter Stateless Routing (GPSR). In this security scheme, every node in the VANET estimates the behavior of other nodes to know if a node has ever tampered or dropped packets previously. The scheme can detect malicious nodes and keep the validation of the routes by detecting the malicious nodes. The security solution comprises two mechanisms: routing message protection mechanism and node evaluation mechanism. For the protection of routing data, a signature verified scheme is employed to achieve end-to-end authentication and integrity. A signature field is added to the routing packet.

For node evaluation, every node is turned in a hybrid mode to check all the messages sent by its neighbors. The reliability of a node is estimated according to its forwarding ratio. The evaluation mechanism used comprises forward evaluation and backward evaluation. Forward evaluation algorithm aims to find out the drop malicious nodes. In the

forward evaluation, a sender assesses the receiver to know if it has relayed the packet. The backward evaluation algorithm is used to find out the tamper malicious node. When a node sends a packet to a neighbor node, the later one assesses the source of the received packet. In a backward evaluation, the integrity of the packet is verified using the digital signature. an evaluation value is calculated using forward and backward evaluation values. Then, the calculated value is compared to the threshold one in order to decide if the corresponding node can be selected as a next hope.

In [22], the security solution relies on location information and corresponding time. A mobility pattern which allows the detection of misbehaving nodes was proposed in order to enhance security and privacy. Vehicles periodically sign and broadcast their current locations. In each time slot, nodes construct their public key and their anonymous pseudonyms address and broadcast them to their neighbor. Location and time id are exchanged between nodes in small intervals of time. The location is used to reveal the existence of the vehicle while keeping its privacy protected because there is no link between the physical vehicle location and the identity of the vehicle. The communication paradigm among vehicles and the periodic location information is used to detect misbehavior.

A vehicle is represented by series of locations in its trajectory. If random locations are received, this behavior is considered abnormal. In order to protect vehicles privacy, nodes communicate using their dynamic locations since vehicles are assumed to be equipped with positioning systems (GPS). When a vehicle gets its location coordination via GPS, it generates two pairs of keys based on group signature, then, the location and time are signed using the private key. A Location Anonymous Message (LAM) is used by the vehicle to broadcast the signed information to its neighbour nodes. When the later receive the message, they store the location in a Location/Time Table (LTT) with the corresponding time. The main contribution of this work is the mobility pattern formation and misbehaving node detection based on it. The mobility pattern helps predicting some possible attacks. LA messages stored in the LTT serve to build the mobility pattern. The location information gathered by the vehicle is compared to the road map to detect malicious nodes which consist on locations that are not within the road perimeter. The mobility pattern helps nodes to evaluate the integrity of the received messages. For example, if a node claims its presence in different locations in a short period of time, this information could be used to detect possible attacks such as Sybil attack. Therefore, the suspect node is removed from the VANET.

In [35], a protocol for Authentication with Multiple Levels of Anonymity (AMLA) is proposed. In this approach, each vehicle is assumed to be connected to a Security Service

Provider (SSP). This server is responsible for providing privates keys to vehicles. When a vehicle decides to be a part of a VANET, it needs from the SSP, a number of pseudonyms and the desired life time of each pseudonym. Each vehicle is supposed to be equipped with a tamper proof device which stores its secret keys. These keys are accessed only by the SSP to keep the privacy of the vehicle. To ensure authenticity of messages, AMLA uses the Identity-Based Encryption (IBE) and signature mechanism. A vehicle transmits messages signed with its private key corresponding to one of its pseudonyms, so its identity remains hidden. The private key of a vehicle is a function of its pseudonym. When the neighboring nodes receive the message, they use the public key of the sender and the public key of the SSP. AMLA provides different levels of anonymity to vehicles which are determined by the number of pseudonyms and the lifetime of each pseudonym. AMLA implements short term credentials without the use of any public key certificate; this keeps the overhead in the network low compared to certificate based approaches.

3.3 Conclusion

In recent years, the development of new technologies has favored an evolution of transport systems. This change aims to make transportation safer, more efficient, more reliable and more environmentally friendly, without necessarily having to alter physically existing infrastructure. In this chapter, we described the entities in a wireless vehicular and their roles, and type of communication (V2V, V2I). We especially noticed that communications V2V raise the constraints of network performances (delay, multi-hop routing and dynamic topology) and a need for confidence (lack of infrastructure); that is why we are interested in V2V communications.

Vehicles may be in radically different environments from a cluttered city center, to a lonely country road or a busy motorway. To better understand the VANET networks, we have detailed and discussed their security issues. The vehicle communications are standardized across all standards IEEE 1609. This set of standards defines the various layers of the OSI model for wireless vehicular communications. So we have detailed the role and function of each layer standard IEEE 1609.

In the remainder of this thesis, we focus on an interconnection network in which each vehicle is equipped with a DSRC equipment that meets the IEEE 1609 standard.

Part IV

Improving QoS in MANETs

"Improving tcp performance in manet by exploiting mac layer algorithms. IRACST-International Journal of Research in Management & Technology (IJRMT), 2011. Published"

CHAPTER 4

Improving QoS in MANETs

4.1 Introduction

Transmission Control Protocol (TCP) [53, 21] is the transport protocol used in the most IP networks [68] and recently in ad hoc networks like MANET [63]. It is important to understand the TCP behavior when it is coupled with IEEE 802.11 MAC protocol in an ad-hoc network.

Important examples include Carrier Sense Multiple Access (CSMA) with collision avoidance that uses a random back-off even after the carrier is sensed idle [56]; and a virtual carrier sensing mechanism using RTS/CTS control packets [62]. Both techniques are used in IEEE 802.11 MAC protocol [56] which is a current standard for wireless networks.

When the interactions between the MAC and TCP protocols are not taken into account, this may degrade MANET performance notably TCP performance parameters (like throughput and end-to-end delay) [60, 79, 82]. To adapt the behavior of these two protocols to ensure better TCP performance and then better QoS [70], it is very important to study the interactions between them. This chapter discusses our contribution, IB-MAC, which takes into account the mobility of nodes, and compares it with other solutions that have been proposed in the same context.

After a short presentation of MAC and TCP protocols, we will present our IB-MAC and study its incidences on TCP performance parameters (throughput and end-to-end delay). IB-MAC proposes a dynamic adaptation of the maximal limit of the MAC backoff algorithm. This adaptation is a function of the number of nodes in the network and their mobility.

4.2 Interactions between MAC and TCP

4.2.1 MAC 802.11 and TCP Protocols in MANET

The IEEE 802.11 MAC protocol is the access technology to the channel we used in this chapter. There are two modes of operation of this protocol:

- PCF mode (Point Coordination Function): is used to support synchronous traffic such as traffic in real time. This mode is used in the case of networks with infrastructure, as an access point is required.
- DCF mode (Distributed Coordination Function): is used by mobile ad hoc networks.

We are focusing on the DCF mode which is based on the use of CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) for the transmission of asynchronous data. The operating principle of the DCF is to listen to the communication channel to detect whether the channel is free (IDLE) or if another node is transmitting. Before each transmission, the node must check that the channel is free for a certain period called DIFS (Distributed Inter Frame Space).

In the case where the channel is busy, transmission is deferred by a certain time, called backoff time, which is selected randomly within a contention window (Contention Window: CW). The value of the backoff is decremented if the channel is free. However, a collision may occur if two stations transmit at the same time, but the transmitting station has no way to detect this collision. Thus, an acknowledgment mechanism (ACK) is required to inform the station issuing of the receipt of the package.

In addition, to avoid the hidden node problem and reduce the number of collisions stations, the RTS / CTS mechanism [58, 23, 60] (Request To-Send / Clear-To-Send) is used. With this mechanism, the transmitting station sends a RTS control packet in order to inform the neighboring resorts of its wish to transmit and the transmission time called NAV (RTS). Once the receiving station receives the RTS packet correctly, it will respond with another CTS control packet in order to inform its neighbors of its receiving state during a term NAV (CTS). All stations receiving either the control packet RTS, CTS must be blocking their transmission during NAV (RTS) or NAV (CTS) respectively. When the transmitting station receives the CTS packet, it concludes that its RTS packet has been received by the receiving station and therefore it has reserved the channel for transmitting. It will therefore start the transmission of the DATA packet. If the receiving station receives the DATA packet successfully, it will respond with an acknowledgment to inform the transmitting station of the receipt of the DATA packet.

It has been shown that TCP does not work well in a wireless network [53, 66]. The wireless channel is subject to noise, and packet losses are common. TCP associates the packet loss to the congestion, and then it starts its congestion control mechanism. Therefore, transmission failures at the MAC layer lead to the congestion control activation by TCP protocol and then the number of packets is reduced (throughput). Several mechanisms have been proposed to address this problem [26, 32, 29], but most of them focus on the cellular architecture. The problem is more complex in multi- hop networks such as MANET where there is no base station and each node can act as a router [47, 48].

The TCP Performance parameters (like throughput and end-to-end delay) have been the subject of several evaluations. It has been shown that these parameters degrade when the interactions between MAC and TCP are not taken into account [53, 58]. The major source of these effects is the problem of hidden and exposed nodes [58, 23]. The most important solution which has been proposed to the hidden node problem is the use of RTS and CTS frames [40, 75]. Although the use of RTS/CTS frames is considered as a solution to the hidden node problem, it was shown in [58, 80] that it also leads to further degradation of the TCP flow by creating more collisions and introducing an additional overhead which decreases the TCP performance.

4.2.2 Related Works

In [26, 27, 32, 90, 97, 95, 64, 23, 22, 35], many analyses of TCP protocol performance are done and several solutions on how to improve its performance are proposed. In this subsection we present the most important solutions.

Yuki et al. [95] have proposed a technique that combines data and ACK packets and have shown through simulation that this technique can make radio channel utilization.

Altman and Jimenez [23], proposed an improvement for TCP performance by delaying 3-4 ACK packets. In their approach, the receiver always delays 4 packets (except at the startup) or less if its timeout interval expires. The receiver uses a fixed interval of 100ms and does not react to packets that are out-of-order or filling in a gap in the receiver buffer, as opposed to the recommendation of [31].

Kherani and Shorey [64], suggest signicant improvement in TCP performance as the delayed acknowledgement parameter and the TCP window size.of the approach is the analytic modelling of TCP over IEEE 802.11 networks with a delayed acknowledgement parameter, and a TCP window size both greater then 2.

Allman [22], conducted an extensive evaluation on Delayed Acknowledgment (DA) strategies, and presented a variety of mechanisms to improve TCP performance in the presence of side-effect of delayed ACKs.

Chandran [35] proposed TCP-feedback, with this solution; when an intermediate node detects the disruption of a route it explicitly sends a Route Failure Notification (RFN) to the TCP sender. On receiving the RFN, the source suspends all packet transmissions and freezes its state. But when a middle node learns of a new route to the destination, it sends a Route Re-establishment Notification (RRN) to the source.

Holland and Vaidya [53] proposed a similar approach based on Explicit Link Failure Notification (ELFN): when the TCP sender is informed of a link failure, it freezes its state. However, the source continues to send out packets at regular intervals to determine if a new route is available.

Liu and Singh [71] proposed the ATCP protocol; it tries to deal with the problem of high Bit Error Rate (BER) and route failures. The ATCP layer is inserted between the TCP and IP layers. ATCP puts TCP agent into the appropriate state after listening to the network state information provided by Explicit Congestion Notification (ECN) messages and by ICMP ”Destination Unreachable” message. On receiving a ”Destination Unreachable” message, TCP agent enters a persisting state.

Fu et al. [46] investigated TCP improvements by using multiple end-to-end metrics instead of a single metric. They claim that a single metric may not provide accurate results in all conditions. They used four metrics: inter-packet delay difference at the receiver, short-term throughput, packet out- of order delivery ratio, and packet loss ratio. These four metrics are cross-checked for accurate detection of the network internal state.

Biaz and Vaidya [30] evaluated three schemes for predicting the reason for packet losses inside wireless networks. They applied simple statistics on observed Round-Trip Time (RTT) and/or observed throughput of a TCP connection for deciding whether to increase or decrease the TCP congestion window. The general results were discouraging in that none of the evaluated schemes performed really well.

Liu et al. [72] proposed an end-to-end technique for distinguishing between packet loss due to congestion from packet loss by a wireless medium. They designed a Hidden Markov Model (HMM) algorithm to perform the mentioned discrimination taking RTT measurements over the end-to-end channel.

Kim et al. [65] proposed the TCP Buffering capability and Sequence information (TCP-BuS), uses the network feedback in order to detect route failure events and to take convenient reaction to this event. The novel scheme in this proposal is the introduction of buffering capability in mobile nodes. The authors select the source initiated on-demand ABR [54] (Associativity-Based Routing) routing protocol.

Oliveira and Braun [36] propose a dynamic adaptive strategy for minimizing the number of ACK packets in transit and mitigating spurious retransmissions. Using this strategy, the receiver adjusts itself to the wireless channel condition by delaying more ACK packets when the channel is in good condition and less otherwise.

Hamadani and Rakocevic [50] address the problem of TCP intra-flow instability in multi-hop ad hoc networks. They propose a cross-layer algorithm called TCP Contention Control that it adjusts the amount of outstanding data in the network based on the level of contention experienced by packets as well as the throughput achieved by connections.

Zhai et al. [96] show that TCP suffers severe performance degradation and unfairness. Realizing that the main reason is the poor interaction between traditional TCP and the MAC layer, they propose a systematic solution named Wireless Congestion Control Protocol (WCCP) to address this problem in both layers. WCCP uses channel busyness ratio to allocate the shared resource and accordingly adjusts the senders rate so that the channel capacity can be fully utilized and fairness is improved.

Lohier et al. [73] proposes to adapt one of the MAC parameters, the Retry Limit (RL), to reduce the drop in performance due to the inappropriate triggering of TCP congestion control mechanisms. Starting from this, an MAC layer Loss Differentiation Algorithm (LDA) is proposed. This LDA scheme is based on the adaptation of the RL parameter depending on the quality of the 802.11 wireless channels.

All the approaches presented above suggest improvements to TCP performance based either on MAC protocol or TCP protocol or on both. Our approach also improves the TCP performance, and it is based on the backoff algorithm of MAC protocol. In what follows, we examine the interactions between MAC and TCP protocols before proceeding to the presentation of our solution.

4.2.3 IB-MAC Improvement of the backoff algorithm

The MAC protocol is based on the Backoff algorithm that allows it to determine which node will access the wireless medium in order to avoid collisions. In the case of station finding a channel busy, the transmission is differentiated in accordance to the Backoff procedure whose principle is: as long as the channel is free for a DCF Inter-Frame Space (DIFS) time (after a successful reception) or for an Extended Inter-Frame Space (EIFS) time (after a failed reception), the Backoff time is decreased. This time is calculated as follows:

in 4.1, where SlotTime is a constant time and BackoffCounter is an integer from a uniform distribution in the interval [0, CW] and CW is the contention window who is minimum and maximum limits are (CW_{min}, CW_{max}) and are defined in advance in. The CW value is increased in the case of non-availability of the channel using the following formulas in 4.2.

$$Backoff time = Backoff counter \times SlotTime \tag{4.1}$$

$$\begin{aligned} m &= m + 1 \\ CW(m) &= (CW_{min} + 1) \times 2^m - 1 \\ CW_{min} &\leq CW(m) \leq CW_{max} \end{aligned} \tag{4.2}$$

m: the number of retransmissions.

The first parameter used by our IB-MAC solution is the number of nodes in the network. When the number of nodes in the network increases, the performance of TCP deteriorates. The cause of this degradation is the frequent occurrence of collisions between nodes. As the number of node increases, the collisions become more frequent. These collisions become more frequent with a small backoff interval because the probability of having two or more nodes choose the same value in a small interval is greater than the probability that these nodes choose the same value in a larger interval. Note by *I* this interval, *S* its size, and $Pr(i, x)$ is the probability that the node i chooses the x value in the interval I. The problem then is how to ensure that for any two nodes i and j in the network with $i \neq j$, the formula (4.3) is verified.

For an important number of nodes in the network, and for a high probability that the formula 4.3 will be verified, we must have a larger *S*. To do this we have to make the size *S* adaptable to the number of nodes in the network, then we intervene on one of the limits of this interval, we then propose the maximum limit CW_{max}.

$$|Pr(i,x) - Pr(j,x)| \neq 0 \tag{4.3}$$

If n is the number of nodes in the network. Lets note by F(n) shown in formula 4.4.

$$F(n) = Log(n) \tag{4.4}$$

Log () is used here because the effects of the large values of the nodes number on the TCP performance are almost the same.

Our IB-MAC also takes into account the mobility of nodes. In fact, node mobility often leads to the breakdown of connectivity between nodes, resulting in loss of TCP packets and then the degradation of the TCP performance parameters (throughput and end-end-end delay). At the MAC protocol, when the packets losses are detected, they are associated to the collisions problem, which is not the case here. Then, when the mobility increases, the backoff interval also increases, something that should not have happened because these packets are lost due to the rupture of the connectivity and not to the collisions. Therefore, we will try to find a compromise between the effect of mobility and the size of the backoff interval.

Mobility is generally characterized by its speed and angle of movement. These two factors determine the degree of the impact of mobility on packets loss. Consider a node i, in communication with another node j, then we note by:

- α_i: the angle between the line (i, j) and the movement direction of node i.

