THESIS

In Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
from TELECOM ParisTech

Specialization: Communications and Electronics

Daniel Câmara

Techniques to Support Alert and Crisis Management in Public Safety Networks

Defense scheduled on the 4th of March 2010 before a committee composed of:

Reviewers	Prof. Khaldoun Al Agha, Université Paris-Sud, France
	Prof. Marcelo Dias Amorim, Université Pierre et Marie Curie, France
Examiner	Dr. Paolo Santi, Instituto di Informatica e Telematica, Italy
Thesis supervisors	Prof. Christian Bonnet, EURECOM, France
	Dr. Fethi Filali, Qatar University Wireless Innovations Center, Qatar

THESE

présentée pour obtenir le grade de

Docteur de TELECOM ParisTech

Spécialité: Communication et Electronique

Daniel Câmara

Techniques Pour le Support des Phases d'Alerte et de Gestion de Crise des Réseaux de Sécurité Civile

Thèse prévue le 4 mars 2010 devant le jury composé de :

Rapporteurs	Prof. Khaldoun Al Agha, Université Paris-Sud, France
	Prof. Marcelo Dias Amorim, Université Pierre et Marie Curie, France
Examinateur	Dr. Paolo Santi, Instituto di Informatica e Telematica, Italy
Directeurs de thèse	Prof. Christian Bonnet, EURECOM, France
	Dr. Fethi Filali, Qatar University Wireless Innovations Center, Qatar

To my wife, Wanessa, my son, Arthur, and my daughter, Helena,

for their support and undestanding.

Acknowledgements

As any research work this thesis is the result of the collaborative work with a number of different researchers and research projects. The collaboration with other EURECOM and outside researchers was decisive in the final quality of the work. For the friendly and uncompromised, yet highly productive environment we have here at EURECOM I must thank to all, students, professors and employees.

However I would like to specially thank, professor Fethi Filali for providing me this opportunity of working here at EURECOM, and professor Christian Bonnet, for the insightful and clear view, not only of the problems we faced, but also of the PhD process as a whole. I learned a lot here during the last three years and without the guidance of professor Bonnet and Filali this work wouldn't be possible.

I am rely grateful to all PhD students of EURECOM, but I would like to specially thank some of them. I am sincerely and deeply thankful to Randa Zakhour, for all the endless reviews and for being so patient with me and my stupid jokes during the time we shared the office. I want also to thank Ikbal Chammakhi Msadaa, for the work we developed together, and the numerous reviews. I am also deeply grateful to Giuliana Iapichino for give me the wonderful opportunity to work with her in a book chapter that greately helped to put this whole thesis together. I would like to thank also all my office mates, Erhan Yilmaz, Antony Schutz, Agisilaos Papadogiannis and Konstantinos Papakonstantinou, for providing a friendly and productive work environment.

I would also like to thanks to all the secretariat people, mainly Gwenaëlle Le Stir, Christine Mangiapan, Christine Roussel and Emilie Vivier for the guidance, patience and help over the bureaucratic process.

Specially I would like to thank my great friend and co-author Nikolaos Frangiadakis to whom I owe more than I will be ever able to pay. Nick thanks for the long conversations, reviews and, above all, for jumping with me into all the crazy stuff I have proposed to you without blinking even once. I am really and deeply grateful to you my friend.

I would like to express here also my deepest gratitude to my family, Wanessa Nascimento Câmara, Arthur Nascimento Câmara and Helena Nascimento Câmara, for the patience and understanding over the lost weekends. Finally, I would like to acknowledge and thank my mother, Maria Rosa Câmara, and my father, Pedro Izidoro Câmara, for the basis they provided me and that were, surely enough, the seeds to this thesis.

Abstract

Public Safety Networks (PSNs) are the kind of networks deployed by the authorities, in case of a natural, or man made, disaster to spread information and coordinate rescue teams. This particular kind of network is mission critical, if it does not work, or works poorly, lives may be lost. This theses aims to help PSNs in two distinct situations: warning message distribution and field teams network organization.

In the advent of a crisis, normally, authorities have interest in spreading warnings and information about the measures one should take to avoid any danger. These messages have been broadcasted by regular broadcast mediums, e.g. sirens, radio and TV. Unfortunately, in the case of a huge catastrophe, traditional broadcast mediums may fail to reach all the interested people in a given region. However, with the next generation of vehicles developed targeting road safety, the communication devices built into the cars may be used to broaden even more the coverage of these warning messages. We propose here a simple, yet efficient, technique to increase the network coverage using such devices

The second part of this thesis focus on the organization of the rescue nodes on the field. Having a well defined and stable network is of paramount importance for PSNs. We propose here not only a topology control algorithm to deploy the CHORIST network architecture, but also a generic topology admission control and topology management method that is reliable enough to be used in PSNs. The technique is based on the economy laws of supply and demand leading to a Pareto optimal organization of the nodes.

Contents

List of Figures

Acronyms

Here are the acronyms used in this dissertation. They are also defined when they first appear in the text.

ACK	Acknowledge Message
AP	Access Point
BE	Best Effort
BS	Base Station
CBR	Constant Bit Rate
CH	Cluster Head
CH	Cluster Head
CHORIST	Integrating Communications for enHanced envirOnmental RISk management and citizens safe
CRC	Cyclic Redundancy Check
DAD	Duplicate Address Detection
DCH	Default Cluster Heads
DTN	Disruption/Delay Tolerant Network
DTN	Disruption/Delay Tolerant Networks
DTNRG	Delay-Tolerant Networking Research Group
EAS	Emergency alert system
ertPS	Extended Real-time Polling Service
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
HI	Identifier
HIP	Host Identity Protocol
Host HIT	Host Identity Tag
I2V	Infrastructure-to-Vehicle
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IN	Isolated Nodes

IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPNRG	Interplanetary Internet Research Group
IRTF	Internet Research Task Force
LAN	Local Area Network
LOS	Line-of-Sight
MAC	Medium Access Control
MIPv6	Mobile IPv6
MN	Mobile Node
MR	Mesh Router
MR	Mesh Router
MULEs	Mobile Ubiquitous LAN Extensions
nrtPS	Non-real-time Polling Service
OFDM	Orthogonal Frequency Division Multiplexing
PHY	Physical Layer
PMIPv6	Proxy Mobile IPv6
PRADA	PRobe-based Distributed protocol for knowledge range Adjustment
PSN	Public Safety Network
QoS	Quality of Service
RATCOM	Réseau d'alerte aux Tsunamis et Côtiers en Méditerranée
RN	Relay Node
RN	Relay Node
RSU	Roadside Unit
rtPS	Real-time Polling Service
SINR	Signal to Interference and Noise Ratio
SNR	Signal-to-Noise Ratio
SS	Subscriber Station
SWIM	Shared Wireless Infostation Model
SWIM	Shared Wireless Infostation Model
TCP	Transmission Control Protocol
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TIGER	Topologically Integrated Geographic Encoding and Referencing
UGS	Unsolicited Grant Service
V2V	Vehicle-to-Vehicle
VAP	Virtual Access Points
VDTN	Vehicular DTN
WCIDS	Weakly Connected Independent Dominating Set
WiMAX	Worldwide Interoperability for Microwave Access

WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WWAN	Wireless Wide Area Network

Part I

Intodoction

Chapter 1

Thesis Motivation

This thesis proposes a new set of techniques to enhance the coverage and organization of wireless mobile networks in the Public Safety context. Public Safety Networks (PSNs) are networks established by the authorities to either warn the population about an imminent catastrophe or coordinate teams during the crisis and normalization phases. A catastrophe can be defined as an extreme event causing a profound damage or loss as perceived by the afflicted people. PSNs have the fundamental role of providing communication and coordination for emergency operations.

Disasters can be of different types: natural disasters (e.g. hurricanes, floods, earthquakes and epidemics), or man-made disasters (e.g. industrial and nuclear accidents, maritime accidents and terrorist attacks). In both cases, human lives are in danger and the telecommunication infrastructures may be seriously affected or even no longer operational. Disaster management is required to handle the damages. It involves three main phases: preparedness, crisis and return to normal situation. These three phases are presented in Figure 1.1. In this work we focus on the crisis phase. This phase goes from the break-out point, when the authorities decide to respond to the specific event, to the immediate disaster aftermath, when lives can still be saved. The crisis phase can even be further subdivided into alert and crisis handling phases. The alert phase is when the population needs to be informed about an eminent threat or the occurred disaster. Crisis handling consists of the measures taken by the authorities to deal with the disaster.

This thesis presents contributions to help in both alert and crisis handling phases.

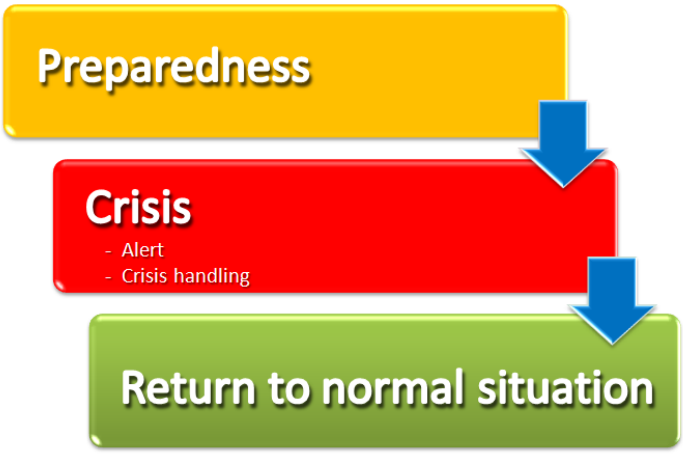


Figure 1.1: Disaster management phases

The alert phase is crucial in the sense that, if efficiently done, lives can be saved, since people may be able to completely avoid the endangered zone. Many methods can be employed such as sirens, TV and radio broadcast. However, these methods rely first on the existence of an already deployed structure and second on assuming that the population will have access to a siren, TV or radio. The problem with relying on a deployed structure is that, in case of a catastrophe, this structure may be severely compromised. The problem with the second assumption is that people may not be near the deployed sirens or watching TV. This is especially true for people on the move, e.g. traveling by car, or walking on the streets. This work provides an alternative option for spreading the information and increasing the warning coverage in a non-intrusive and transparent way.

The solution proposed in the thesis to help in the alert phase is based on opportunistic networks and uses the communication equipment available with people, and that will be soon available also in cars, to overcome the lack of coverage problem. This technique, which we term Virtual Access Points (VAPs), creates a distributed and cooperative cache among the mobile nodes in the affected area. When using the VAP technique, nodes cooperatively work as virtual access points by re-broadcasting messages they have received before and which are stored in their own cache: they thus act in a receive-store-and-forward way. This helps to spread the message to nodes that did not have access to it before. The main advantages of the proposed technique are that it does not rely on any specific characteristics of the network, is transparent, and highly improves the efficiency of data dissemination.

The crisis handling phase also presents challenging problems and consists of a fertile terrain for research. The problem we address here is topology management and network admission control. We provide solutions for building stable and reliable network structures, which are crucial in the coordination of rescue teams during the most difficult and adverse situations.

Topology management for PSNs is particularly challenging for a series of reasons. First, the main concerns for PSNs are rapid deployment and survivability. Second, PSNs are required to be highly adaptive since the network requirements for different disaster scenarios may differ completely. For example, the number of nodes, the people served, the mobility pattern and deployment environment for a wildfire site differ greatly from the ones for an earthquake relief effort one. However, people working on these sites and their communication equipment are basically the same.

This work not only presents a solution for the establishment and maintenance of the PSN architecture proposed for some governmental projects, but also introduces a new technique capable of addressing, in a simple and efficient way, the different needs of different disaster sites. The proposed technique takes into consideration the economic concepts of supply and demand. The approach permits the dynamic adaptation of the topology to the specific needs of a target site, and enables the modification of the organization of an already established network.

Wireless Public Safety Networks are an extreme case where area coverage, dynamic and self-adaptive mechanisms become critically important. The techniques exposed in this thesis are applied to PSNs but are quite general and can be further applied to a broader range of situations in other networks, such as sensor and vehicular networks.

This thesis proposes solutions for problems in the alert and crisis handling sub-phases of the crisis phase. To detail our work, we have organized the text into four parts. The first part presents an introduction of the whole theme and a deeper look into the Public Safety Networks field. The second part describes our contribution to improve the communication during the alert phase and evaluates the results obtained with the use of the technique. The third part details our contribution for topology management to help PSNs during the crisis handling phase. Finally, the last part presents a conclusion of the thesis and its contributions. It also points out some future work and research directions in this field. The next section presents the thesis' chapters, along with a summary of the content of each one.