- Wi : the speed of mobile node i.

To consider the impact of mobility on the loss of packets is equivalent to considering the impact of its two parameters, Wi and α_i. For the effect of Wi, we use a logarithmic function because for large values of speed mobility the results converge. But when the node is static (Wi=0) the effect of the mobility becomes zero, and then we must add 1 to the equation, so lets note by H(Wi):

$$H(Wi) = 1/Log(Wi + 1) \tag{4.5}$$

Also, the direction of the node movement determines the degree of the influence of mobility on packets loss; it is given by G(Wi, α_i):

$$\mathrm{G}(W_i, \alpha_i) = \begin{cases} 1 & if -\pi/4 \leq \alpha \leq \pi/4 \\ 1/\sqrt{(W_i + 1)} & \text{else} \end{cases} \tag{4.6}$$

Note that G(W, α) = 1 when W = 0 (without mobility). We added 1 to ensure that G will be defined for all the W values, and we used a ratio to get a positive effect of G on the backoff algorithm.

With 4.5, 4.6 we can guarantee that when the mobility of nodes is significant, the adaptation of the backoff algorithm is not important because this mobility is more probable to be the cause of many loss packets. But with weak mobility the same equation makes it possible to get a significant adaptation to the backoff algorithm because in this case the collisions between frames are more probable to be the cause of the losses packets.

From 4.4, 4.5 and 4.6, we will have now the new expression of CW_{max} for node i as follows:

$$CW_{max}(n, W_i, \alpha_i) = CW_{max0} + F(n) \times H(W_i) \times G(W_i, \alpha_i) \tag{4.7}$$

CW_{max0}: initial CW_{max} defined by the MAC protocol (for the 802.11 version, it is equal to 1024).
n: the number of nodes in the network.

Our approach is fully distributed within the MANET; each node may determine alone the values of n, W and so it can then calculate the value of CW according to formula (4.7). The value of n is updated always when a new node arrives to the network or leaves.

After having made the values of CW_{max} adaptive to the number of used nodes and their mobility, the IB-MAC (improved version of that given by the formula 4.2 for node i) becomes:

$$\begin{aligned} m &= m + 1 \\ CW(m) &= (CW_{min}(n) + 1) \times 2^m - 1 \\ CW_{min} &\leq CW(m) \leq CW_{max}(n, W_i, \alpha_i) \end{aligned} \tag{4.8}$$

m:	the number of retransmissions.
n:	the number of the used nodes .
α_i:	the angle between the line formed by the mobile node and its corresponding node and the movement direction of this mobile node.
CW_{max}(n, W, α):	see 4.7
W_i:	the speed of mobile node i.

4.2.4 Evaluation of IB-MAC and its impact on TCP performance

The evaluation is performed through the simulation environment NS-2 [5] from Lawrence Berkeley National Laboratory (LBNL) with wireless extension of CMU [6]. The MAC level uses the model 802.11b with the DCF (Distributed Coordination Function) which the values of its basic parameters are listed in the in TABLE 4.1.

Parameters	Values
Preamble length (bit)	144
RTS length (bit)	160
CTS/ACK length (bit)	112
MAC header (bit)	224
IP header (bit)	160
SIFS(μs)	10
DIFS(μs)	50
Slot time(μs)	20
Contention window	31
Retry limit	7

Table 4.1: IEEE 802.11b Basic parameters

All nodes communicate through wireless links in half-duplex with an identical bandwidth of 1 Mb/s. For our simulations, the effective transmission range is of 250 meters and an interference range of 550 meters. Each node has a queue buffer link layer of 50 packets managed with a mode drop-tail [45].

The scheduling packet transmissions technique is the First in First out (FIFO) type. The propagation model used is the two-ray ground model [33].

Our simulations are done with reactive routing protocol AODV (Ad hoc On Demand Distance Vector) [85]. We used TCP NewReno [44] which is a reactive variant, derived and widely deployed, and whose performances were evaluated under conditions similar

to those conducted here. This choice is because the previous work [51] has shown almost similar results for different routing protocols and TCP versions used. TCP traffic was used as the main traffic network. The different TCP variants are analyzed on the same topologies and the same pair source/destination are chosen by trial to ensure fairness and relevance of results.

The values, such as the duration of the simulation, the speed of the nodes, and the number of connections have been established in order to obtain interpretable results compared to those published in the literature. The simulations are performed for 1000 seconds, in order to analyze the full spectrum of TCP throughput.

We considered two cases: without and with mobility. In the first case, chain topology is studied where node 1 will transmit to node n (n is the length of the chain).

The distance between two neighboring nodes is 200 meters and each node can communicate only with its nearest neighbor. The interference range of a node is about two times higher than its transmission range (550 meters in our case).

In the mobility case, we study a random topology with two cases: low and high mobility. In both cases, it is only the node 1 that sends for the node n. The mobility model uses the random waypoint model, this particular model is widely used in the literature [55]. In this model, the node mobility is typically random and all nodes are uniformly distributed in space simulation. The nodes move in 2200m*600m area, each one starts its movement from a random location to a random destination. Once the destination is reached, another random destination is targeted after a pause time.

We have simulated several scenarios with different numbers of nodes n and mobility values. We are interested in each scenario into two parameters. The first is the throughput which is given by the ratio of the received data on all data sent. The second parameter is the end-to-end delay which is given by (time for receipt of data - the data transmission time) over number of data packets received.

In these scenarios, we compare our solution (IB-MAC) with MAC standard and two other solutions proposed in the literature. Like our IB-MAC improvement, these solutions use the MAC layer to improve TCP performance in the MANET. The first solution is WCCP [96] and the second one is MAC-layer LDA (Loss Differentiation Algorithm) [73]. The principle of each solution is given in the section of related work. Two cases are also considered, with and without mobility.

We see, through Figure 4.1, with MAC protocol, the throughput decreases when the number of nodes participating in the network increases. This degradation at a given time (from n=100 nodes) begins to take stability. This degradation is due to TCP packet loss, and it becomes more important as the size of the network increases. With the analysis of the trace files for these graphs, we found that RTS and CTS frames, handled at the MAC level, are sensitive to the network size, and, as the number of nodes increases, the rate of loss of those two frames increases too. Such frames losses in such conditions of simulations are mainly due to the consequences of hidden and exposed nodes.

But when the IB-MAC is used as MAC protocol we see that the throughput is smaller. There is an important improvement of this parameter, even if there is a slight decrease when the number of nodes increases but this decrease is much smaller compared to the first case when the MAC protocol is used. This improvement is due to the use of the adaptive nature of our solution IB-MAC to the nodes number in the network.

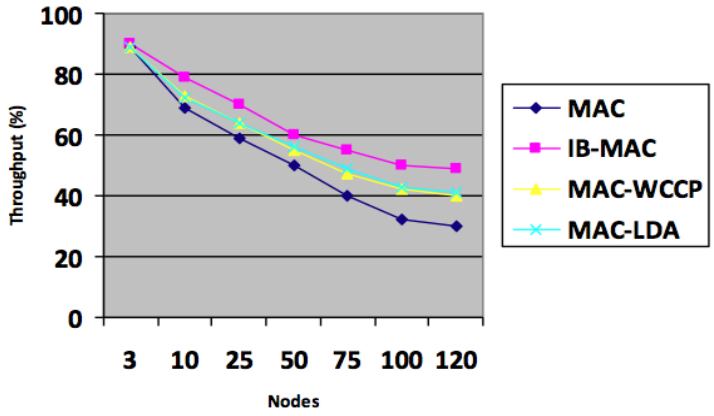

Figure 4.1: Throughput variation without Mobility (chain topology).

Figure 4.2, shows the evolution of the second parameter studied which is the end-to-end delay when the nodes number increases. With MAC protocol, we find that this parameter significantly increases with the increase of the number of used nodes . The increase of the end-to-end delay is essentially due to the detection of frequent loss of TCP packets in the network as the number of nodes increases. These losses will cause the frequent start of the congestion avoidance mechanism by the TCP protocol, so that will result in delaying the transmission of TCP packets. This increase in delay begins to stabilize from n = 110 nodes and it occurs below t = 1.2 s approximately.

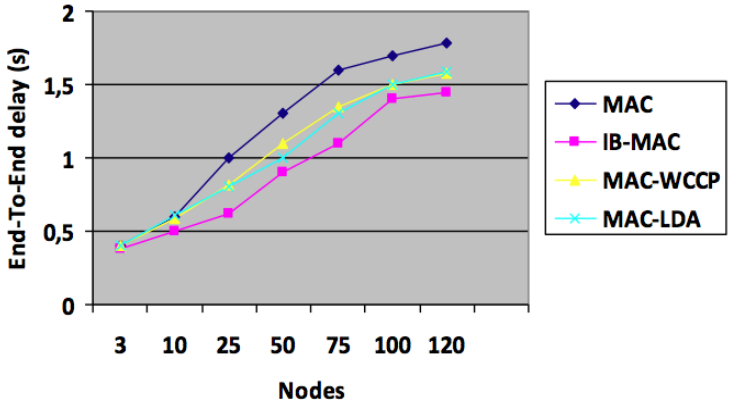

Figure 4.2: End-To-End Delay variation without mobility (chain topology).

When the IB-MAC is used as MAC protocol we see that the end-to-end delay is better. There is an important improvement of this parameter, even if there is a slight increase when the number of nodes increases but this decrease is smaller compared to the first case when the MAC protocol is used. Figure 4.1 and Figure 4.2 show that our IB-MAC outperforms not only MAC standard, but also similar techniques that have been proposed in the literature. The results of the variation of the throughput and the end-to-end delay parameters are better than those of MAC-LDA, MACWCCP and MAC standard. The improvement of the throughput and end-to-end delay parameters is due to the dynamic nature of our new IB-MAC algorithm which makes the size of the backoff interval adjustable to the nodes number in the network. This adjustment reduces the probability of collisions between nodes, thus the number of lost packages decreases while the throughput and delay are improved.

For the weak mobility (Figure 4.3 and Figure 4.4), when the MAC protocol is used, we found an important degradation of the throughput and end-to-end delay parameters in comparison to the first case (without mobility). To explain this degradation, we analyzed the obtained trace files and we found:

- i) The increase of RTS/CTS frames losses with the increase of nodes number in the network (same as the first case without mobility).

- ii) There are TCP packets losses even if there are successful RTS/CTS frames transmissions. In this case, these losses are caused by the unavailability route due the nodes mobility (the used route is outdated, denoted by "NRTE" in the trace file).

We deduce through i) and ii) that the mobility of nodes, although it is weak (here speed W = 5 m/s), participates to the degradation of the throughput and end-to-end delay parameters.

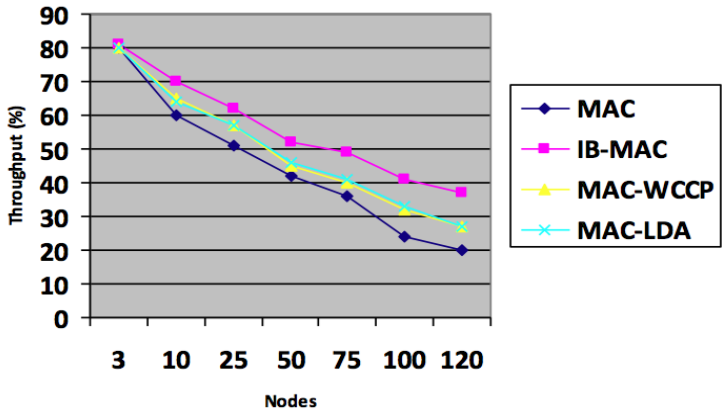

Figure 4.3: Throughput variation with weak mobility (speed W=5 m/s).

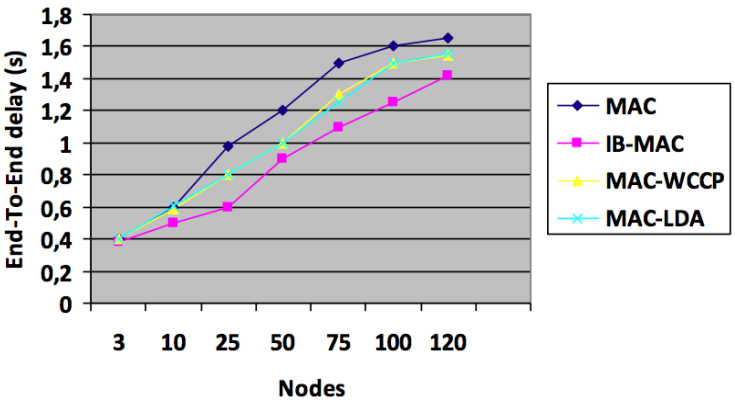

Figure 4.4: End-To-End Delay variation with weak mobility (speed W = 5 m/s).

With our IB-MAC solution, always with weak mobility, we found an important improvement of the throughput and end-to-end delay parameters in comparison to the first case when the MAC protocol is used. Our IB-MAC algorithm makes the size of the back-off interval adjustable to the nodes number in the network and their mobility. For this reason, even for the case where the nodes are mobile, the probability of collisions between nodes is reduced, and then throughput and the end-to-end delay parameters are improved. Figure 4.3 and Figure 4.4 shows also that IB-MAC outperforms the others protocols used (MAC-LDA and MAC-WCCP). The results of the variation of the throughput and the end-to- end delay parameters are better than those of the others protocols. Although there is a

slight difference in performance our strategy remains better than the other three used here.

For strong mobility (Figure 4.5 and Figure 4.6), we see that there is also a degradation of the throughput and end-to-end parameters when the MAC protocol is used, more important than the case with weak mobility because here the breaks connectivity increases then the links stability becomes more important. We have done the same analysis as above to know the reasons of this degradation; we found that the causes of this degradation are related to those discussed in i) and ii) in weak mobility case.

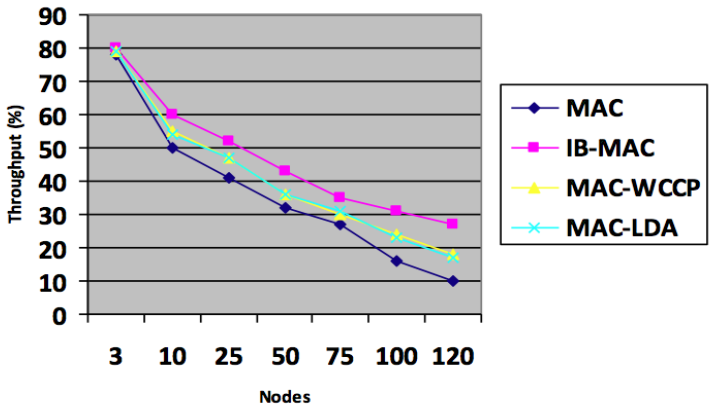

Figure 4.5: Throughput variation with strong mobility (speed W=25 m/s).

In fact, when the network has weak mobility (nodes with low speeds), it presents a rather high stability; in this case links failures are less frequent than in the case of a high mobility. Consequently, the fraction of data loss is smaller when the nodes move at low speed (strong mobility mean moving at low speed) and grows with the increase in their mobility. In this case too (weak mobility), with our solution IB-MAC, we found an important improvement of the throughput and end-to-end delay parameters in comparison to the first case when the MAC protocol is used. We also found an improvement of the throughput and end-to-end delay parameters in comparison to the others protocols (MACLDA, MAC-WCCP). From these results, we can say that even in the case of a random topology where nodes are mobile (a feature specific to MANET networks) the IB-MAC solution improves the performance of TCP.

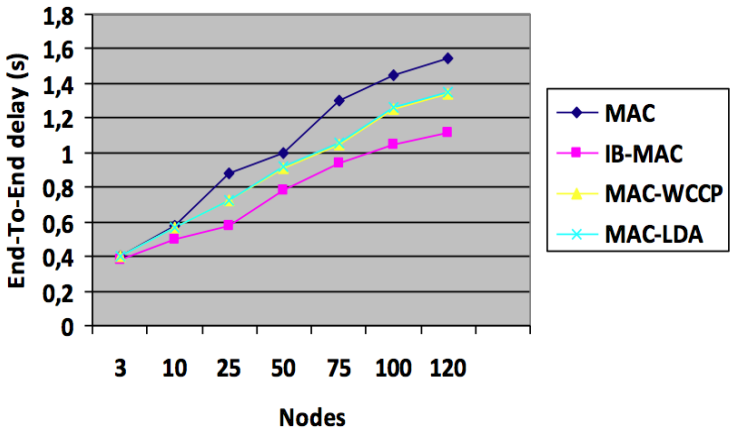

Figure 4.6: End-To-End Delay variation with strong mobility (speed W = 25 m/s).

4.3 Conclusion

Improving TCP performance over 802.11 MAC protocol in multi-hop mobile ad-hoc networks is truly a problem on the interaction between two layers. In this chapter, we proposed an improvement of TCP protocol performance (throughput and end-to-end delay) in MANET. Our solution is IB-MAC which is a new Backoff algorithm making dynamic the CW_{max} terminal in depending on the number of nodes used in the network and their mobility. We studied the effects of IB-MAC on TCP performance, we limited our studies on very important parameters in such networks which are throughput and end-to-end delay because they have great effects on the performance of TCP protocol. The results are enough good and showed that our algorithm can outperform not only MAC standard, but also similar techniques that have been proposed in the literature like MAC-LDA and MAC-WCCP.

We do not claim that our IB-MAC solution is the optimal backoff algorithm that can be used for the purpose of improving TCP performance, but the results we achieved are indeed encouraging, justifying further investigation on this direction.

Part V

Improving TCP Performance on WAVE Networks

"Improving TCP Performance on WAVE Networks, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, 2015, Published"

CHAPTER 5

Improving TCP Performance on WAVE Networks

5.1 Introduction

The idea to introduce a certain level of intelligence in vehicles by equipping them with sensors, actuators and processing units is interesting. But in order to to build a comprehensive view of all the traffic and the environment, vehicles equipped with intelligence must exchange information. Several standards were introduced as IEEE 802.11p and frequency ranges have been dedicated to the vehicular communication as the Dedicated Short Range Communication Standard (DSRC) [7] and Wireless Access in Vehicular Environment (WAVE) [16].

DSRC covers the frequency band [5.850GHz, 5.925GHz] (75MHz) to support the communication for short and medium range (between 300 and 1000 m) with a transfer rate data from 3 to 27Mbps. This frequency band is segmented into seven channels, 10 MHz each, with the first 5MHz used as guard interval. All the channels are divided into a control channel (CCH) and six service channels (SCH).

The channel numbers are determined by the offset of the center frequency 5.000 GHz with units of 5 Mhz (the first 10 Mhz are distributed from 5855 to 5865 GHz with a center frequency of 5.860 GHz which is 860 Mhz above the baseline, corresponding to an offset of 172 units of 5 Mhz, hence the number 172). The channels 174 and 176 can be combined to form the channel 175 of 20 MHz; this is the case also for channels 180 and 182. The control channel is reserved for the transmission of network management messages and high priority messages, such as the critical messages related to road safety. The six other channels are dedicated to the transmission of data from different services advertised on the control channel. The DSRC spectrum is shared between the OBU (On Board Unit) and the RSU (Road Side Unit) in a given space. With this sharing, interference is possible between a node that transmits and another node that listens. Two types of interference are identified; co-channel interference (if both nodes use the same channel), the interference

between two channels (if both nodes are in different channels but are spectrally close).

Since 2003, the IEEE organization has initiated work to define a new standard dedicated to communications in the DSRC band. This standard known as IEEE 802.11p / WAVE (Wireless Access in Vehicular Environments) [18] uses the concept to ensure multichannel communications for safety applications. This protocol addresses a lack of homogeneity between automobile manufacturers and provides sufcient support for the organization functions, management and operation mode for vehicular communication. WAVE provides a set of services and interfaces that allow collectively ensuring V2V or V2I.

IEEE 802.11p is the protocol on which WAVE supports at the MAC layer and the physical layer. At the MAC layer, 802.11p is based on CSMA/CA. Extensions 802.11p MAC address management the message priority to better manage delay-sensitive applications. At the 5,9GHz physical layer, IEEE 802.11p uses OFDM (Orthogonal Frequency Division Multiplexing) similar to IEEE802.11a, but with channels of 10MHz.

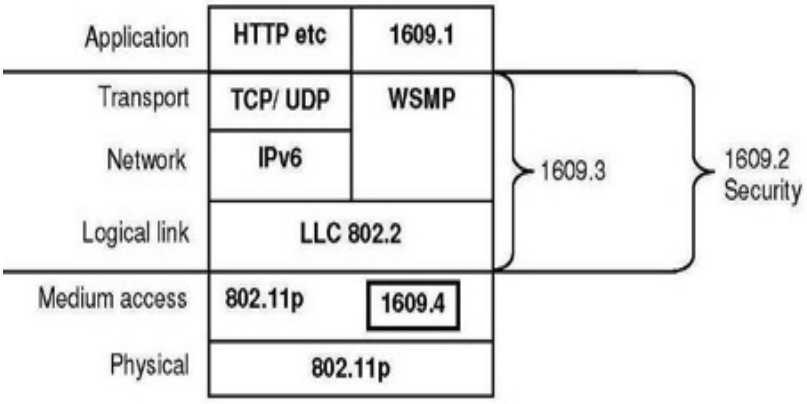

Figure 5.1: Protocols stack of an IEEE 802.11p/1609 network.

The WAVE protocol is based on family IEEE1609 protocols to operate in the band DSRC. The IEEE 1609.4 standard has a strong relationship with the EDCA (Enhanced Distributed Channel Access) mechanism of the MAC sublayer [17]. EDCA provides access to distributed and differential media using eight user priority levels for four access categories (Voice, Video, Best Effort, Background). This mechanism allows to assign a priority to each message. For example, a road traffic security application message will have a higher priority than an application comfort message.

The CCH channel is dedicated to exchange network control messages while SCHs are used by nodes to exchange their data packets and WAVE-mode short messages. The link bandwidth of these channels is further divided into transmission cycles on the time axis, each comprising a control frame and a service frame. These frames are presented by the

pink blocks and blue blocks, respectively in Figure 5.2. In the draft standard defined in [17], it is suggested that the duration of a frame (either a control or a service frame) is set to 50 milliseconds. A footnote in the draft standard states that this value may be adjusted in the future standard, showing that different values may be used for different applications. In a transmission cycle, the control frame must be on CCH whereas the service frame can be on a specific SCH. The operation of the WAVE mode is briefly explained below.

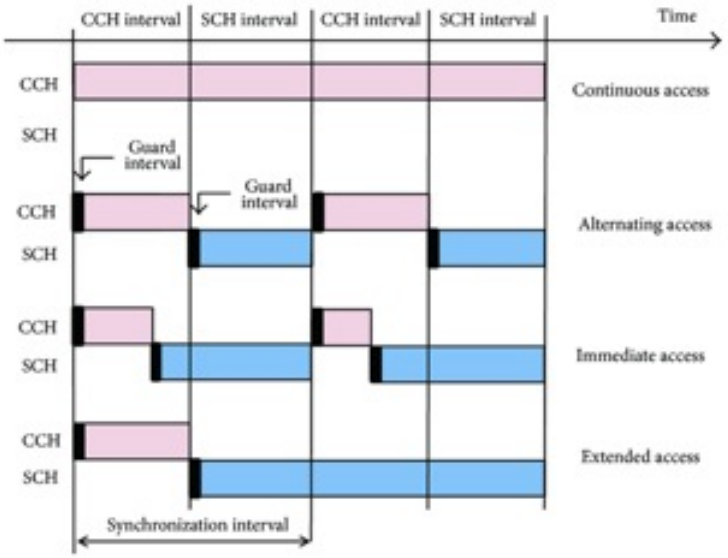

Figure 5.2: Four channels switching schemes [17].

The above CCH/SCH channel is a switching scheme results in a bandwidth wastage problem. Suppose that a packet transmission is going to take place (after the DIFS and Back-off time mandated by IEEE 802.11(a)) near the end of a service frame. The estimated transmission time (ETT) for this packet, however, exceeds the residual time of the current service frame. Because all nodes must switch back to CCH at the beginning of the following control frame, the receiving node cannot completely receive this packet with success. As such, the IEEE 802.11p/1609 draft standards recommend that in such a condition the transmitting node should prevent sending out this packet but instead should send it in the next service frame. Although this design avoids bandwidth wastage caused by incomplete packet reception, it results in bandwidth wastage at the end of each service frame due to not using the residual time.

Assume that in an IEEE 802.11p/1609 network a node is serving a flow that continuously generates packets of 1400bytes in length, and the data rate of a channel is fixed to 3 Mbps, which is the mandatory data rate that an IEEE 802.11p device must support. As such, the ETT of a 1400-byte data packet is 3.646 milliseconds. Suppose that the duration of a service frame is set to 50 milliseconds. In such a condition, if a node refrains itself

from transmitting a packet near the end of a service frame due to the reason stated above, it will waste the channel bandwidth by 7.3% (3.646/50) in the worst case. Such bandwidth wastage will increase as the duration of a service frame decreases. For example, it will increase up to 18.23% if the frame duration decreases to 20 milliseconds. As stated above, the draft standard states that different durations can be used for IEEE 802.11(p)/1609 networks. Sometimes, it may be advantageous to use shorter frame duration to achieve less end-to-end packet delays for real-time and emergent safety applications. In such applications, this bandwidth wastage problem can be significant.

5.2 Improving TCP Performance

5.2.1 Enhanced ETT scheme

In this subsection, we evaluate the TCP performances of IEEE 802.11p/1609 networks under various network configurations. Then, we propose an easy-to-implement scheme E-ETT (Enhanced ETT) to reduce bandwidth wastage caused by channel switching in an IEEE 802.11p/1609 network.

As explained in the introduction, for a transmitting node if the ETT of the first packet in its output queue exceeds the residual time of the current service frame, it should prevent transmitting this packet. To reduce the bandwidth wasted by this design, we propose the E-ETT scheme to utilize the residual time at the end of a service frame. Assume that a transmitting node is going to transmit a data packet pkt near the end of a service frame, as shown in Figure 5.3, as such there is no unused time (bandwidth) in a service frame, which mitigates the bandwidth wastage problem.

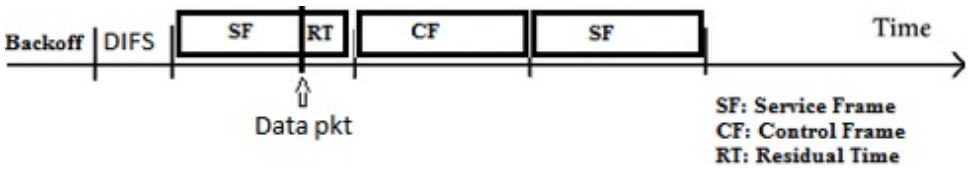

Figure 5.3: Bandwidth wastage problem.

In the E-ETT scheme, we use a partition of the transmitting pkt into two fragments pkt_1 and pkt_2. Based on the adopted data rate, the transmitting node determines the length of pkt_1 so that the ETT of pkt_1 is equal to the residual time of the current service frame.

The fragmentation scheme utilizes the residual bandwidth of a service frame as shown in Figure 5.4 at a small cost of one MAC-layer header and ACK packet for the second

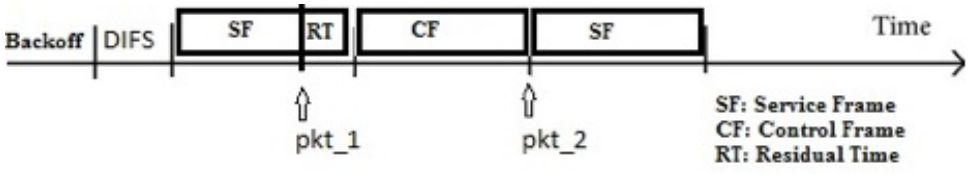

Figure 5.4: E-ETT Scheme.

fragment (i.e., pkt_2) of a fragmented packet. Using the E-ETT scheme, the packet fragment pkt_1 can be transmitted in the current service frame to the receiving node. However, the receiving node cannot deliver the received packet fragment pkt_1 to the upper-layer application in the current service frame. Instead, it must keep pkt_1 until it receives the second packet fragment pkt_2 in the next service frame. Only at that time it can reassemble these two packet fragments into the original packet pkt and send it to the upper-layer application. From this observation, one can formulate the delay experienced by a packet pkt using equation 5.1.

$$Delay(pkt) = DIFS + T_{Backoff} + TCF + ETT_{pkt\_1} + ETT_{pkt\_2} \tag{5.1}$$

where ETTpkt_x denotes the ETT values of pkt_1 and pkt_2, respectively, TBackoff denotes the backoff time and DIFS DCF Interframe Space, TCF denotes the time duration of a control frame currently the standard suggests that it is set to 50 milliseconds. We propose the E-ETT scheme to utilize the residual bandwidth of service frames and decrease the delays experienced by an applications packets.

5.2.2 E-ETT Performance Evaluation

In this subsection, we use the NS-2.35 network simulator to evaluate the TCP performances of our proposed E-ETT scheme and the original scheme defined in the IEEE 802.11(p)/1609 standards. Our simulation results analyze several important TCP performances parameters under various network configurations [91]. The important parameters used in our simulations are presented in Table 5.1, TCL scripts are given in Table 5.2, 5.3 and Table 5.4.

Simulated time	**100s**
Data rate of each nodes MAC layer	2 Mbit/s
Max transmission range of each node	500m
TCF	50ms
DIFS	50ms

Table 5.1: Simulations parameters

```
set opt(chan) Channel / WirelessChannel ; # channel type
set opt(prop) Propagation / TwoRayGround ;
# radiopropagation model
set opt(netif) Phy/WirelessPhyExt; # network interface type
set opt(mac) Mac/802_11Ext ;# MAC type
set opt(ifq) Queue/DropTail/PriQueue;# interface queue type
set opt(ll) LL ;# link layer type
set opt(ant) Antenna/OmniAntenna
set opt(ifqlen) 50 ;# max packet in ifq
set opt(nn) 2 ;# number ofmobilenodes
set opt(adhocRouting) DSDV ;# routing protocol
set opt(sc) "cbr1" ; # node movement file.
set opt(x) 1500 ;# x coordinate of topology
set opt(y) 1500 ;# y coordinate of topology
set opt(seed) 0.0 ;# seed for random number gen
set opt(stop) 250 ;# time to stop simulation
```

Table 5.2: IEEE 802.11p Parameters in TCL file

```
Mac/802_11Ext set CWMin_15
Mac/802_11Ext set CWMax_1023
Mac/802_11Ext set SlotTime_0.000013
Mac/802_11Ext set DIFS_0.000050
Mac/802_11Ext set ShortRetryLimit_7
Mac/802_11Ext set LongRetryLimit_4
Mac/802_11Ext set HeaderDuration_0.000040
Mac/802_11Ext set SymbolDuration_0.000008
Mac/802_11Ext set BasicModulationScheme_0
Mac/802_11Ext set use_802_11a_flag_true
Mac/802_11Ext set RTSThreshold_2346
Mac/802_11Ext set MAC_DBG 0
```

Table 5.3: MAC layer Parameters in TCL file

The first simulated topology is a network composed of only two nodes; each one is equipped with an IEEE 802.11p radio. The distance between them is set to 200 meters, which is less than the maximum transmission range. We consider in our simulations a TCP flow that sends its data only in one direction on the TCP connection. The source node of the TCP flow continuously transmits large TCP data packets of the same size to the other node.

The size of these large data packets is the Maximum Transmission Unit of the network interface and is normally 1500 bytes. On the other hand, under the control of the TCP congestion and error control protocols, the other node continuously transmits small (50 bytes) TCP ACK packets back to the source node when TCP data packets are received. Figure 5.5 shows that our algorithm improves TCP throughput compared to standard base 802.11p.

Phy/4WirelessPhyExt set CSThresh_3.9810717055349694e-13
Phy/WirelessPhyExt set Pt_5.0e-2
Phy/WirelessPhyExt set freq_5.9e+9
Phy/WirelessPhyExt set noise_floor_1.26e-13
Phy/WirelessPhyExt set L_1.0
Phy/WirelessPhyExt set PowerMonitorThresh_3.981071705534985e-18
Phy/WirelessPhyExt set HeaderDuration_0.000040
Phy/WirelessPhyExt set BasicModulationScheme_0
Phy/WirelessPhyExt set PreambleCaptureSwitch_1
Phy/WirelessPhyExt set DataCaptureSwitch_1
Phy/WirelessPhyExt set SINR_PreambleCapture_3.1623
Phy/WirelessPhyExt set SINR_DataCapture_10.0
Phy/WirelessPhyExt set trace_dist_1e6
Phy/WirelessPhyExt set PHY_DBG_0
Phy/WirelessPhyExt set CSThresh_3.9810717055349694e-13
Phy/WirelessPhyExt set Pt_5.0e-2
Phy/WirelessPhyExt set freq_5.9e+9
Phy/WirelessPhyExt set noise_floor_1.26e-13
Phy/WirelessPhyExt set L_1.0
Phy/WirelessPhyExt set PowerMonitorThresh_ 3.981071705534985e-18
Phy/WirelessPhyExt set HeaderDuration_0.000040
Phy/WirelessPhyExt set BasicModulationScheme_0
Phy/WirelessPhyExt set PreambleCaptureSwitch_1
Phy/WirelessPhyExt set DataCaptureSwitch_1
Phy/WirelessPhyExt set SINR_PreambleCapture_3.1623
Phy/WirelessPhyExt set SINR_DataCapture_10.0
Phy/WirelessPhyExt set trace_dist_1e6
Phy/WirelessPhyExt set PHY_DBG_0

Table 5.4: Physical layer Parameters in TCL file

In the second scenario, both nodes are competing for the wireless link. The packets transmitted in service frames consist of TCP data and TCP ACK. Figure 5.6 shows that in this case also our E-ETT performs better than the basic IEEE 802.11p.