1.1 Thesis Summary

Chapter 2 - Public Safety Networks

In this introductory chapter we present a summary of the fundamental properties of Public Safety Networks. The greatest part of the work described in this thesis is related to the application of the developed techniques to Public Safety Networks environments. The main aim of this chapter is to provide a broad view of the PSN field, by presenting the different emergency management phases, the PSNs requirements and some of the associated challenges.

Some part of this chapter was published in:

- Giuliana Iapichino, Daniel Câmara, Christian Bonnet, Fethi Filali, Public Safety Networks, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010.

Chapter 3 - Vehicular Disruption Tolerant Networks

Some of the techniques presented in this thesis use the concept of Disruption Tolerant Network (DTN), more specifically Vehicular DTN (VDTN) to address some of the issues related to the increasing area coverage in the case of a disaster and to spreading warning messages.

Disruption Tolerant Networks, referred also as Delay Tolerant (DTN) or opportunistic networks, have been developed as an approach to building architecture models tolerant to long delays and/or disconnected network partitions in the delivery of data to destinations. In this chapter, we present the characteristics of DTNs, and some of the techniques developed to ensure packet delivery in these networks.

Some part of this chapter was published in:

- Daniel Câmara, Nikolaos Frangiadakis, Christian Bonnet, Fethi Filali, Vehicular Delay Tolerant Networks, In Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010.

Chapter 4 - Virtual Access Points for Mobile Communication

In the future, in a pervasive wireless world, all roads and cities are expected to be covered by roadside base stations and network access will be provided to both pedestrians and vehicular users. However, for the moment, roadside equipment or Access Points (APs) are not always present, and even if they are, as a result of a disaster the network can be compromised. The main consequence of these situations is the existence of uncovered areas where the only possible communication mode is from one vehicle to another. Furthermore, equipping roads with each new generation of networking access devices requires time for large scale deployment. In the near future user equipments will be easier to update and will have more capabilities than the roadside infrastructure. This chapter discusses a simple, yet powerful, technique to extend coverage to nodes outside covered areas. We focus on warning message and streaming data dissemination.

Some part of this chapter was published in:

- Daniel Câmara, Christian Bonnet, Fethi Filali, Propagation of Public Safety Warning Messages, IEEE Wireless Communications & Networking Conference (WCNC) 2010, Sydney, Australia, 18-21 April 2010
- Daniel Câmara, Nikolaos Frangiadakis, F. Filali, A. A. F. Loureiro, Nick Roussopoulos, Virtual Access Points for Disaster Scenarios, IEEE Wireless Communications & Networking Conference (WCNC) 2009, IEEE, Budapest, Hungary, April 5-8, 2009
- Daniel Câmara, Nikolaos Frangiadakis, F. Filali, A. A. F. Loureiro, Nick Roussopoulos, Virtual Access Points for Stream Based Traffic Dissemination, 2008 IEEE Asia-Pacific Services Computing Conference, IEEE, Yilan, Taiwan, December 9-12, 2008
- Nikolaos Frangiadakis, Daniel Câmara, Fethi Filali, Antonio Alfredo FLoureiro, Nick Roussopoulos, Virtual access points for vehicular networks, Mobilware 2008, 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, ACM, February 12th-15th, 2008, Innsbruck, Austria

Chapter 5 - Mesh Networks

In the last years Wireless Mesh Networks (WMNs) have been attracting a huge amount of attention from both academia and industry. Indeed, WMN is now emerging as a promising technology for broadband wireless access. WMNs are a type of network where each node may act as an independent router, regardless of whether it is connected to another network or not. In general, for small environments, the deployment of plain mesh networks is the easiest and fastest way to set a network in the field. The objective of this chapter is to discuss and present this kind of network, since the crisis handling networks typically rely on a mesh structure to provide communication capabilities to the teams on the field.

Some part of this chapter was published in:

- Ikbal Chammakhi Msadaa, Daniel Câmara, and Fethi Filali, Scheduling and CAC in IEEE 802.16 Fixed BWNs: A Comprehensive Survey and Taxonomy, to appear in IEEE Communications Surveys & Tutorials, No4, 2010

- Erlon R. Cruz, Daniel Câmara, Hélio C. Guardia, Providing Billing Support in WiMAX Mesh Networks, The 5th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2009), IEEE, Marrakech, Morocco, 13-14 October 2009
- Daniel Câmara and Fethi Filali, Scheduling and Call Admission Control A WiMax Mesh Networks View, Guide to Wireless Mesh Networks, Chapter 17, Springer, January, 2009
- Azzedine Boukerche, Daniel Câmara, Carlos M.S. Figueiredo, and Antonio A.F. Loureiro, Algorithms for Mobile Ad Hoc Networks, Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, Chapter 1, edited by Azzedine Boukerche, John Wiley and Sons, ISBN: 0470383585, October, 2008

Chapter 6 - Topology Management

This chapter presents an introductory discussion of topology management and its importance in the context of wireless networks. Self organizing networks are one of the key factors to enable the utilization of wireless mesh networks on the field.

Some part of this chapter was published in:

- Ikbal Chammakhi Msadaa, Daniel Câmara, and Fethi Filali, Mobility Management in WiMAX Network, WiMAX Security and Quality of Service: Providing an End to End Explanation, Wiley, accepted for publication, to appear in late 2009
- Azzedine Boukerche, Daniel Câmara, Carlos M. S. Figueiredo, and Antonio A.F. Loureiro, Algorithms for Mobile Ad Hoc Networks, Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, Chapter 1, edited by Azzedine Boukerche, John Wiley and Sons, ISBN: 0470383585, October, 2008

Chapter 7 - Dynamic Topology Implementation and Maintenance for the CHORIST Network

This chapter presents a proposal for a stable and efficient solution to implement and manage the structure designed by the CHORIST project [33], taking into account the constraints imposed by the communication model. CHORIST is a European Commission project that addresses environmental risk management focusing on natural hazards and industrial accidents [33].

Some part of this chapter was published in:

- Daniel Câmara, Christian Bonnet, Fethi Filali, Implementation and Dynamic Topology Maintenance for the CHORIST Network, The 20th Personal, Indoor and Mobile Radio Communications Symposium 2009, PIMRC'09, IEEE, Tokyo, Japan, September 13-16, 2009

Chapter 8 - Market Based Strategy

This chapter describes a distributed and flexible mechanism to perform network admission control and topology management for wireless mesh/ad hoc networks in general. The proposed method uses the economy concepts of supply and demand to dynamically organize the wireless network. Topology control for mesh networks, especially for PSNs, is an interesting problem since the needs of two disaster sites, even though using the same kind of equipment and protocol stack, may vary significantly. A network structure that suits perfectly to one site may be unacceptable to another.