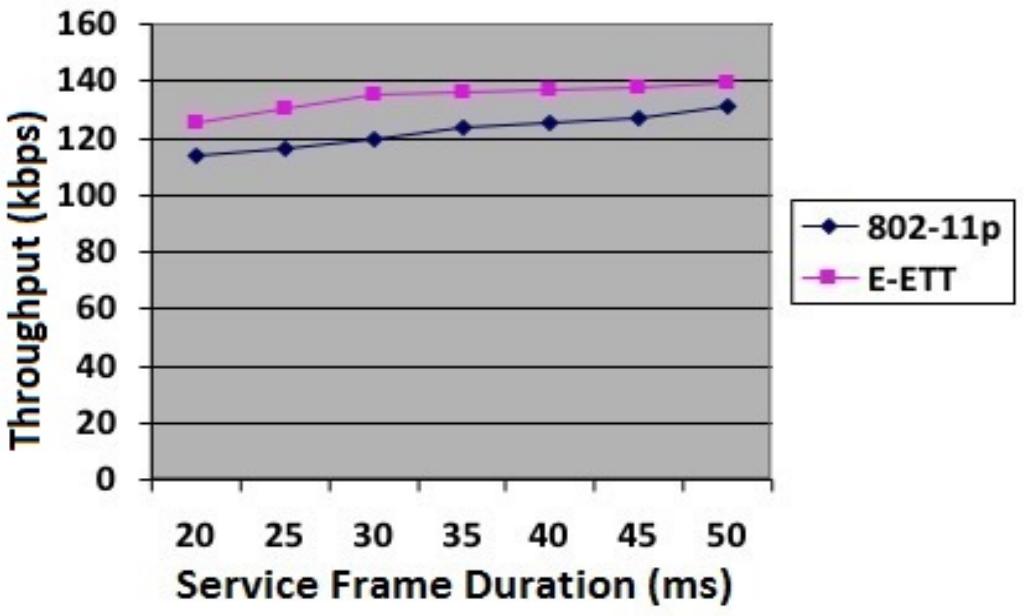

Figure 5.5: TCP throughputs over different frame durations.

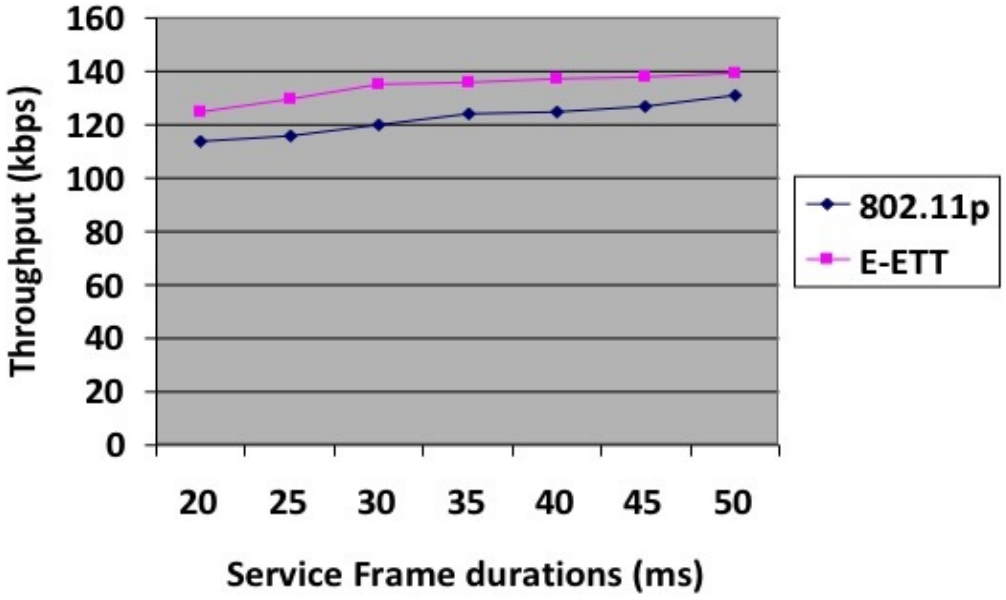

Figure 5.6: Aggregate TCP throughput over different frame durations.

The last scenario consists on multiple TCP unidirectional TCP flows with 30-ms frame. Figure 5.7 shows that our scheme continues to provide more throughput than IEEE 802.11p. One new event is that as the number of competing flows (nodes) increases, the total throughput decreases. This can be explained by the property of the CSMA/CA protocol, which IEEE 802.11 p uses.

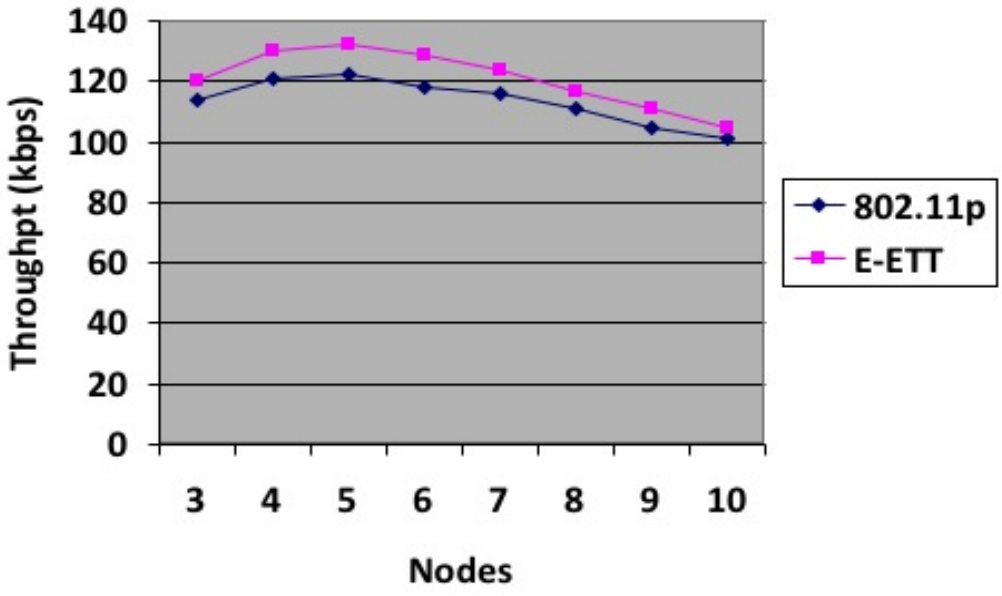

Figure 5.7: Aggregate TCP throughput for multiple nodes.

5.2.3 Security cost for WAVE

A WAVE network needs many security services. Authentication is very important in the deployment of secure VANETs. The IEEE 1609.2 standard specifies that authentication must be provided by a digital signature mechanism: the protocol ECDSA (Elliptic Curve Digital Signature Algorithm).

The introduction of authentication imposes an extra cost:

- **Temporal:** Calculation time (digital signature, certificate, hash, etc.).
- **Communication Load:** the signed or encrypted messages are larger than the unsecured messages. Each security mechanism causes a message exchange (certificate verification, CRL retrieval, sending the private key, etc.).
- **Financial:** the equipment dedicated to security adds a financial cost to the production of each DSRC unit.

That is why we need to analyse analytically and by simulation the impact of ECDSA on the performance of the basic IEEE 802.11p and the performance of our E-ETT scheme. We consider the same scenarios used in the previous section. With the introduction of authentication, the delay will be given by equation 5.2:

$$Delay(pkt) = T_{ath} + T_{Backoff} + DIFS + TCF + ETT_{pkt\_1} + ETT_{pkt\_2} \quad (5.2)$$

where ETTpkt_x denote the ETT values of pkt_1 and pkt_2, respectively, T_{ath} denotes the authentication duration, TBackoff denotes the backoff time, DIFS denote DCF Inter-frame Space and TCF denotes the time duration of a control frame (currently the standard suggests that it is set to 50 milliseconds).

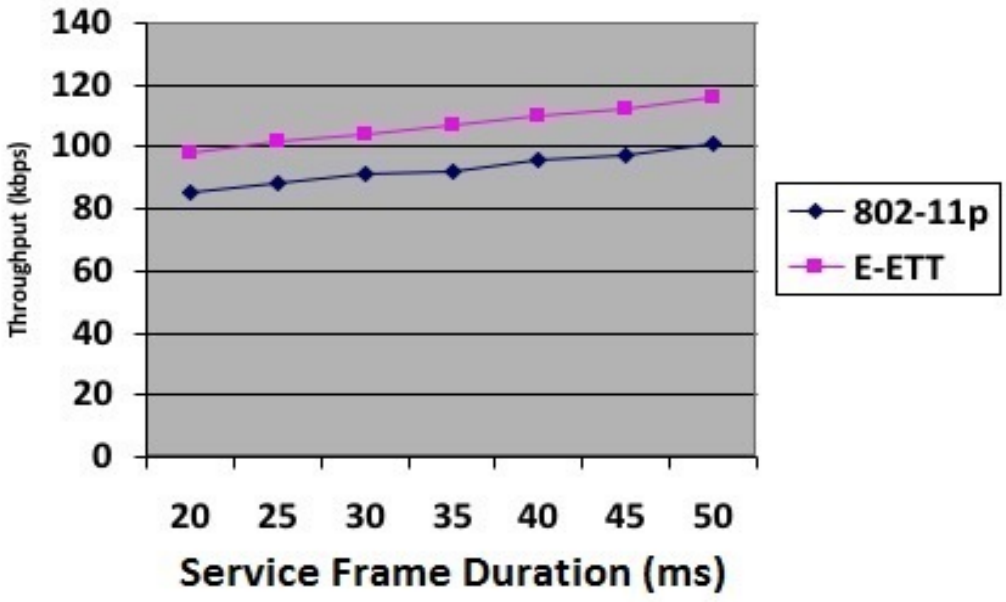

Figure 5.8: TCP throughputs over different frame durations with authentication.

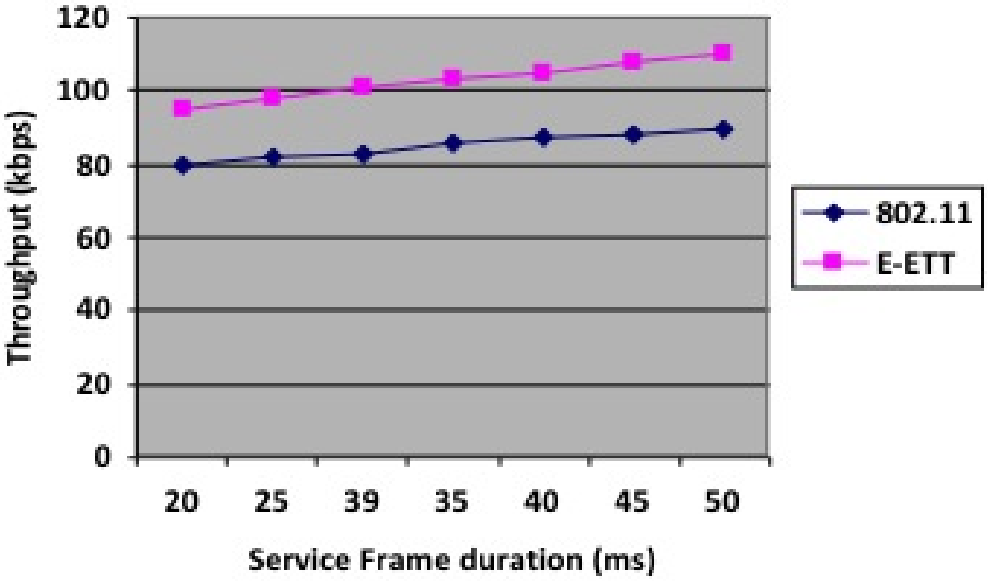

Figure 5.9: Aggregate TCP throughputs over different frame durations.

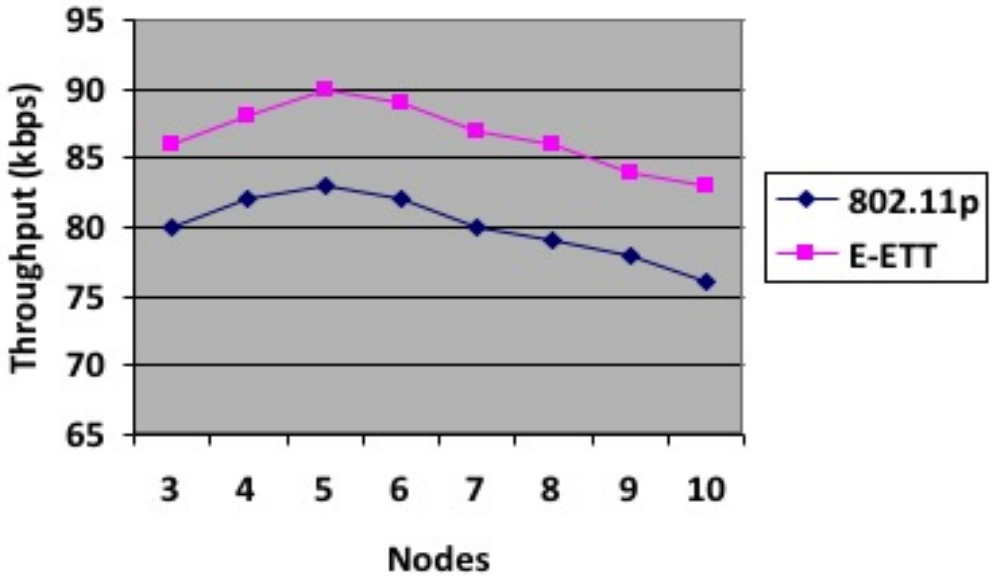

Figure 5.10: Aggregate TCP throughputs for multiple nodes.

Figures (5.8, 5.9 and 5.10) show that our E-ETT continues to perform better than the basic IEEE 802.11p and the authentication has an extra cost which is manifested as a reduction in throughputs in comparison to the results obtained without authentication.

5.3 Conclusion

In this chapter, we evaluated the performance of TCP over IEEE 802.11p/1609.x with various networks configurations. We considered the bandwidth wastage problem caused by channel switching in the standards IEEE 802.11p m/1609.x. To overcome this problem, we proposed a scheme that we called E-ETT and we showed that our scheme has better performance then the scheme used by IEEE802.11p. We also introduced security to study the additional cost and the impact on the performances. Overall, our scheme improves the performance by about 5% in the presence or not of the security aspect.

Part VI

NEtwork MObility (NEMO)

"Design and implementation of a secure nemo. International Journal of Computer Science and Information Security, ISSN 1947-5500, 2012. Published"

CHAPTER 6

A Deploy ability Analysis of NEMO in VANETs and Application

6.1 NEtwork MObility (NEMO)

As IPv4 can not meet the demand anymore, the IPv6 protocol [37] has been standardized in 1998. It can allocate much more addresses and allows interconnecting decillions of nodes at the same time. Nodes that connect to the Internet can automatically acquire an address thanks to the auto-configuration mechanism (”IPv6 Stateless Address Auto-configuration”) [89]. IPv6 also simplifies the use of multicast that allows many to many (including one to many) communications without wasting the bandwidth.

Besides those core features, IPv6 also allows the integration of new features such as improved security, quality of service where IPv4 only provides best effort, and mobility mechanisms with Mobile IPv6 and NEMO Basic Support.

The scalability offered by IPv6 will thus allow to interconnect any equipment and to design new services (such as connecting each car to the Internet) and new usages of the Internet (for instance use the vehicle connectivity for monitoring purposes) that we could not imagine with IPv4.

When a node using an Internet wireless access physically moves, it can be at some point of time out of the coverage area of its access network and needs to move to another one. In addition, because distinct operators may operate or the public target is different (pedestrians, cars etc.), usually no single access technology can cover one big area (such as a city). The node thus has to select the best access technology available.

When a node moves from one access network to another or switches between its access technologies, it acquires a new IPv6 address and is not reachable via its previous one anymore. It implies that all current communications (for example streaming video from the Internet) are stopped and later restarted by the user or the application.

The Mobile IPv6 protocol [61] has been defined to address those issues and to allow the node to be always reachable at the same IPv6 address whatever the access network it uses. It allows the host to move transparently for the applications and the users, without the need to reset all the current connections each time the host moves to another access network.

With Mobile IPv6, a host has two addresses while moving in the Internet topology: one permanent address that identifies the host, and the other representing the location in the Internet topology. The Mobile IPv6 protocol takes care of the binding between these two addresses (thanks to a Home Agent), and ensures that the host is always reachable at its permanent address even if it moves in the Internet topology.

On one side Mobile IPv6 manages mobility for only one host, on the other side NEMO Basic Support [39] manages mobility for one whole network. Such a network can be for instance a PAN (Personal Area Network, a small network made of IPv6 sensors and PDAs), or an access network deployed in cars, buses or trains. Thanks to NEMO Basic Support, the only computer that needs to have mobility functionalities when the whole network moves is the one that connects the network to the Internet (this computer is called a Mobile Router), whereas with the Mobile IPv6 approach each host in the network would have to handle mobility.

Running Mobile IPv6 on each node can be expensive, especially for little devices such as sensors. NEMO Basic Support only requires changes on the router, all others hosts in the moving network do not need any new feature. Thus, all movement in the Internet topology will be handled by the router, transparently to the hosts.

With NEMO, we can imagine lots of scenarios where mobility can play an important role. Using Network Mobility in a train would allow the customers to stay connected to the Internet without disruption during their entire trip. Network Mobility in cars can allow to set up a PAN (Personal Area Network) made of tiny IPv6 sensors that can be queried from outside, and PDAs that can have permanent access to the Internet.

To allow nodes to remain reachable, even if it changes its point of attachment to Internet, Mobile IP uses a Mobile Router (MR). The MR allows local fixed and mobile nodes and even visiting nodes to still connecting to the Internet. The MR reduces transmission power needs. Nodes communicate with an MR rather than an access router on the Internet. Furthermore, the MR reduces handoffs because it handles link layer handoffs. MR reduces the bandwidth consumption and location update delays. When a network

changes its point of attachment to the Internet, all mobile and fixed nodes inundate their Home Agent (HA) with registration messages, but with the use of an MR, one registration message is sent to HA to register the whole network.

The HA is a router which delivers packets to a mobile node when it is away from its home network and maintains current location information for the mobile node. When away from its home network, a mobile node is associated a Care-of Address (CoA)that reflects its current point of attachment. This allows nodes to keep their home IP address and to receive packets sent to it by a Correspondent Node. The mechanisms of MIP make the movement of nodes being transparent to transport and higher-layer protocols and applications.

In [61], MIPv6 was defined as a protocol allowing mobile nodes to move from a link to another while keeping their home address unchangeable. The use of IPv6 routing header by MIPv6 results in reduced overhead, then improves the use of the resources of the communication medium.

However, MIPv6 is unable to support network mobility. In addition, once a device is attached to the MR on a mobile network, it may not see any link-level handoffs even as the network moves. Thus, the host mobility protocols such as MIP and MIPv6 do not get triggers indicating link-level hand-offs and, as a result, will not initiate handover. This paved the way to the development of a Mobility management mechanism which consists on Network mobility basic support. Till now, only nodes mobility is considered. However, different scenarios of entire moving networks exist (WLANs on trains, planes, ships etc.). In order to support Network Mobility (NEMO), an extension of MIPv6 was created.

NEMO Basic Support (NEMO BS) [39] is developed to cope with the before mentioned insufficiencies of MIPv6. NEMO BS is an extension of MIPv6 protocol. It allows terminals within a mobile network to globally and continuously be connected to the Internet. The NEMO BS is designed so that network mobility is transparent to the node inside the mobile network in fact, only MR and HA are aware of the network changes, since Mobile Network Nodes (MNNs) continue to be connected with MR using the same address configured using the Mobile Network Prefix (MNP).

6.2 Issues for QoS and security in NEMO-based VANET

In [87], a handover mechanism based on CoPP is proposed. The vehicle adopting this handover mechanism can acquire a unique CoP from the new BS with CoPP. The proposed solution leaves out the DAD phase, and then significantly reduces the handover delay. In order to cope with the interruption of the communication when a vehicle moves from an access point to another, a CoPP is deployed on the NAR (New Access Router). When an MR moves, it acquires a unique CoP carried by the CoPP, so the MR CoA DAD phase is omitted. The CoPP provides a unique CoP and generates the candidate CoA. The maintaining algorithm of the CoPP guarantees the uniqueness of the CoP and generates the candidate CoA, which is acquired by the MR in the vehicles. So the DAD process, can be omitted directly.

The authors in [8] have proposed a link-layer authentication and key agreement scheme. This protocol uses CL-AKA scheme to secure public hotspots in a NEMO-based VANET. When an MNN decides to connect to the OBU/MRs public hotspot, it first verifies the OBU/MRs public key using an online certificate verification web-site. Putting a threshold time, T, for the certificate verifications response, the MNN authenticates the MR if it receives the response within T. The MNN sends an authentication request to the OBU/MR that contains three parts of information which consist on its identity encrypted by OBU/MRs public key, one MNP that the MNN chooses from the MNPs found in the periodically broadcasted messages and the MNNs credentials such as payment data. The security of the proposed protocol is based on the hardness of the encryption algorithm used in this mechanism, namely the Elliptic Curve algorithm which necessitate an exponential time to be resolved. Using CL-AKA scheme only authorized users that send valid authentication requests can gain Internet access from OBU/MR. Containing valid credentials such as payment data, the authentication request message is accepted by the OBU/MR that stores the MNNs identity along with its credentials. Therefore, malicious MNNs that send invalid credentials cannot access the hotspot. CL-AKA achieves lower computation and communication over-heads, higher security levels, and lower energy consumption.

6.3 Design and Implementation of a Secure NeMo

In the near future, airplanes, automobiles, trains and even people will carry entire networks of IP devices that connect to the Internet. In July 2004 the European Space Agency (ESA) funded a project called Broadband to Trains [8] shown if 6.1 that used satellite communications as a connection service to provide internet broadband to passengers and train operators.

However, as they move, these networks must change their point of attachment to the Internet due to the availability of Internet connectivity. NEMO would enable devices on these networks to maintain unchanged (in the sense of unchanged IP address and network prefix) connections to other devices on the Internet.

Until recently, wireless devices have been prohibited on commercial airline flights due to the risk of interference with airplanes electrical systems. However, in June of 2005, the Federal Aviation Administration (FAA) gave permission to United Airlines to install Wi-Fi (802.11) wireless network equipment on some of its aircraft [9]. This new regulation will open the door for in-flight Internet service and invite NEMO as a solution to provide uninterrupted Internet connectivity to multiple passengers.

It is not difficult to imagine networked systems, or even Internet-enabled navigation, multimedia, or driving systems on automobiles. NEMO has the potential to provide a single, shared Internet access point to these systems. In the case of critical driving systems, NEMO would be essential in order to maintain continuous connectivity and availability [42].

6.3.1 System Architecture

The system architecture is based on two-way Ku-band satellite transmission to provide connectivity between the internet backbone and a master server on the train. Direct reception of satellite television channels on the same satellite is also possible but has not been tried in this project.

A hub earth station provides the connection from the Internet backbone (and from the network operations center) via the satellite directly to a low-profile tracking antenna on the train. GPRS and Wi-Fi access between the train and available networks are also provided (e.g. in stations and in tunnels). On the train, Wi-Fi (wireless LAN) connections are used between the master server and customers with Wi-Fi enabled laptops and PDAs shown in 6.1 and 6.2.

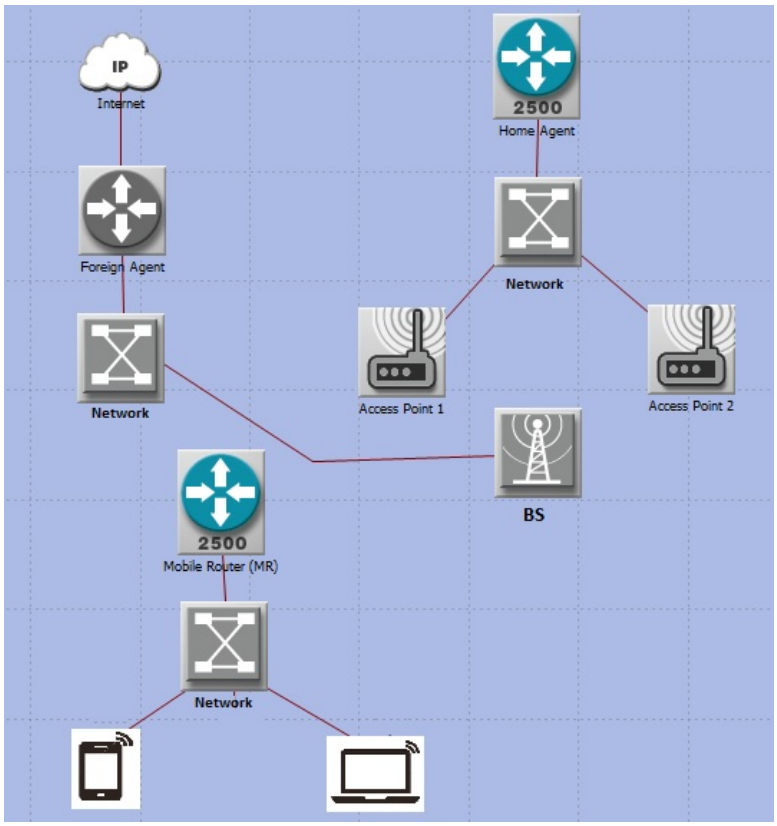

Figure 6.1: System view.

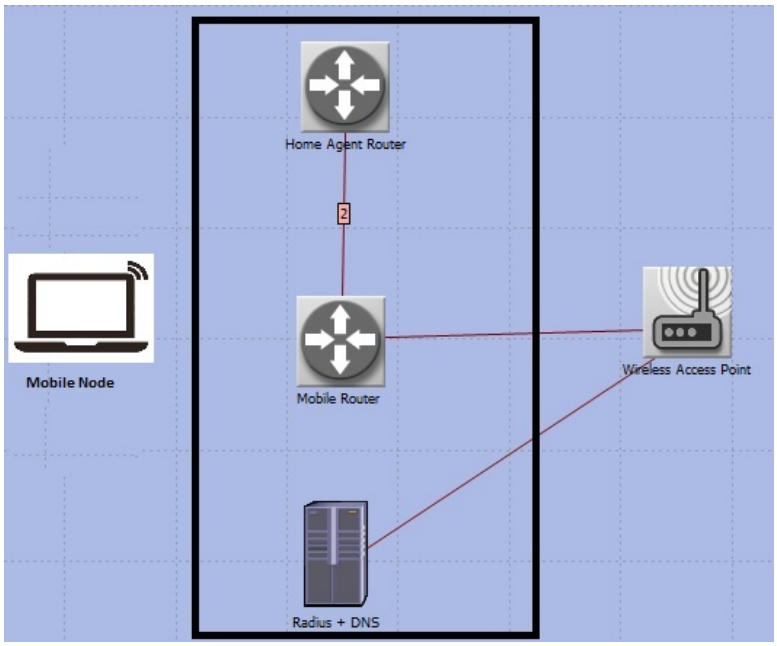

Figure 6.2: System Architecture.

6.3.2 Experimental Setup

For implementation, we used the above architecture. It consists of a quad-core server that runs the home agent, mobile router, and radius server. There is also an access point router

and a mobile node. There are two links between HA and MR. The access point connects to MR and radius server.

Now, we will cover the configuration of the MR. Table 6.1 shows modified a UMIP Mobile Router configuration. Changes made in the file are marked with NEMO ADDITION.

```
# Sample UMIP configuration file for a Mobile Router
NodeConfig MN;
# Set DebugLevel to 0 if you do not want debug messages
DebugLevel 10;
# Enable the optimistic handovers
OptimisticHandoff enabled;
# Disable RO with other MNs (it is not compatible
# with IPsec Tunnel Payload)
DoRouteOptimizationMN disabled;
# The Binding Lifetime (in sec.)
MnMaxHaBindingLife 60;
# Use NEMO Explicit Mode
MobRtrUseExplicitMode enabled; ## NEMO ADDITION ##
# List here the interfaces that you will use
# on your mobile node. The available one with
# the smallest preference number will be used.
Interface ”eth0” {
MnIfPreference 1;
}
Interface ”wlan0” {
MnIfPreference 2;
}
# Replace eth0 with one of your interface used on
# your mobile node
MnHomeLink ”eth0” {
IsMobRtr enabled; ## NEMO ADDITION ##
HomeAgentAddress 2001:db8:ffff:0::1000;
HomeAddress 2001:db8:ffff:0::1/64
(2001:db8:ffff:ff01::/64); ## NEMO ADDITION ##
}
# Enable IPsec static keying UseMnHaIPsec enabled; KeyMngMobCa-
pability disabled;
# IPsec Security Policies information
IPsecPolicySet {
HomeAgentAddress 2001:db8:ffff:0::1000;
HomeAddress 2001:db8:ffff:0::1/64 ;
IPsecPolicyMhUseESP 10;
IPsecPolicyTunnelPayloadUseESP 11;
}
```

Table 6.1: UMIP configuration

We enable the NEMO explicit registration mode with the MobRtr Use Explicit Mode parameter. Note that this is not mandatory as this is enabled by default.

All the other changes take place in the Mn Home Link block. We allow the MR to act as a router by enabling the Is MobRtr parameter. The prefix that we previously configured on the NEMO HA side has been added to the Home Address statement. No changes are needed in the IPsec configuration. All the traffic from the mobile network will also automatically be protected with IPsec tunnel mode.

The IPsec SAs needed on the MN are the same as the one installed on the HA for that MN. You can then use the same IPsec SAs as the one we described in the HA section, and copy them on the MN in the /usr/local/etc/setkey.conf file. The MR needs to advertise its MNP in the mobile network using Router Advertisements (RA). For that purpose, we use the radvd software with the configuration shown in table 6.2.

```
# Mobile Router radvd configuration file
# Replace eth1 with your ingress interface name
interface eth1
{
AdvSendAdvert on;
MaxRtrAdvInterval 3;
MinRtrAdvInterval 1;
AdvIntervalOpt on;
IgnoreIfMissing on;
# Mobile Router address on the ingress interface
prefix 2001:db8:ffff:ff01::1/64

AdvRouterAddr on;
AdvOnLink on;
AdvAutonomous on;
AdvPreferredLifetime 60;
AdvValidLifetime 120;
 ;
};
```

Table 6.2: radvd software configuration

For wireless security measures, we deployed the Wired Equipment Privacy (WEP) method. Then it is showed that this method can be easily cracked using the BackTrack 5 operating system [10] and the airecrack-ng [11] application. To solve the security problem, a Wi-Fi

Protected Access II (WPA2) Enterprise method is implemented using a Windows Server 2008 R2 with Network Policy Services (NPS) as a radius server and a simple router as a radius client.

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark. To setup the radius server on windows server 2008 r2, we configured the following services:

- Access Points
- Active Directory Domain Services
- DNS
- Network Policy and Access Services
- Active Directory Certificate Services

To test the implementation, we used a video streaming from HA to Mobile Node. During the stream, we disconnect one of the links between HA and MR, and the stream did not interrupt.

6.4 V-Learning: VANETs for Social and Mobile Learning

In this section, we present V-Learning, a system based on a VANET platform that permits to have access to learning to populations who often travel on roads.

Mobile learning supports learning processes through Information and Communication Technologies (ICT), and by virtue of the extended context provided by mobility it can be understood as a specialization of e-learning, even if the end devices have different technical features from static, cabled PCs. Their independence from power sources and their permanent network connections make the devices immediately available when needed in

the situational context or within the learning process.

Social learning is also a tried-and-tested form of learning in the pedagogical sense. It implicitly depends on the emergence of (learning) communities and on working within these. In relation to new technologies, social learning means learning in social structures and networks via the Internet. The online components are complementary to traditional off-line learning.

Social media are based on Web 2.0 technologies and are comprised of social networks on online platforms. Examples of these social networks are the business community platform Xing, LinkedIn, Foursquare and, currently the largest social network, Facebook, while the video platform YouTube also belongs to this category. Users establish personal profiles on these social networks, make contact with others, form interest groups and share ideas and opinions. They also create media content of all kinds, known as user-generated content and post this on the Internet which makes it accessible worldwide. The most characteristic features of social media are participation and collaboration.

Mobile learning and social learning, in particular, facilitate learning within the work process and cooperative interaction between learners who are often dispersed across locations. Informal learning and the need for cooperation and collaboration in companies and workplaces are increasing.

These forms of learning continue to advance in step with the new technologies [67, 49]. It is becoming easier and easier to access knowledge and information on the Internet. New mobile phone standards like VANETS and NEMO will bring significantly higher download rates. Ubiquitous learning will replace learning tied to one location.

As we saw in chapter 3, VANETs have individual characteristics that are decisive in the design of the communication system. These include: dynamic topology, large scale network, high computational capability, unpredictable mobility, infinite energy supply in order to provide real-time message dissemination platform to share data between vehicles and guarantee the reliable exchange of information.

Infinite energy supply: vehicles in VANETs are not energy constrained. The vehicle can provide energy to the OBU continuously via the battery.

Rapid changes in the network topology: due to the high speed of vehicles, the topology of the network is very dynamic. VANETs will not have constant connectivity because of the high-speed movement between vehicles. In low-density vehicles, the link is highly likely

to be disconnected.

Predictable mobility: unlike MANET where nodes move in a random way, VANET topology is not absolutely random. VANET movement restrictions are defined by road layout, topology, traffic rules, and the reaction to messages sent by other vehicles.

High computational capability: Because the nodes in VANET are vehicles, they can be equipped with a sufficient number of sensors and computational resources; such as processors, a large memory capacity, advanced antenna technology and Global Position System (GPS).

Till now, only nodes mobility is considered. However, different scenarios of entire moving networks exist. In order to support NEMO, an extension of MIPv6 was realized.