Some part of this chapter was published in:

- Daniel Câmara, Christian Bonnet, Topology Management for Public Safety Networks, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany, June 21-24, 2009
- Daniel Câmara, Christian Bonnet, Fethi Filali, Dynamic Topology and Communication Control for Highly Dynamic Wireless Mesh Networks, A Public Safety Network Point of View, Tenth Workshop on Mobile Computing Systems and Applications (HotMobile 09), Doctoral Consortium, ACM Sigmobile, Santa Cruz, CA, February 23-24, 2009

Chapter 9 - Conclusions and future directions

This chapter performs an evaluation of the work highlighting the most important aspects and achievements of the thesis. It also points to some future directions for this work and perspectives for research in the fields concerned by this thesis.

Chapter 2

Public Safety Networks

2.1 Introduction

The greatest part of this thesis is related to the application of the techniques developed to Public Safety Networks (PSNs) environments. The main aim of this chapter is to provide a broad view of the PSN field, presenting the different emergency management phases, PSNs requirements and some of the challenges for this field.

Public Safety Networks are networks established by the authorities to either warn and prepare the population for an imminent catastrophe, or to provide support during the crisis and normalization phases. As shown in Figure 2.1, catastrophes can vary in nature and intensity. PSNs have the fundamental role of providing communication and coordination for emergency operations. Many of the problems of the PSN field come from the heterogeneity of systems and agencies involved at the crisis site and from their mobility patterns within the disaster site.

2.2 Main aspects of Public Safety Networks

The characteristics and requirements of Public Safety Networks may vary considerably depending on their purpose and placement. However, they are always mission critical; once deployed, PSNs have to be reliable since lives may depend on them. As an example, reports from September 11th point

Japan, ship crash - Feb/2/2009
Australia, wild fire - Feb/9/2009
France, storm - Jan/24/2009
China, flooding - June/16/2008
China, earthquake - May/24/2008

Figure 2.1: Different disaster scenarios.

out that communications failures contributed directly to the loss of at least 300 firefighters and prevented good management of the rescue efforts which contributed to the loss of many other lives, [4] [74]. Moreover, communication failures were one of the obstacles in the coordination of the rescue resources in the 1995 Kobe earthquake [72]. These failures further prevented outsiders from receiving timely information about the severity of the damages. The communication breakdowns delayed the relief efforts which could have prevented the loss of numerous human lives.

Reliability of equipments and protocols is a serious matter for any type of network, but it is even more important in the context of PSNs. Maintaining communication capabilities in a disaster scenario is a crucial factor for avoiding preventable loss of lives and damages to property [104]. During a catastrophe such as an earthquake, power outage or flooding, the main wireless network structure can be severely affected and "historically, major disasters are the most intense generators of telecommunications traffic" [104]. The public communication networks, even when available, may fail not only because of physical damages, but also as a result of traffic overload. Therefore, the regular public networks alone are often not sufficient to allow rescue and relief operations [104].

However, equipment failures and lack of connectivity are not the only problems faced in PSNs. Traditionally, PSNs have been owned and operated by individual agencies, such as law enforcement, civil defense and firefighters. Furthermore, they may belong and obey to commands related to federal, state or municipal governments. All these different PSNs are often not interoperable, which may represent a problem in the case of a catastrophe [10]. During the last few years some initiatives, such as MESA [76], have tried to solve the problem of interconnectivity among different agencies.

2.3 Emergency management phases

Disasters can be of different types: natural disasters, such as hurricanes, floods, drought, earthquakes and epidemics, or man-made disasters, such as industrial and nuclear accidents, maritime accidents, terrorist attacks. In both cases, human lives are in danger and the telecommunication infrastructures may be seriously affected or even no longer operational.

Disaster management involves three main phases:

1. **Preparedness**, at this phase all the equipment and people should be ready to enter in action, if needed. It consists of training, equipment maintenance, hazards detection and education.

2. **Crisis**, this phases goes from the break-out point (decision to respond), to the immediate disaster aftermath, when lives can still be saved. Crisis is understood as the society's response to an imminent disaster; it is different from the disaster itself.

3. **Return to normal situation**, this phase consists of the building and maintenance of temporary communication mechanisms/structures while the regular mechanisms are being repaired or rebuild.

2.3.1 Crisis parties

In a situation of crisis the involved parties can be classified in the following way, taking also into account the degree of mobility they need:

- Local Authority(ies); fixed: the group in the administrative hierarchy competent to launch a warning to the population and to the Intervention Teams.
- Citizens; either mobile or fixed: nonprofessional people involved in the crisis.
- Intervention Teams; mobile: professionals (civil servants or militaries) in charge of rescuing Citizens in danger, preventing hazard extension or any time-critical mission just after the break-out of the crisis; in charge of caring for injured people once the crisis is over.
- Risk Management Centre; fixed: group of experts and managers in charge of supervising operations. The Risk Management Centre works in close cooperation with Local Authorities.
- Health Centers; fixed: infrastructure (e.g. hospital) dedicated to caring injured citizen and backing intervention teams as for this aspect of their mission.

2.3.2 Alert phase

It is important to manage properly this critical phase as it is the moment where a quick response is the most efficient in terms of lives and goods saved. This means notifying professionals and people of the incoming hazard. Warning makes sense if there is a delay between the very break-out of the hazard and the damages it could cause. This leaves time for people to escape and avoid the endangered area. Warning the population is typically the Local AuthoritiesŠ responsibility since they are the only ones who can clearly appreciate the danger depending on local circumstances. Deciding that the situation is critical may be taken at governmental, national level. This is the case for example for earthquakes in all European countries.

2.3.3 Crisis handling phase

Coordination of Intervention Teams begins when the crisis breaks out. The Local Authorities alert them just before the population and then transfer the supervision to the Risk Management Centre. Later on, Intervention Teams still receive instructions from their Local Authorities, from the Risk Management Centre and from the Health Centre.

Intervention Teams send back information to Local authorities, to the Risk Management Centre, to Health Centers about the situation and request for help. They typically use a specific purpose network deployed specially to attend to the needs of that particular event. Normally the same network is used for receiving instructions and returning feedback.

2.4 Important factors for Public Safety Networks

A flexible Public Safety Communication infrastructure has some specific requirements that need to be considered within the context of emergency response scenarios [38]. They are summarized in the following sections.