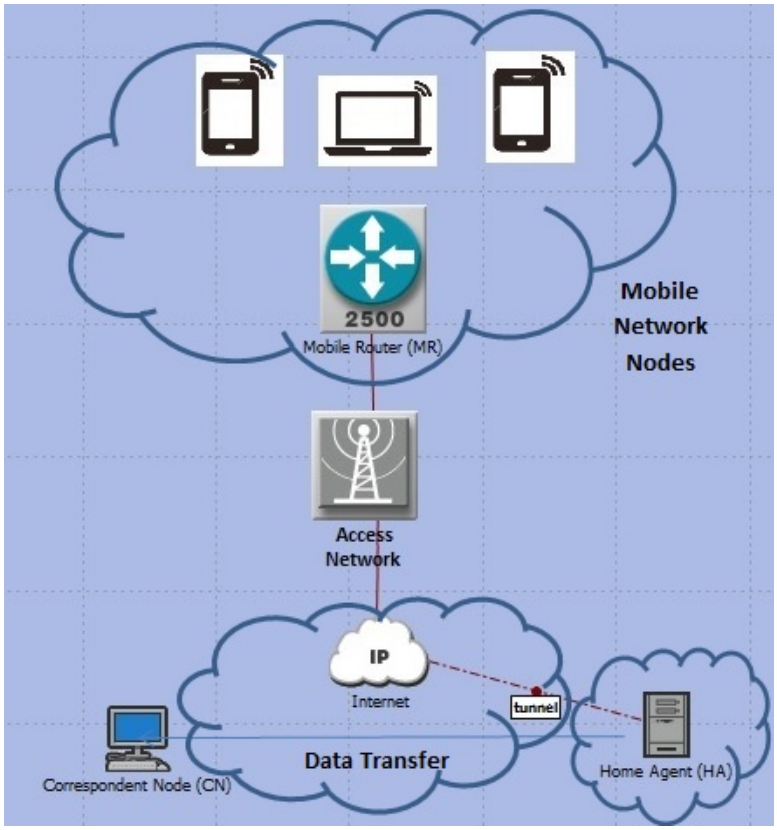

Figure 6.3: Nested NEMO.

NEMO BS is an extension of MIPv6 protocol. It allows terminals within a mobile network to globally and continuously be connected to the Internet. The NEMO BS is designed, see Figure 6.3, so that network mobility is transparent to the node inside the mobile network, only mobile router MR and HA are aware of the network changes, since MNNs continue to be connected with MR using the same address configured using the MNP.

A particular approach of this type, on which recent research has been focusing, is the use of nested NEMO [41].

A precondition for a nested NEMO is that the Mobile Router of the sub-NEMO can attach itself, directly or indirectly to the ingress interface of the Mobile Router of the parent NEMO.

Definition : We define as VANET-NEMO a solution to apply NEMO in VANETs, in which multi-hop communication between VANET nodes and an infrastructure is achieved passing through at least one NEMO Mobile Router running on a different node.

Our architecture has been designed to allow populations who often travel on roads, to have access to learning for educational purposes. Figure 6.4. outlines the basic setup of our V-learning platform. The box labeled HA refers to the home network with the knowledge servers. The boxes labeled AP1 and AP 2 are the access technologies like Long Term Evolution (LTE). Learners are on board vehicles. MR box is configured as NEMO mobile router to provide network connectivity. Instead of each learner using equipment with internet connection, 3G, for example, they all share the connection to the same router that provides an access to the knowledge servers.

We have examined the power consumption of the learners device. We conducted experiments to study the impact of the transport layer protocols TCP and UDP on to consumption of energy of the learner Smartphone. Based on our results, see Figure 6.5, we show that a TCP connection consumes a larger amount of power over time compared to UDP.

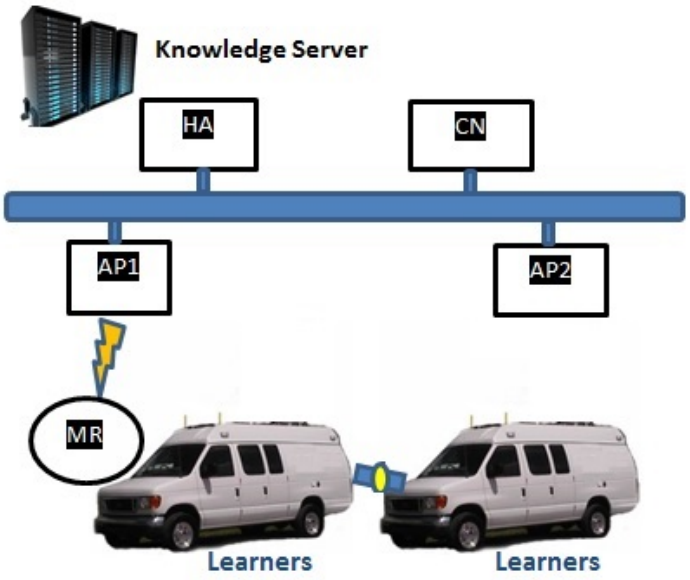

Figure 6.4: V-learning Platform.

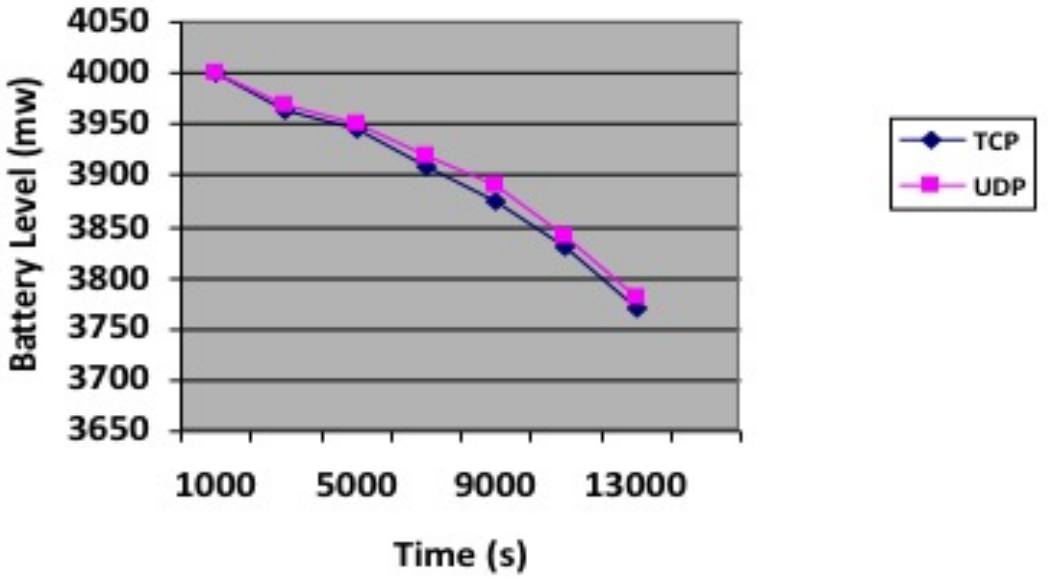

Figure 6.5: The difference in power consumed between TCP and UDP.

For the second experiments, we compare the power consumption of the learner Smartphone having access to knowledge servers with his own 3G connection and the learner Smartphone having access with VANET-NEMO router. The results show, see Figure 6.6, that there is a gain on the battery life using VANET-NEMO with compared to the use of 3G.

Social and Mobile learning made learners more willing to participate and allowed

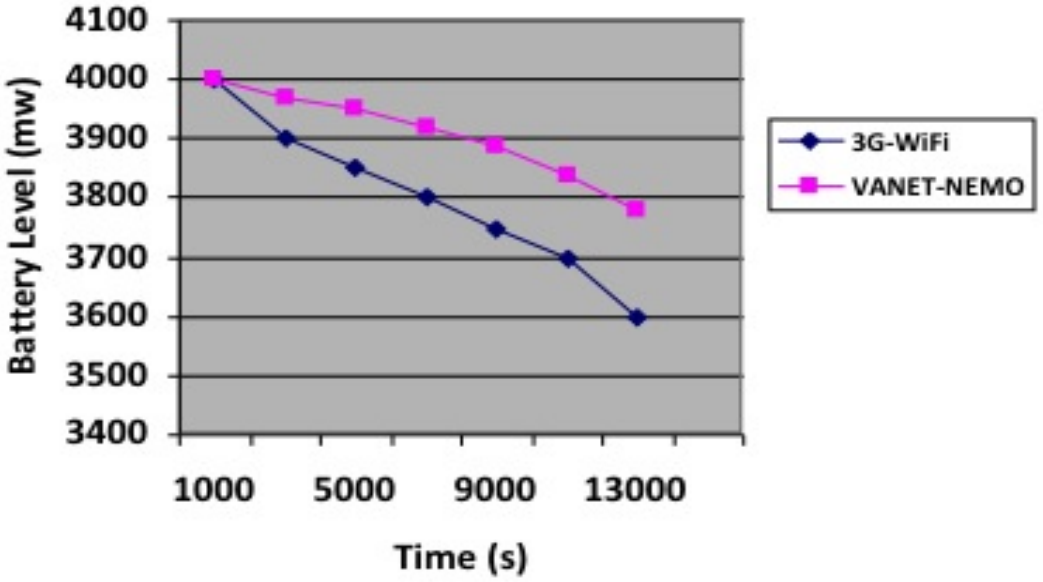

Figure 6.6: The difference in power consumed between 3G-WiFi and VANET-NEMO.

them to express themselves more freely. Our V-learning approach allows the immediate access to relevant resources and information helped them advance their understanding on the subject. Our results should not be taken as absolute values in themselves but should be considered relatively. Based on our results, learners can have more time access to resources using VANET-NEMO than a 3G connection.

6.5 Conclusion

In this chapter, we have presented an approach based on a VANET environment that appeals to NEMO to improve the quality of access and ensure a level of security. The results obtained on the basis of implementations and experimentation show that the proposed approach opens the door to several uses and applications of this VANET NEMO-access platform. We operate the V-learning application in the field of learning. This approach allows communities, who had difficulty to access to learning, to join the world of teaching and education in good conditions.

Part VII

Conclusion and Perspectives

CHAPTER 7

Conclusion and perspectives

7.1 Conclusion

Nowadays, the need of users to access the Internet anywhere at any time is increasingly becoming a necessity. The exponential increase in mobile data traffic has led to the massive deployment of wireless systems. Future technologies are mobile and wireless with a high level of security and quality of service.

To prepare the future, we considered VANETs as a good example for future technologies and we proposed several study and experiments to improve the quality of service and security for VANETs. Unlike other wireless environments that are mostly stationary or with low mobility, data transmission in VANETs poses more challenges that must be addressed. Since the topology is constantly changing, vehicles could move away from their home network and cause connectivity breakage. In order to cope with this problem, a vehicle connected to the wireless network should be able to move using different access points available along the road. These access points could belong to different networks or wireless technologies like Wi-Fi, WiMAX, 3G, LTE.

We started our research from the origin of VANETs which are MANETs. We have contributed to improving the quality of service by proposing a new algorithm at the MAC layer. Our second contribution has focused on the study and improvement of the standard IEEE 802.11p performance. Then, we proposed an approach based on the use of NEMO in VANETs environment to improve performance in terms of QoS and security. We also gave an example of an application in the area of social and mobile learning.

We believe that a PhD thesis is interesting only if it meets and solves some problems and opens the track to other issues and problematics. In this PhD thesis, we improved some QoS and security aspects, but we think that the performance with the traditional RF technologies is still not good enough. In that perspective, we will now briefly introduce a future technology, Light Fidelity (Li-Fi), that we think can improve the performance of

future mobile technologies like VANETs. Li-Fi wireless network would complement existing heterogeneous RF wireless networks, and would provide significant spectrum relief by allowing cellular and Wireless Fidelity (Wi-Fi) systems to offload a significant portion of wireless data traffic.

7.2 Perspectives

The idea to transmit the information trough light is not new, for already in the 1880 Alexander Graham Bell had developed the Photophone. Our attention will be focused on the use of Visible Lighting Communications (VLC) Li-Fi and how it can provide a valid technology for communication purposes in VANETs and others future mobile technologies. Unlike RF modulation methods, VLC adopts the intensity modulation to carry binary data by turning LED on and off quickly. The LED can turn on and off multiple times, and thus transmit binary information. This LED variation is invisible to the eye, but it is received by a sensor which is capable of receiving and transforming the received information. Potentially, the number of ignition timing on/off of the LED can be very large, up to 1 billion times per second currently, which represents a theoretical speed of 1.3 Gbit/s [81].

During the last ten years, there have been continuous reports of improved point-to-point link data rates using off-the-shelf white LEDs under experimental lab conditions. Recently, data rates in excess of 1Gbps has been reported using off-the-shelf phosphor-coated white LEDs, and 3.4 Gbps has been demonstrated with an off-the-shelf Red-Green-Blue (RGB) LED. To the best of the authorś knowledge, the highest speed that has ever been reported from a single color incoherent LED is 3.5 Gbps. The experiment was led by researchers of the University of Edinburgh.VLC and the Li-Fi Consortium was formed in Oslo, Norway in 2011 with the purpose of providing a high speed and wireless optical network [12, 13].The vision is that a Li-Fi wireless network would complement existing heterogeneous RF wireless networks, and would provide significant spectrum relief by allowing cellular and Wi-Fi systems to off-load a significant portion of wireless data traffic. The Li-Fi technology has several advantages:

- The flow can be important.
- A light source is simple to implement.
- In contrast to electromagnetic waves, light waves do not pass through the human body, and, therefore, are not likely to cause health problems.
- It is directional, so the information can only be received in the path of the light wave, we can think that it can be more secure than RF technologies.

- This prevents saturation of RF networks in the future by proposing a new distribution of digital information channel.

The number of possible applications of VANETs is expanding. In addition to safety applications, vehicles are foreseen to support entertainment applications such as peer-to-peer applications and Internet connectivity applications. For all this, most mobile data traffic is consumed. Li-Fi offers many key advantages and effective solutions.

Figure 7.1: Li-Fi for V2V communications.

The use of Li-Fi represents a viable alternative that can achieve high data rates while also providing illumination. This configuration minimizes packet collisions due to Line Of Sight (LOS) property of light and promises to alleviate the wireless bottleneck that exists when there is a high density of rich-media devices seeking to receive data from the wired network.

The cooperative techniques and protocols between Li-Fi and the existing RF networks need further study. RF networks are widely used and gradually became indispensable in our lives. Integrating Li-Fi into RF communications will not only accelerate the marketization of Li-Fi, but it will also offload traffic from the extremely crowded cellular networks. However, a large number of feedback packets and considerable delay may exist when performing handover between Li-Fi and RF network, and that need to be investigated.

APPENDIX A

Networks Simulator NS

A.1 Introduction

There are many network simulation tools available to evaluate the performance of the proposed mechanisms and protocols for simulating both the wireless and wired networks. NS-2 (Network Simulator 2) [14], is probably the most used by the networks community. It was the result of collaboration between UC Berkeley, USC (University of Southern California) and Xerox PARC as part of the VINT project (Virtual Inter Network Testbed) [5]. This project is supported by DARPA (Defence Advanced Research Projects Agency). Other programs which have been used include Global Mobile Information System Simulation Library (GloMoSim), OPNET Modeler, QualNet, MATLAB, and CSIM.

The free source feature in NS-2 increasingly encourages the research community to use it as a potential simulation tool. NS-2 is a very useful tool for designing and understanding of networks behaviour. NS-2 allows the user to set a network and simulate communication between nodes. Simulation of wired, as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP), can be done using NS2 [57].

The simulator NS2 uses the object-oriented language Objective Tool Command Language (OTCL) derived from TCL Tool Command Language for describing simulation conditions in script form. In the script, the user provides topology network, the characteristics of the physical links, protocols, the type of traffic generated by sources, events, etc.

The script is written in Otcl but the routines are written in C ++ for they have greater power calculations. The result of a simulation is a text file (.tr of extension) containing all files events of the simulation. Subsequent treatment of this file makes it possible to subtract the desired information.

Furthermore, the simulator allows the creation of an animation file (.nam of extension) to visualize the simulation GUI NAM. This Visualization provides a representation of the

network graph on which we can see packets circulate, monitor the level of queues and observe the flow of current links.

In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. NS2 is a discrete event simulator that targets networking research and provides substantial support for simulation of the various aspects of a modern communications network, Like packet routing, unicast and multicast, packet delivery, etc.

Since most of the research in ad hoc networks has been implemented using Network Simulator (NS-2), and its the case of this thesis also, this annex provides a general overview of NS-2, and describes its structure, and illustrates how we used the NS-2 in this work. The Network Simulator (NS-2) is a real network environment simulator, and an open source discrete event and object-oriented simulator intended mainly for networking research. NS-2 now is considered as a reliable simulation tool for computer communication networks both in academia and industry. It was developed by the University of California at Berkeley, University of Southern Californias Information Sciences Institute (USC/ISI), Lawrence Berkeley National Laboratory (LBNL) and Xerox Palo Alto Research Center (PARC) under the VINT (Virtual InterNetwork Testbed) project [43]. Its main sponsors are the Defence Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF).

There are several versions of NS-2, the latest one is termed NS-3.12, it was released on 31 August 2011 [14]. This release is mainly a maintenance release but contains a few new features, and many bugs fixed. In our work, however, we used version NS-2.35 Allinone.

A.2 NS2 Architecture

Ns-2 is a discrete event simulator. One of the most important parts is the scheduler as it schedules the events and calls the appropriate event handler methods when they occur. In NS2, there are five schedules available in the simulator, each of which is implemented by using a different data structure: a simple linked-list, heap, calendar queue (default) and a special type called ”real-time”. The scheduler runs by selecting the next earliest event, executing it to completion, and returning to execute the next event.