2.4.1 Disaster categories

Disasters differ from each other depending on their scale, which is crucial to consider in designing an appropriate response/recovery system. This can be defined by the degree of urbanization or the geographic spread. Degree of urbanization is usually determined by the number of people in the affected area, which is very important in disaster handling as the impact of the event changes based on the number of people involved and the breadth of spatial dispersion, both of which impact response and recovery from disasters.

Another key factor to consider is whether the disasters have been predicted or not. Clearly, sudden natural or man-made disasters do not give sufficient warning time. Other disasters may give a longer time window to warn people and take appropriate actions. Thus, if there is advance notification, it is potentially possible to set up a better communication infrastructure and possibly even have a backup technology in place before the disaster occurs.

2.4.2 Specific technology requirements

Each kind of disaster site has its own nature and has specific communication needs. For example, the number of attendees, mobility pattern and QoS parameters for a wildfire differ drastically from the ones in an earthquake relief effort. Users also may have different devices such as laptops, palms, or cell phones which may work with different network technologies such as WLAN, WiMAX, WWAN, Satellite, or wired networks. Additionally a communication network needs to be easily configurable and quickly deployable at low cost.

2.4.3 Mobility, reliability and scalability

In order to help emergency personnel to concentrate on the tasks, emergency network should be mobile, deployed easily and fast with little human interference. Therefore devices must be capable of automatically organizing into a network. Procedures involved in self-organization include device discovery, connection establishment, scheduling, address allocation, routing, and topology management. The system should also be able to support large number of users and data load without noticeable impact on the performance.

2.4.4 Interoperability and interdependency

Communication technology provides the tool to send data; however when information is sent over different channels or systems, interoperability may not necessarily have been planned for. First responders should be equipped with devices capable of using different technology by choosing the appropriate interface card and still working together to form a mesh network and communicate data. Therefore, regardless of what technology each individual might use, they are uniformly connected to the relaying mesh nodes and able to exchange data.

2.4.5 Multimedia broadband services

Communications for the benefit of local rescuers, national authorities or international assistance are mainly to coordinate efforts of field teams and connect teams to remote decision-making centers. In particular, retrieving monitoring data from the disaster site and distributing data to local teams or remote expertise centers are important requirements for an emergency communication system. Thus, providing broadband communication capacity during emergency or crisis times is becoming more and more necessary. Concerning services, users' basic requirements are voice and data communications with short and long range capabilities, but users require also multimedia communications with large volume of data able to provide the logistics of the situation, medical data, digital map, blueprints or intelligence data.

2.4.6 Knowledge and training

An important issue to be considered as addressed is the lack of knowledge of exact capabilities of the new technology being deployed and lack of training. The new technology needs to be installed and fully tested in drills and preparation exercises well before it is used in an actual disaster. It is also very important to consider who will be the users of this technology and what level of knowledge and technical background they have. We would like to design future emergency communication tools and public awareness systems to be user-friendly with minimal training requirements, yet also secure.

2.4.7 Warnings and alerts

Warning messages should be provided with the consideration that some people may disregard the warnings, therefore even the well-designed warning system must consider human error or resistance. People may not evacuate to safe areas even if asked or ordered to do so for different reasons such as family, belongings, and pets, or they may not trust the accuracy or source of the warning. They may not take the warning seriously if they hear different messages from different sources, or if the source of the warning has not proven to be accurate or reliable in the past. The warning should provide a clear explanation of the nature of the disaster and appropriate actions to be taken.

2.5 Emergency alert systems

Emergency alert systems (EASs) play an important role in many countries and have also evolved and received considerable investment through time. For example, only in 2009 the budget requested to develop the new American EAS, the Integrated Public Alert and Warning System (IPAWS), was 37 million dollars [36]. IPAWS development is under the responsibility of the Federal

Emergency Management Agency [43]. When complete it will permit the broadcast of emergency messages not only through radio and TV but also by e-mail, cell phones and other different mediums. During a test pilot conducted in 2007 in Alabama, Louisiana, and Mississippi the system was able to send alerts to 60,000 residential phones in ten minutes and also with Spanish and Vietnamese translations [43].

The Japanese nationwide warning system, J-Alert, was launched in February 2007. It uses satellite wireless communication to issue a simultaneous warning to all municipal governments and interested agencies [68]. J-Alert works with warning sirens and an emergency broadcast system. The system is automatically activated and, from the time an emergency is confirmed, it is able to warn the population in less than 7 seconds.

RATCOM project [88], depicted in Figure 2.2, is one of the next generation EAS dedicated to detect and warn of tsunamis in the Mediterranean Sea.

When RATCOM will become operational, sensors will capture data and, if a real anomaly is detected, warning messages will be distributed automatically over the endangered region. The RATCOM alert system is composed of two main components: one ascendant and one descendant. The ascendant component is responsible for sensing the related data, filter false positives and retransmitting the relevant collected information to the coordination center. The descendant component is responsible for spreading the information of the imminent dangerous situation among the authorities and population in general.

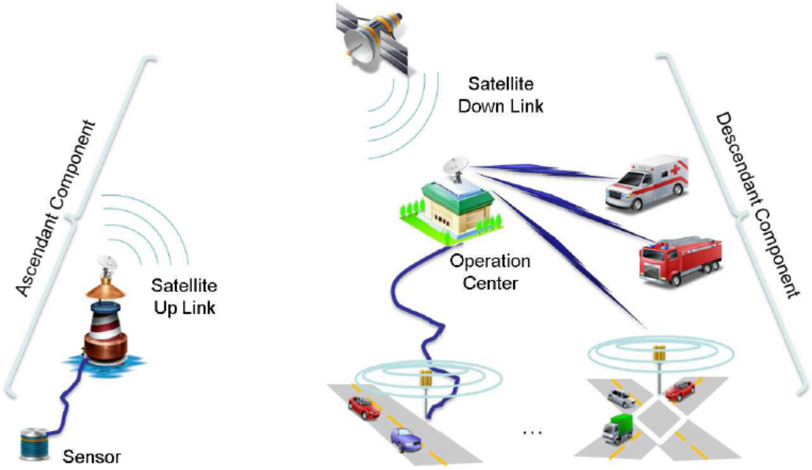


Figure 2.2: RATCOM project main architecture.

2.6 Public Safety Network projects

Public Safety Networks have attracted much research interest in the last few years. This section will present some research projects conducted in the field of PSNs.

The CHORIST project [33] is funded by the European Commission, and addresses Environmental Risk Management in relation to natural hazards and industrial accidents [33]. The backbone topology, presented in more detail in Section 7.2, is composed of Cluster Heads (CHs), Mesh Routers (MRs) and Relay Nodes (RNs). All the nodes' roles must be defined dynamically and based only on local information.

The WIDENS project [108] was a European project that aimed to design and prototype a next generation of interoperable wideband Public Safety

Networks. The project was concluded in 2006 and successfully proposed an easily deployable system for PSNs. Many of the results of the WIDENS project were incorporated in the MESA project.

The MESA project [76] is an international ongoing project in partnership between the European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA) to create a global specification for mobile broadband public safety and disaster response networks. The mobile broadband specifications produced by the MESA project will touch the most different aspects and technologies related to PSNs, from remote patient monitoring to broadband satellite constellations interconnection, passing through mobile robotics and network reliability algorithms.

2.7 MAC layer challenges

Public Safety Networks present many challenges regarding the Medium Access Control and Physical (MAC/PHY) layers. Communication systems for this kind of network must be reliable and robust to failures. A rupture at the MAC/PHY level will compromise the whole purpose of the network. This is also true for any kind of network, but because they may be deployed in highly unstable environments, e.g. wildfire site, robustness is especially important in the context of PSNs. For this reason one of the most important research aspects of the MAC/PHY layer in PSNs is to provide robust and reliable protocols. On the other hand, past PSNs were narrow-band access only, enough for voice communication but not for multimedia applications. However, data-intensive multimedia applications have the potential to greatly improve the quality of the work and efficiency of first responders and relief efforts. For example, being able to download the blueprints of a industrial disaster site, online and on demand, can give to firefighters valuable hints of the best way to proceed during their operations. Wideband access with support for many different classes of Quality of Services (QoS) will be, in the next few years, not only desirable, but also mandatory for PSNs.

Nowadays there are many different wireless technologies in use, the integration and interoperability of such technologies is another big challenge for PSNs. However, the challenge is bigger than only taking care of the integration of the many technologies. The same technology is not necessarily suitable to every environment and every situation, seamless smart control of lower layer adaptation would enable the creation of better and more useful upper layer applications.

2.8 Network layer challenges

2.8.1 Topology control

The deployment and management of nodes for WMNs are challenging problems and they become even more interesting when we consider them in the context of PSNs. Not only PSNs are, by nature, life-critical but they also have strict requirements. Moreover, these requirements may vary significantly for different disaster sites [56]. For example, the number of nodes, people served, mobility pattern and deployment environment for a forest fire fight differs from the ones for an earthquake relief effort. Well-defined and maintained network structure is a fundamental step to enable the creation of efficient higher layer algorithms [85]. Thus topology control becomes a fundamental step for enhancing scalability and capacity of large-scale wireless ad hoc networks [91].

The main concerns in the establishment of public safety networks are rapid deployment and survivability [12]. PSNs must be reliable and endure even when deployed through rough environments. The network organization is a key factor to ensure endurance. In general, for small environments, the deployment of plain mesh networks is the easiest and fastest way to set a network in the field. However, this kind of structure is hardly scalable and appropriate for use on large scale and reliable environments. Structured networks, on the other hand, are more scalable, but the price to pay for this is the creation and maintenance of the structure.

Midkiff and Bostian [77] present a two-layer network deployment method to organize PSNs. Their network consists of a hub, and possible many-purpose specific routers, to provide access to nodes in the field. However, this work presents two characteristics that would be interesting to avoid in the PSN context. First, the hub represents a single point of failure. If something happens to it, all the communication would be down, even between nodes inside the field. It is important for PSNs to be as resilient as possible. The second issue is long range communications, all transmissions must pass through the hub, so the messages may transverse twice the whole network. Sarrafi, Firooz and Barjini [93] also present another interesting algorithm for topology control focusing on the power consumption optimality of the network.

2.8.2 Mobility management

PSNs may involve different equipments used by different Public Safety agencies, which need to move from the coverage of one mobile mesh router to another transparently and seamlessly, relaying on a dynamic, easy to configure and scalable infrastructure at the disaster site. There is an urgent need for a local mobility management scheme for PSNs to support location and handoff management, as well as interoperability between different heterogeneous Public Safety organizations and terminals. Different solutions try to support mobility management in different layers of the TCP/IP protocol stack reference model. IP-based heterogeneous PSNs can greatly benefit of a network layer solution, which provides mobility-related features at the IP layer level without relying on or making any assumptions about the underlying wireless access technologies.

Mobility management enables the serving networks to locate a mobile subscriber's point of attachment for delivering data packets (i.e., location management) and maintain a mobile subscriber's connection as it continues to change its point of attachment (i.e., handover management). Mobile IPv6 (MIPv6) [66] is one of the most representative efforts on the way toward next generation all-IP mobile networks.

Recently, a network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) [50] is being actively standardized by the Internet Engineering Task Force (IETF) NETLMM working group. It is starting to attract considerable attention among the telecommunication and Internet communities and we believe it has great potentialities in the field of PSNs. With PMIPv6 the serving network handles the mobility management on behalf of the Mobile Node (MN); thus, the MN is not required to participate in any mobility-related signaling. No requirement for modifications on Public Safety terminals is expected to accelerate the practical deployment of PMIPv6 for PSNs as any type of equipment from rescue teams can be used. Moreover, as the serving network at the disaster site controls the mobility management on behalf of the Public Safety users, the tunneling overhead as well as a significant number of mobility-related signaling message exchanges via wireless links can be reduced. Moreover, the handover latency is also massively reduced due to the fact the terminals keep their IPv6 addresses independently from their points of attachment to the deployed network, thus eliminating the procedures of Duplicate Address Detection (DAD), which represents one of the most time-consuming phases during handoff. Taking into account all these considerations, PMIPv6 may become an important candidate for mobility management in PSNs [59].

2.9 Application layer challenges

PSN still lack a uniform and complete solution to ensure the equipments, and applications, used by the rescue teams will always be connected to a secure and reliable communication infrastructure. The main problem comes from the fact that the IP address is used for describing the topological location of the host and, at the same time, to identify the host.

The Host Identity Protocol (HIP) [78] is a promising new basis for a secure mobile architecture for future PSNs [59]. The cornerstone of HIP is the idea of separating a host's identity from its present topological location in the Internet. HIP introduces a Host Identifier (HI) for each MN and a new layer between the network and the transport layer. In HIP, the transport layer connections are bound to the Host Identity Tag (HIT), a 128-bit hash of the HI, and no longer to the IP address. This simple idea provides a solid basis for mobility and multi-homing features [82]. HIP also includes security as an inherent part of its design, because its host identities are cryptographic keys that can be used with many established security algorithms and cryptographic identities are used to encrypt all data traffic between two HIP hosts by default.