The units of time used by the scheduler are seconds [43]. An event is handled by calling the appropriate Handler class. The most important Handler is NsObject (Network Simulator Object). TclObject and NsObject provide all the basic functions allowing objects to interact one with another. NsObject is the parent class for some important classes as the

Classifier, the Connector and the TraceFile class:

- TclObject: This is the root of all the other classes in both the compiled and tree interpreted. The TclObject class is therefore the base class for most other classes. All objects in the simulation model are instances of the class TclObject. this class serves to objects whose creation was initiated by the interpreter. It has the necessary interfaces the links between the variables that must be visible in both C ++ and otcl. It defines command () function that is very useful to add commands to the interpreter. the class TclObject and other sources of tclcl directory is shared between NS-2 and the project MASH Berkeley. In the hierarchy of otcl classes, the name of the root class is called otherwise and is named SplitObject.

- NSObject: it is a subclass of class TclObject but remains a superclass to other classes. The main difference with the TclObject class is that it is able receiving packets and process events. It inherits the Handler class. This class is the main root objects in NS-2. It contains functions necessary common simulator and defines the virtual function: void recv (Packet * Handler callback * = 0) = 0; This function is a generic function used by all objects derived from NSObject to receive a packet. It is actually defined by the subclasses:

- Application: mother of all Class applications (ftp, telnet, Web)

- Agent: the agent class provides methods useful for the development of the layer transportation and other signaling protocols or management plan. This is the base class to define new protocols in NS-2. It provides local and destination address, the functions to generate the packet, the interface to the Application class. Currently NS-2, there are many agents include: UDP routing protocols, different versions of TCP, RTP, etc.

- Node: a node can be a machine, a switch, a router, a gateway, etc. Each node contains at least the following components:
  1. An address or identifier (id_) automatically incremented by one unit (from 0) when the nodes are created.
  2. A list of neighbor nodes (neighbor_).
  3. A list of agents (agent_).
  4. An identifier of the node type (nodetype_).
  5. A routing module.

- Tail: the superclass of all buffers (DropTail, RED)

- LinkDelay: This class simulates the propagation delay and transmission time on the links network. With the Queue class, this class simulates the layer 1 and 2 of the Internet. Packet: the class of all packets on the network.

- TimerHundler: superclass of all timers (timers) used by the protocols of network.

Figure A.1 explains the NS2 basic architecture.

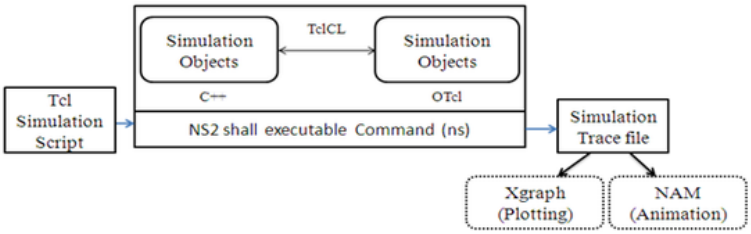

Figure A.1: NS2 Basic architecture. [1]

The NS2 all-in-one package is used for installation to reduce the complexity during installation. All the necessary packages are archived in the ns-allinone-2.x.tar.gz, where x is for the version. For the simulation purposes, we have used ns-allinone-2.35.tar.gz . If any other packages or patches need to be used then, they should be downloaded separately or written by the user.

There are three steps in the NS2 simulation. The first step in simulating a network is to design the simulation. In this step, the users should determine the simulation purposes, network configuration and assumptions, the performance measures, and the type of expected results. The second step is to configure and run the simulation. It consists of two phases:

1. **Network configuration phase:** In this phase network components (e.g., node, TCP and UDP) are created and configured according to the simulation design. Also, the events such as data transfer are scheduled to start at a certain time.

2. **Simulation Phase:** This phase starts the simulation which was configured in the network configuration Phase. This phase usually runs until the simulation clock reached a threshold value specified in the network configuration Phase.

The last step is the post-simulation processing. The main tasks in this step include verifying the integrity of the program and evaluating the performance of the simulated network. While the first task is referred to as debugging, the second one is compiling simulation results.

A.3 Simulation

A.3.1 Tcl script

In this section, we will introduce TCL and the used simulation script. However, we will discuss the most basic features of a generic simulation script rather than the one use in the simulation carried out as a part of the thesis. This information has been taken from the TCL/tk documentation which can be downloaded for free at `http://www.TCL.tk/doc/`. A detailed TCL simulation script used for simulation can be found in [57], [24].

The TCL simulation script is used for configuring and parameterizing (manipulating) a simulation in NS2. TCL is a mixture of:

- LISP/Scheme (mainly for its tail recursion capabilities)
- C (control structures, expr syntax)
- UNIX shells (with better structuring)

The TCL simulation script is a sequence of commands separated by newlines or semi-colons. All commands are strings which is a list of words separated by a space. Word is a string that begins and ends with the braces ().Arithmetic and logical expressions are not part of the TCL language itself, but the language of the expr command (also used in some arguments of the, if, for, and while commands) is basically equivalent to C's expressions, with infix operators and functions. Here are some basic syntax rules in TCL.

- Semi colons and newlines are command separators. Close brackets are command terminators during command substitution (see below) unless quoted.
- A command is evaluated in two steps. First, the TCL interpreter breaks the command into words and then performs substitutions. The first word is used to locate a command procedure to carry out the command, and then all of the words of the commands are passed to the command procedure.
- Words of a command are separated by white spaces.
- The first character of a word denotes its type. If it is a double quote (), it must have a matching closing double quote. All the characters inside the closing double quote are considered as normal characters or string.
- If the first character is the open brace ({) then it should also be closed by the matching closing brace and they can be nested that there can be multiple pairs of open braces within an open brace.

- The words between a pair of the open big bracket ([) performs command substitution.
- This means the order of substitution is from left to right and one at a time.
- Words with a dollar sign ($) perform variable substitution. E.g. $name(index) where name gives the name of an array variable, and index gives the name of an element within that array. Name must contain only letters, digits, underscores, and namespace separators, and may be an empty string. Command substitutions, variable substitutions, and backslash substitutions are performed on the characters of the index.
- A word with a backslash \ gives backslash substitution. E.g. \n is for newline, for backspace, \t for tab, \v for vertical tab and so on.
- Comments should always start with a hashtag (#). All the words are considered as characters, and the compiler and interpreter ignore the line.
- The data types are also similar to the ones found in any other programming language. The data types available are strings, lists, numbers, Booleans, characters, and the internal representation (the interpreter will choose between string and structured representation based on the situation).

A.3.2 Network stack and node

The basic wireless model can be categorised as network stack and node and where network stack comprises of link layer, address resolution protocol (ARP), interface queue, and the physical (PHY) and MAC layer parameters. The network stack for a mobile node consists of a link layer (LL), an ARP module connected to LL, an interface priority queue (IFq), a MAC layer (MAC), and a network interface (netIF).

The LL simulates the data link layer of the network stack where packet fragmentation and reassembly are performed. The tasks of this layer are:

- To add MAC destination in the MAC header of the packet.
- To hand all the outgoing packets to LL by Routing Agent which then hands it to interface queue.
- To hand all incoming packets to LL by MAC layer which is then forwarded to node entry point.

The class LL is implemented in /ns-allinone-2.35/ns2.35/mac/ll.cc,h and /ns-allinone-2.35/ns2.35/TCL/lan/ns-ll.TCL.

The wireless model in NS2 has a node type mobile at its core. These nodes are assisted by supporting features that help in multi-hop ad hoc network simulations. The Mobile Node object is a split object for class Mobile Node which is derived from class Node. The basic features of Node are incorporated in class Mobile Node along with mobility in a defined topology and ability to be a transceiver in a wireless channel.

The main purpose of creating a Mobile Node is to use it in a wireless scenario i.e. link-less medium where it can change positions with time. Thus the node has features like mobility within the defined topology and periodic node position updates. Figure A.2 shows the basic architecture of a node [57], [43] shows the basic architecture of a node.

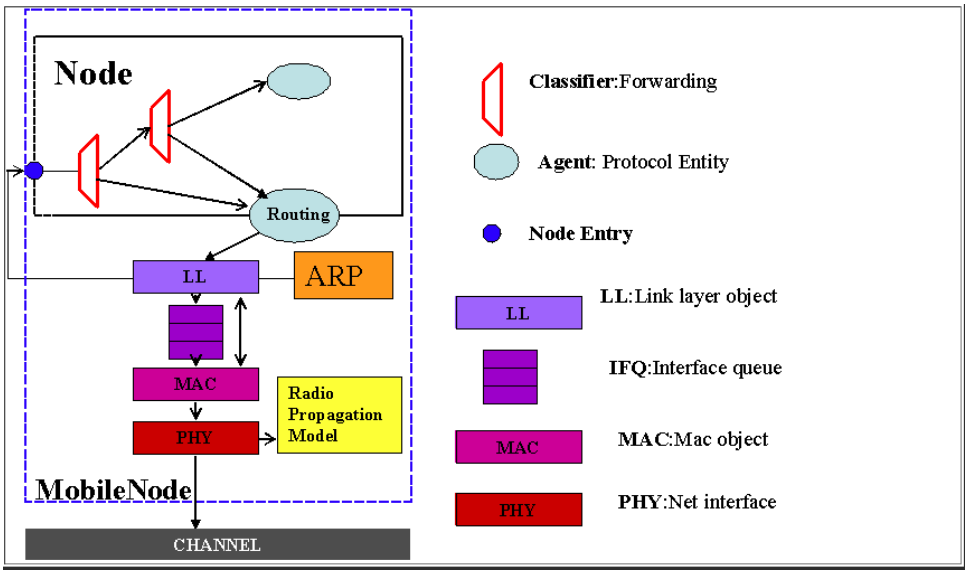

Figure A.2: Basic node architecture. [2]

We have discussed in brief the architecture of NS2 and how a mobile node works. Now let us further discuss how traffic is generated in those mobile nodes. In any mode of communications, there is a load which basically carries all the information. In wireless mode, the load is the data packets sent from one node to the other. Before transmission, these data packets are first placed over a TCP or a UDP agent. These packets are then sent to the node for transmission via its entry point and receive data through its node classifiers. Thus, the agent is not always the source of data.

Being open source, it is very important for NS2 to maintain a directory structure which also has C++ files that are used by the TCL simulation script. The node created in wireless mode is different from the normal mode because of mobility factor and periodic node

position update. There are various network layer components which need to be described in the tcl file during simulation. When a simple TCL script is run in the network, then the script is compiled on a top-down approach. Each line in the TCL script is then executed in a chronological order to provide us with the output results. The following is an example of TCL program that simulates standard 802.11p.

```
#============802.11p ================#
Phy/WirelessPhyExt set CSThresh_    3.162e-12;
#-85 dBm Wireless interface
#sensitivity (sensitivity defined in the standard)
Phy/WirelessPhyExt set Pt_0.0003108 ;#0.00000051
for distCST_ 80.0mts range
Phy/WirelessPhyExt set freq_5.9e+9
Phy/WirelessPhyExt set noise_floor_1.26e-13;
#-99 dBm for 10MHz bandwidth
Phy/WirelessPhyExt set L_ 1.0;
#default radio circuit gain/loss
Phy/WirelessPhyExt set PowerMonitorThresh_6.310e-14;
#-102dBm power monitor #sensitivity
Phy/WirelessPhyExt set HeaderDuration_ 0.000040;
#40 us Phy/WirelessPhyExt set BasicModulationScheme_0
Phy/WirelessPhyExt set PreambleCaptureSwitch_ 1
Phy/WirelessPhyExt
set DataCaptureSwitch_ 0
Phy/WirelessPhyExt set SINR_PreambleCapture_2.5118;
;# 4 dB
Phy/WirelessPhyExt set SINR_DataCapture_100.0;
;# 10 dB
Phy/WirelessPhyExt set trace_dist_1e;
Phy/WirelessPhyExt set PHY_DBG_0

Mac/802_11Ext set CWMin_$cwmin
Mac/802_11Ext set CWMax_$cwmax
Mac/802_11Ext set SlotTime_0.000013
Mac/802_11Ext set SIFS_0.000032
Mac/802_11Ext set ShortRetryLimit_7
Mac/802_11Ext set LongRetryLimit_4
Mac/802_11Ext set HeaderDuration_0.000040
Mac/802_11Ext set SymbolDuration_0.000008
```

```
Mac/802_11Ext set BasicModulationScheme_0
Mac/802_11Ext set use_802_11a_flag_true
Mac/802_11Ext set RTSThreshold_2346
Mac/802_11Ext set MAC_DBG   0

#=== Configure RF model parameters ======================
Antenna/OmniAntenna set Gt_ 1.0
Antenna/OmniAntenna set Gr_ 1.0

#=== Node configuration options ==========================
set val(chan) Channel/WirelessChannel;# channel type
set val(prop) Propagation/TwoRayGround;# radio-propagation model
set val(netif) Phy/WirelessPhyExt;# network interface type
set val(mac) Mac/802_11Ext;# MAC type
set val(ifq) Queue/DropTail/PriQueue;# interface queue type
set val(ll)  LL;# link layer type
set val(ant) Antenna/OmniAntenna;# antenna model
set val(ifqlen) 20;# max packet in ifq
set val(nn)  $val(num);# number of mobilenodes
set val(x)  2000;# X dimension of topography
set val(y)  200;# Y dimension of topography
set val(stop) 100;# time of simulation end
set val(rtg) DumbAgent;# routing protocol

#============ Create a ns simulator ============#
set ns_ [new Simulator]

#============ Setup topography object ============#
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
set god_ [create-god $val(nn)]
 $god_ off

#============ Open the NS trace file ============#
set tracefile [open out_vanet-802-11-p.tr w]
$ns_ use-newtrace
$ns_ trace-all $tracefile
#============Open the NAM trace file ============#
set namfile [open out_vanet-802-11-p.nam w]
```

```
$ns_ namtrace-all-wireless $namfile $val(x) $val(y)
#============Configure the Nodes============#
set chan [new $val(chan)]
$ns_ node-config -adhocRouting $val(rtg) \
     -llType $val(ll) \
     -macType $val(mac) \
     -ifqType $val(ifq) \
     -ifqLen $val(ifqlen) \
     -antType $val(ant) \
     -propType $val(prop) \
     -phyType $val(netif) \
     -channel $chan \
     -topoInstance $topo \
     -agentTrace ON \
     -routerTrace OFF \
     -macTrace OFF\
     -phyTrace OFF
#============Creating node objects ============#
for {set i 0} {$i < $val(nn) } { incr i } {
 set ID_($i) $i
 set node_($i) [$ns_ node]
 $node_($i) set id_ $ID_($i)
 $node_($i) set address_ $ID_($i)
 $node_($i) set X_ [expr $i * $nodedist]
 $node_($i) set Y_ 50
 $node_($i) set Z_ 0.0

 $node_($i) random-motion 0;# disable random motion
}
#============ PBC Agents Definition ============#
for {set i 0} {$i < 1 } { incr i } {
 set agent_($i) [new Agent/PBC]
 $ns_ attach-agent $node_($i) $agent_($i)
 $agent_($i) set payloadSize 500
 $agent_($i) set periodicBroadcastInterval 0.01
 $agent_($i) set periodicBroadcastVariance 0.01
 $agent_($i) set modulationScheme 1
 $agent_($i) singleBroadcast
 #packetType (0 = safety , 1 = service)
```

```
 #Safety Type packet, set the channel number to -99
 $agent_($i) set channel_ -99
 $agent_($i) set type_dsrc_ 0
}
for {set i 1} {$i < $val(nn)} { incr i } {
 set agent_($i) [new Agent/PBC]
 $ns_ attach-agent $node_($i) $agent_($i)
 $agent_($i) set payloadSize 500
 $agent_($i) set periodicBroadcastInterval 0.5
 $agent_($i) set periodicBroadcastVariance 0.05
 #$agent_($i) set modulationScheme 1
 $agent_($i) Repeater ON $retransmission
 #packetType (0 = safety, 1 = service)
 #Safety Type packet, set the channel number to -99
 $agent_($i) set channel_ -99
 $agent_($i) set type_dsrc_ 0
}
#============ Define node initial position in nam ============#
for {set i 0} {$i < $val(nn) } { incr i } {
 $ns_ initial_node_pos $node_($i) 0
}
#============ Define a 'finish' procedure ============#
proc finish {} {

 global ns_ tracefile namfile
 $ns_ flush-trace
 close $tracefile
 close $namfile
 #exec nam scenario1.nam &
}
#============ Tell node to stop============#
for {set i 0} {$i < $val(nn) } { incr i } {
 $ns_ at $val(stop).0 "$node_($i) reset";
}

$ns_ at $val(stop) "$ns_ nam-end-wireless $val(stop)"
$ns_ at $val(stop) "finish"
$ns_ at $val(stop).0002 "puts \"End Simulation\" ; $ns_ halt"
puts "Starting Simulation..."
```

```
$ns_ run
```

NS2 provides users with an executable command .ns which takes an input argument, the name of a TCL simulation scripting file with file extension.tcl. The TCL simulation script acts as an input argument of an NS2 executable command ns. After simulation, NS2 outputs either text-based trace file .tr or animation-based simulation .nam results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used.

AWK scripts are then used to filter files ".tr" and calculate the desired performance parameters. AWK is a tool to search, simple or complex, in text files. It is a programming language from 1977, date of its appearance in the Unix world. It takes its name from three programmers who developed it: Alfred V. Aho, Peter J. Weinberger and Brian W. Kernighan. Awk works by reading the data. This data can be well handled by the user. User can choose to read data from files or standard input channel. The execution is done by the command:

awk -f file.awk file.tr.

where file.awk : is the AWK command file registered under the ".awk" extension. The command executes the program sequentially lying in the file called "file.tr".