2.10 Conclusions

This chapter provided a broad view of the PSNs field explaining the emergency management phases, challenges and highlighting some research projects in this field. Public Safety Networks play an important role in every one of the emergency management phases and, because lives may depend on them, PSNs are mission critical. They are a growing research field, which considers all the phases. This is due to the fact that, not only there are still many open problems that need to be solved, but also researchers are always trying to find better ways to improve the available infrastructure at the disaster site to provide faster and better solutions to detect hazards, manage crisis and return to the normal situation.

Part II

Alert Phase Support

Chapter 3

Vehicular Disruption Tolerant Networks

During the alert phase it is of paramount importance to reach the vast majority of the concerned population as fast as possible. Our solution makes use of Disruption, or Delay, Tolerant Network (DTN) techniques to improve the message spreading process. This chapter presents a broad overview of DTNs, particularly focusing on Vehicular DTNs (VDTNs). Even though the proposed techniques could also be implemented in a Packet Switched Network the main characteristics and challenges remain basically the same for both Packet Switched and VDTN.

3.1 Introduction

Traditional networks suppose the existence of some path between end-points, short end-to-end round-trip delay time and small loss ratio. Today, however, new applications, environments and types of devices are challenging these assumptions. In Disruption Tolerant Networks, also called sometimes opportunistic networks, an end-to-end path from source to destination may not exist. In this environment nodes can still connect and exchange information, but in an opportunistic way.

Delay Tolerant Networks have been developed as an approach to building architecture models which are tolerant to long delays and/or disconnected network partitions when delivering data to destinations. This chapter discusses the characteristics of these architectures, and many of the protocols developed to ensure packet delivery in these networks. We henceforth use DTN to refer to Delay Tolerant Networking, Disruption Tolerant Networks and Opportunistic Networks. For Vehicular DTN, the acronym VDTN is used.

The vehicular network research field, and more specifically the VDTN research field, have attracted great attention in the last few years. Initiatives such as the i2010 Intelligent Car Initiative Intelligent Car (2009) aim to decrease the number of accidents and CO_2 emissions in Europe, utilizing sensors and vehicle-to-vehicle (V2V) communication. As part of these projects, cars equipped with wireless devices will exchange traffic and road safety information with nearby cars and/or roadside units. In fact, according to the ETSI 102 638 technical report [41], by 2017 20% of the running vehicles will have wireless communication capabilities. The same report estimates that by 2027 almost 100% of the vehicles will be equipped with communication devices.

The design of the core Internet protocols is based on a number of assumptions: these include the existence of some path between endpoints, short end-to-end round-trip delay time, and the perception of packet switching as the right abstraction for end-to-end communications. Furthermore, the efficiency of these protocols is based on assumptions about the resources available to the nodes and the properties of the links between them. Traditionally nodes are considered to be fixed, energy unconstrained, connected by low loss rate links, and communication occurs through the exchange of data between two or more nodes. Today, however, new applications, environments and types of devices are challenging these assumptions and call for new architectures and modes of node operation. Some of these challenges are: intermittent and/or scheduled links, very large delays, high link error rates, energy-constrained devices, with heterogeneous underlying network architectures and protocols in the protocol stack, and most importantly, the absence of an end-to-end path from a source to a destination. Applications on the following environments may pose such challenges: spacecrafts, planetary/interplanetary, military/tactical, disaster response, mobile sensors, vehicular environments, satellite and various forms of large scale ad hoc networks. The variety of these applications, the impossibility of having a fixed wired Internet infrastructure everywhere, and the inclusion of mobility in most of these applications, make these challenges more difficult to surmount. This leads us to a new approach of designing networks, taking into account several constraints and characteristics, using DTN.

3.2 Background

VDTNs have evolved from DTNs and are formed by cars and supporting fixed nodes. Fall [42] is one of the first authors to define and discuss DTNs' potential. According to his definition, a DTN consists of a sequence of time-dependent opportunistic contacts. During these contacts, messages are forwarded from their source towards their destination. This is illustrated in Figure 3.1. In the first contact the origin sends the message to A in time t_1, then A holds the message until it is delivered to the destination in the contact at time t_2.

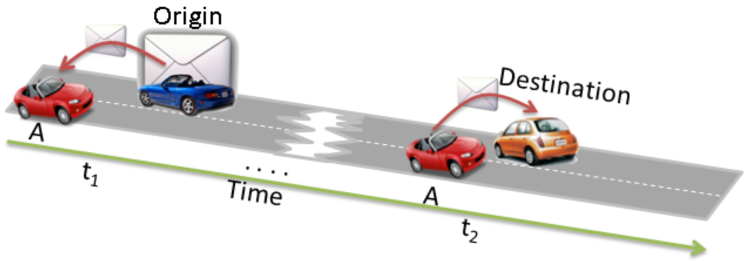


Figure 3.1: A representation of two communication opportunities in a VDTN

Contacts are characterized by their start and end times, capacity, latency, end points and direction. The routing algorithm can use these pieces of information to decide the most appropriate route(s) to deliver a message from its source to its destination. However, routing in a network where the edges among the mobile nodes depend on and vary in time is not a straightforward task. One needs to find an effective route, both in time and space. All nodes along the path should consider the nodes' movement pattern and the possible communication opportunities for message forwarding. Unfortunately, it is not always easy to determine future communication opportunities or even forecast the mobility patterns of the nodes in the network.

Cerf et al. [26] characterizes contacts as:

- Persistent: When they are always available, i.e. a Cable modem.
- On-Demand: When they require an action to start, but after that they work as persistent contacts, for example, a dial-up connection.
- Intermittent scheduled: When the parties involved agree to meet at a

specific location for a determined period of time, i.e., low earth satellite communication window.

- Intermittent opportunistic: Contacts that occur unexpectedly, for example, a car passing by in a non scheduled manner.
- Intermittent predicted: When the contacts are not based on a schedule, but on predictions. A prediction is a contact that is likely to happen, based on the history or other kind of information.

  However, there are no guarantees predicted contacts will actually happen. For example, when people are commuting to work, it is probable that at the same time the same contacts are available, because people normally go at the same time and take the same routes.