References

[1] Website. http://eceng.weebly.com/network-simulator-2.html. accessed: August,2011.

[2] Website. http://www.mathcs.emory.edu/~cheung/Courses/558/Syllabus/18-WirelessSim/intro.html. accessed: August,2011.

[3] Website. http://www.theregister.co.uk/2011/04/07/microsoft_toyota/. accessed:July.2011.

[4] Website. http://www.e-sponder.eu/. accessed: August,2012.

[5] Website. http://www.isi.edu/nsnam/. accessed:February,2011.

[6] Website. http://www.mash.cs.berkeley.edu/. accessed:August,1998.

[7] Website. http://grouper.ieee.org/groups/scc32/dsrc/. accessed: September,2012.

[8] Website. http://www.esa.int/esaTE/SEM1A01YUFF_index_0.html. accessed:July.2004.

[9] Website. http://money.cnn.com/2005/06/06/technology/personaltech/united_wifi/.

[10] Website. https://www.corelan.be/index.php/2009/02/20/cheatsheet-cracking-wep-with-backtrack-4-and-aircrack-ng/. accessed:July,2014.

[11] Website. http://www.cr0.net:8040/code/network/aircrack/.

[12] Website. http://www.vlcc.net/?ml_lang=en. accessed: January,2015.

[13] Website. http://www.lificonsortium.org/. accessed: January,2015.

[14] Website. https://www.nsnam.org/release/. accessed: August,2011.

References

[15] 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 1: high-speed physical layer in the 5 GHz band. *ISO/IEC 8802-11:1999/Amd 1:2000(E); IEEE Std 802.11a-1999*, pages i–83, 2000.

[16] IEEE trial-use standard for wireless access in vehicular environments (WAVE) - Multi-Channel Operation. *IEEE Std 1609.4-2006 -Test*, pages 1–82, Nov 2006.

[17] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services. *IEEE Std 1609.3-2007*, pages 1–99, April 2007.

[18] IEEE Draft Amendment to 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 7: Interworking With External Networks. *IEEE Unapproved Draft Std P802.11u/D3.0, May 2008*, pages – , 2008.

[19] 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. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pages 1–2793, March 2012.

[20] Sasan Adibi and Shervin Erfani. Mobile ad-hoc networks with QoS and RSVP provisioning. In *Electrical and Computer Engineering, 2005. Canadian Conference on*, pages 2069–2072. IEEE, 2005.

[21] Ahmad Al Hanbali, Eitan Altman, and Philippe Nain. A survey of TCP over ad hoc networks. *IEEE Communications Surveys and Tutorials*, 7(1-4):22–36, 2005.

[22] Mark Allman. On the generation and use of TCP acknowledgments. *ACM SIGCOMM Computer Communication Review*, 28(5):4–21, 1998.

[23] Eitan Altman and Tania Jiménez. Novel delayed ACK techniques for improving TCP performance in multihop wireless networks. In *Personal Wireless Communications*, pages 237–250. Springer, 2003.

[24] Eitan Altman and Tania Jimenez. Ns simulator for beginners. *Synthesis Lectures on Communication Networks*, 5(1):1–184, 2012.

References

[25] A. Amine, O.A. Mohamed, and B. Benatallah. *Network Security Technologies: Design and Applications*. Advances in information security, privacy, and ethics (AISPE) book series. IGI Global, 2014.

[26] Ajay Bakre and BR Badrinath. I-TCP: Indirect TCP for mobile hosts. In *Distributed Computing Systems, 1995., Proceedings of the 15th International Conference on*, pages 136–143. IEEE, 1995.

[27] Hari Balakrishnan, Srinivasan Seshan, Elan Amir, and Randy H Katz. Improving TCP/IP performance over wireless networks. In *Proceedings of the 1st annual international conference on Mobile computing and networking*, pages 2–11. ACM, 1995.

[28] Paolo Bellavista and Antonio Corradi. *The handbook of mobile middleware*. CRC press, 2006.

[29] Brahim Bensaou, Yu Wang, and Chi Chung Ko. Fair medium access in 802.11 based wireless ad-hoc networks. In *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, pages 99–106. IEEE Press, 2000.

[30] Saad Biaz and Nitin H Vaidya. Distinguishing congestion losses from wireless transmission losses: A negative result. In *Computer Communications and Networks, 1998. Proceedings. 7th International Conference on*, pages 722–731. IEEE, 1998.

[31] Robert Braden. Requirements for internet hosts-communication layers. 1989.

[32] Kevin Brown and Suresh Singh. M-TCP: TCP for mobile cellular networks. *ACM SIGCOMM Computer Communication Review*, 27(5):19–43, 1997.

[33] Kenneth Bullington. Radio propagation fundamentals*. *Bell System Technical Journal*, 36(3):593–626, 1957.

[34] Pino Caballero-Gil. *Security Issues in Vehicular Ad Hoc Networks*. INTECH Open Access Publisher, 2011.

[35] Kartik Chandran, Sudarshan Raghunathan, Subbarayan Venkatesan, and Ravi Prakash. A feedback-based scheme for improving TCP performance in ad hoc wireless networks. *Personal Communications, IEEE*, 8(1):34–39, 2001.

[36] Ruy De Oliveira and Torsten Braun. A dynamic adaptive acknowledgment strategy for TCP over multihop wireless networks. In *INFOCOM 2005. 24th annual joint conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1863–1874. IEEE, 2005.

[37] Stephen E Deering. Internet protocol, version 6 (IPv6) specification. 1998.

[38] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. Network mobility (NEMO) basic support protocol. Technical report, 2004.

[39] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. RFC 3963 Network Mobility (NEMO) Basic Support Protocol, 2005.

[40] AK Dubey, A Jain, Raksha Upadhyay, and SV Charhate. Performance evaluation of wireless network in presence of hidden node: A queuing theory approach. In *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, pages 225–229. IEEE, 2008.

[41] Thierry Ernst. Network mobility support terminology. *Network*, 2007.

[42] Thierry Ernst and Keisuke Uehara. Connecting automobiles to the internet. In *ITST: 3rd International Workshop on ITS Telecommunications, Seoul, South Korea*. Citeseer, 2002.

[43] Kevin Fall and Kannan Varadhan. The ns manual (formerly ns notes and documentation). *The VINT project*, 47, 2005.

[44] Sally Floyd and Tom Henderson. RFC 2582: The NewReno modification to TCPs fast recovery algorithm. *IETF, April*, 1999.

[45] Sally Floyd and Van Jacobson. Random early detection gateways for congestion avoidance. *Networking, IEEE/ACM Transactions on*, 1(4):397–413, 1993.

[46] Zhenghua Fu, Benjamin Greenstein, Xiaoqiao Meng, and Songwu Lu. Design and implementation of a TCP-friendly transport protocol for ad hoc wireless networks. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, pages 216–225. IEEE, 2002.

[47] Mario Gerla, Ken Tang, and Rajive Bagrodia. TCP performance in wireless multihop networks. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*, pages 41–50. IEEE, 1999.

[48] Abhinav Gupta, Ian Wormsbecker, and C Wilhainson. Experimental evaluation of TCP performance in multi-hop wireless ad hoc networks. In *Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004.(MASCOTS 2004). Proceedings. The IEEE Computer Society's 12th Annual International Symposium on*, pages 3–11. IEEE, 2004.

[49] Richard Halverson and Annette Smith. How new technologies have (and have not) changed teaching and learning in schools. *Journal of Computing in Teacher Education*, 26(2):49–54, 2009.

References

[50] Ehsan Hamadani and Veselin Rakocevic. A cross layer solution to address TCP intra-flow performance degradation in multihop ad hoc networks. *Journal of Internet Engineering*, 2(1):146–156, 2008.

[51] S Hamrioui and M Lalam. Incidences of the improvement of the MAC-Transport and MAC–Routing interactions on MANET Performance. In *International Conference on Next Generation Networks and Services*, 2010.

[52] Sofiane Hamrioui and Mustapha Lalam. Incidence of the improvement of the transport: MAC protocols interactions on MANET performance. In *Proceedings of the 8th international conference on New technologies in distributed systems*, page 15. ACM, 2008.

[53] Gavin Holland and Nitin Vaidya. Analysis of TCP performance over mobile ad hoc networks. *Wireless Networks*, 8(2/3):275–288, 2002.

[54] Jeng-Ji Huang and Yu-Shiang Chiu. A scheme to reduce merging collisions in TDMA-based VANETs. In *Wireless and Pervasive Computing (ISWPC), 2013 International Symposium on*, pages 1–4. IEEE, 2013.

[55] Esa Hyytiä and Jorma Virtamo. Random waypoint model in n-dimensional space. *Operations Research Letters*, 33(6):567–571, 2005.

[56] IEEE. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Standard*, 802(11), 1999.

[57] Teerawat Issariyakul and Ekram Hossain. *Introduction to network simulator NS2*. Springer Science & Business Media, 2011.

[58] Aruna Jayasuriya, Sylvie Perreau, Arek Dadej, and Steven Gordon. *Hidden vs exposed terminal problem in ad hoc networks*. PhD thesis, ATNAC 2004, 2004.

[59] Daniel Jiang and Luca Delgrossi. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040. IEEE, 2008.

[60] Rui Jiang, Vikram Gupta, and Chinya V Ravishankar. Interactions between TCP and the IEEE 802.11 MAC protocol. In *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, volume 1, pages 273–282. IEEE, 2003.

[61] David Johnson, Charles Perkins, and Jari Arkko. Mobility support in IPv6. Technical report, 2004.

[62] Phil Karn. MACA-a new channel access method for packet radio. In *ARRL/CRRL Amateur radio 9th computer networking conference*, volume 140, pages 134–140, 1990.

[63] Vikas Kawadia and PR Kumar. Experimental investigations into TCP performance over wireless multihop networks. In *Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, pages 29–34. ACM, 2005.

[64] Arzad Alam Kherani and Rajeev Shorey. Throughput analysis of TCP in multi-hop wireless networks with IEEE 802.11 MAC. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, volume 1, pages 237–242. IEEE, 2004.

[65] Dongkyun Kim, C-K Toh, and Yanghee Choi. TCP-BuS: Improving TCP performance in wireless ad hoc networks. *Communications and Networks, Journal of*, 3(2):1–12, 2001.

[66] Tianbo Kuang, Fang Xiao, and Carey Williamson. Diagnosing wireless TCP performance problems: A case study. In *In Proc. of SPECTS*. Citeseer, 2003.

[67] Agnes Kukulska-Hulme. *Mobile learning: A handbook for educators and trainers*. Psychology Press, 2005.

[68] James F Kurose. *Computer networking: a top-down approach featuring the Internet*. Pearson Education India, 2005.

[69] Krishan Kant Lavania, GL Saini, H Kothari Rooshabh, and A Yagnik Harshraj. Privacy Anxiety and Challenges in Mobile Ad Hoc Wireless Networks and its Solution. *International Journal of Scientific & Engineering Research*, 2(9):173–177, 2011.

[70] Jian Li. *Quality of service (QoS) provisioning in multihop ad hoc networks*. PhD thesis, Citeseer, 2006.

[71] Jian Liu and Suresh Singh. ATCP: TCP for mobile ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 19(7):1300–1315, 2001.

[72] Jun Liu, Ibrahim Matta, and Mark Crovella. End-to-end inference of loss nature in a hybrid wired/wireless environment. In *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pages 9–pages, 2003.

[73] Stephane Lohier, Yacine Ghamri Doudane, and Guy Pujolle. MAC-layer adaptation to improve TCP flow performance in 802.11 wireless networks. In *Wireless and Mobile Computing, Networking and Communications, 2006.(WiMob'2006). IEEE International Conference on*, pages 427–433. IEEE, 2006.

[74] Joseph Macker. Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations. 1999.

[75] Mahesh K Marina and Samir R Das. Impact of caching and MAC overheads on routing performance in ad hoc networks. *computer communications*, 27(3):239–252, 2004.

[76] Mohammad A Matin. *Handbook of Research on Progressive Trends in Wireless Communications and Networking*. IGI Global, 2014.

[77] John E Miller and Kurt C Reitinger. Force XXI battle command. *Military Review*, 75:5–5, 1995.

[78] Abubakar Aminu Mu'azu, Low Tang Jung, Ibrahim Lawal, Peer Azmat Shah, et al. A QoS approach for cluster-based routing in VANETS using TDMA scheme. In *ICT Convergence (ICTC), 2013 International Conference on*, pages 212–217. IEEE, 2013.

[79] Kitae Nahm, Ahmed Helmy, and C-C Jay Kuo. On interaction between MAC and transport layers for media streaming in 802.11 ad hoc networks. In *Optics East*, pages 99–110. International Society for Optics and Photonics, 2004.

[80] Ping Chung Ng, Soung Chang Liew, Ka Chi Sha, and Wai Ting To. Experimental study of hidden node problem in IEEE 802.11 wireless networks. *Sigcomm Poster*, page 26, 2005.

[81] Stephan Olariu and Michele C Weigle. *Vehicular networks: from theory to practice*. Crc Press, 2009.

[82] Stylianos Papanastasiou, Lewis M Mackenzie, Mohamed Ould-Khaoua, and Vassilis Charissis. On the interaction of TCP and Routing Protocols in MANETs. In *Telecommunications, 2006. AICT-ICIW'06. International Conference on Internet and Web Applications and Services/Advanced International Conference on*, pages 62–62. IEEE, 2006.

[83] Christina Parsa and JJ Garcia-Luna-Aceves. TULIP: A link-level protocol for improving TCP over wireless links. In *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE*, pages 1253–1257. IEEE, 1999.

[84] Charles Perkins. Ip mobility support for IPv4. 2002.

[85] Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. Technical report, 2003.

[86] ASTM Std. E2213-03,Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[87] Sanaa Taha and Xuemin Shen. A link-layer authentication and key agreement scheme for mobile public hotspots in NEMO based VANET. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 1004–1009. IEEE, 2012.

[88] Sanaa Taha and Xuemin Sherman Shen. Fake point location privacy scheme for mobile public hotspots in NEMO based VANET. In *Communications (ICC), 2013 IEEE International Conference on*, pages 2037–2041. IEEE, 2013.

[89] Susan Thomson. IPv6 stateless address autoconfiguration. 1998.

[90] Vassilios Tsaoussidis and Hussein Badr. TCP-probing: towards an error control schema with energy and throughput performance gains. In *Network Protocols, 2000. Proceedings. 2000 International Conference on*, pages 12–21. IEEE, 2000.

[91] R Uzcategui and Guillermo Acosta-Marum. WAVE: a tutorial. *Communications Magazine, IEEE*, 47(5):126–133, 2009.

[92] Anna Maria Vegni, Mauro Biagi, and Roberto Cusani. *Smart vehicles, technologies and main applications in vehicular ad hoc networks*. INTECH Open Access Publisher, 2013.

[93] Lars Wischhof, Andr Ebner, and Hermann Rohling. Self-organizing traffic information system based on car-to-car communication: Prototype implementation. In *International Workshop on Intelligent Transportation (WIT)*, pages 49–53, 2004.

[94] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and localization of sybil nodes in VANETs. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pages 1–8. ACM, 2006.

[95] Taichi Yuki, Takayuki Yamamoto, Masashi Sugano, Masayuki Murata, Hideo Miyahara, and Takaaki Hatauchi. Performance improvement of TCP over an ad hoc network by combining of data and ACK packets. *IEICE Transactions on Communications*, 86:3559–3568, 2004.

[96] Hongqiang Zhai, Xiang Chen, and Yuguang Fang. Improving transport layer performance in multihop ad hoc networks by exploiting MAC layer information. *Wireless Communications, IEEE Transactions on*, 6(5):1692–1701, 2007.

References

[97] Chi Zhang and Vassilios Tsaoussidis. TCP-real: improving real-time capabilities of TCP over heterogeneous networks. In *Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video*, pages 189–198. ACM, 2001.

[98] Bin Zheng and Yuliang Yang. Handover mechanism based on Care-of Prefix Pool in VANET with NEMO. In *Computer Science & Service System (CSSS), 2012 International Conference on*, pages 1014–1017. IEEE, 2012.

List of Publications

1. Sofiane Hamrioui, Mustapha Lalam, Diyar K Arab, Amine Berqia, and Pascal Lorenz. Improving tcp performance in manet by exploiting mac layer algorithms. IRACST-International Journal of Research in Management & Technology (IJRMT), 1(2):5967, 2011.

2. Diyar Khairi M S DEEI, FCT Amine Berqia DEEI, et al. Design and implementation of a secure nemo. International Journal of Computer Science and Information Security, 10(11):1,ISSN 1947-5500, 2012.

3. Diyar Khairi M S, Amine Berqia, "Li-Fi the future of Vehicular Ad hoc Networks", Journal "Transactions on Networks and Communications", UK ISSN: 2054-7420.

4. Diyar Khairi M S, Amine Berqia, "Survey on QoS and Security in Vehicular Ad hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 42-52, 2015.

5. Diyar Khairi M S, Amine Berqia, "Improving TCP Performance on WAVE Networks", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, 2015.

6. Amine Berqia, Diyar Khairi M S, "V-Learning: Vanets for Social and Mobile Learning", The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015), Tunis (Published).