Forwarding and routing strategies may vary significantly according to the type of contacts a node, or a network, is expected to encounter. In the case of a DTN with intermittent contact opportunities, the main priority is to maximize the probability of message delivery, and to minimize the end-to-end delay. For networks with more stable and consistent contact opportunities, it is important to discover an efficient path while trying to save as much as possible of the network resources. In a scenario with deterministic message routing and persistent, on-demand or intermittent but scheduled contacts, we may have a chance to achieve optimal performance of the network and manage efficiently the available resources, i.e. spectrum and node energy. However, this is not frequently the case for mobile networks.

Under unpredictable intermittent network conditions, where the mobility obscures present and future topology, nodes can only forward packets randomly based on the likelihood they will eventually arrive to their destination. Then, the problem of delivering messages to their final destination is paramount and dominates that of resource utilization. In this case, flooding and epidemic message-forwarding are popular approaches. Between the two extremes, deterministic contacts and fully opportunistic ones, a broad range of strategies may be used to balance message delivery and resource optimization. Another issue to keep in mind is the duration and bandwidth of contacts. In a vehicular network, the number of contacts may be high, but the duration of each one can often be expected to last only seconds, especially between cars moving in opposite lanes. This significantly limits the amount of information exchanged between nodes.

In 2002 the Internet Research Task Force (IRTF) [63], started a new group called Delay-Tolerant Networking Research Group (DTNRG) [40]. The group was first linked to the Interplanetary Internet Research Group

(IPNRG) [62], however, it soon became clear that the main characteristics of DTNs, i.e. non-interactive, asynchronous communication, would be useful in a broader range of situations. The main aim of DTNRG is to provide architectural and protocol solutions to enable interoperation among nodes in extreme and performance-challenged environments where the end-to-end connectivity may not exist. E.g. public safety, underwater, sensor and adhoc networks and extremely degraded connectivity, such as country side networks, to name a few.

3.3 Challenges and techniques

The conditions of DTN operation lead to an architecture that challenges the traditional concepts of most of the network layers. In this section we present some of the major challenges faced by DTN protocols at different network layers. Standard network modeling techniques are also challenged and new ways to model nodes and connections should be created to evaluate the considered protocols. Therefore this section also discusses the different network modeling, traffic modeling, transport layer issues, routing and data dissemination strategies.

3.3.1 Routing

The challenges that DTNs need to overcome have lead the research to heavily focus on routing issues. Routing is considered to be the problem of choosing forwarding strategies that enable messages to pass from the source to the destination. The issues presented in this section pertain to most of the network layers and techniques developed for DTNs. For the case of VDTNs, *store-and-forward*, or *store-carry-and-forward* techniques are used [99]. This means that the nodes which receive a message, store it for some time, possibly carry it to another location, and afterwards forward it to other nodes. This is not new, in the Internet nodes also often momentarily buffer packets as well. However, in this case, nodes try to decrease as much as possible these time intervals. On the other hand, in DTN the storing is used to overcome absence of end-to-end connectivity, and to enable waiting until efficient connections are present. In the *store-and-forward* mechanism each intermediate node is in charge of verifying the integrity of the message before forwarding it. In general, this technique helps us cope with intermittent connectivity, especially in the wilderness or environments requiring high mobility, and may be preferable in situations of long delays in transmission and variable or high error rates.

Mundur and Seligman [79] identify mainly two classes of routing algorithms for DTNs. The first class is based on epidemic routing, in which nodes use opportunistic contact to infect other nodes with the message to be delivered. For this group, the need of network knowledge is minimal. The routing algorithms have no control of node mobility and the forwarding process occurs in a fortuitous way. The second class of algorithms utilizes topology information and the algorithms may control node mobility. For Mundur and Seligman [79], this case is characterized by ”islands” of well-connected nodes with intermittent connectivity with other nodes.

Routing issues

Fall [42] and Jain, Fall and Patra [64] present an interesting list of routing issues for DTNs:

- Routing objective: Although the main objective of a routing algorithm is message delivery and DTNs are, by definition, tolerant to delay, that does not mean we should not try to decrease the delay as much as possible. Algorithms should attempt to find a good tradeoff between decreasing the end-to-end delay and saving network resources.

- Reliability: The protocols should be reliable and provide some form of mechanism to inform the nodes that their messages reached the destination. Acknowledged message delivery is an important enhancement of the offered set of services.

- Security: In all types of networks, security is an important factor. However, in DTNs the packets may cross a diverse path to reach the destination and stay for a relatively long time at each intermediate node. The reliability and intentions of the often numerous intermediate nodes may not be always the best ones. Mechanisms to provide message authentication and privacy of the messages’ content are of supreme importance.

- Resource allocation: Normally the main routing objectives of maximizing the message delivery ratio and minimizing resource allocation are conflicting. The easiest way to guarantee the message delivery in the smallest amount of time is flooding the network with the message. However, this means a high use of network bandwidth, nodes memory and processing power. These may lead to other problems such as packet collisions, packet drops because of full message queues and surely the waste of the limited amount of energy of the nodes.

- Buffer space: Considering the disconnection problem, messages may be stored for a long period of time before they can be forwarded. The buffer space must be enough to maintain all the pending messages, i.e. messages that have not reached their final destination yet.

- Contact scheduling: The forwarding waiting time is one of the principal elements on DTNs. It is not always clear how long a node will need to keep a message to enable its forwarding. This period may vary from seconds to days.

- Contact capacity: Not only is it not always possible for the contacts to be predicted, but when they do occur, they may be brief. The protocols should take this into account and try to minimize, as much as possible, the use of the spectrum and time with control messages.

- Energy: Mobile nodes may have limited amount of energy and, possibly, difficult access to power sources. Normally, for VDTNs the energy is a factor to be kept in mind but it is not one of the main factors since the vehicle can normally provide enough energy to maintain the communication system.

Evaluation metrics

To evaluate the routing algorithms for DTNs Jones [67], and Sanchez, Franck and Beylot [90], propose the utilization of:

- Delivery ratio: Jones [67] defines delivery ratio as ”the fraction of generated messages that are correctly delivered to the final destination within a given time period”.

- Latency: Even though the networks and applications are supposed to endure delays, many applications could take advantage of shorter delays. Even more, some applications have time windows of delay resilience, i.e. messages are valid for a certain amount of time, after that the message loses its validity.

- Transmissions: The number of messages transmitted by the algorithms varies and some, that create multiple copies of the message, may send more messages than others.

- Lifetime: Route lifetime is the time a route can be used to forward packets without the need for re-computation.

- End-to-end delay: This evaluation criterion is the time it takes for one message to go from the origin to the destination.
- Capacity: Capacity is the amount of data that may pass through one route during its lifetime.
- Synchronicity: Even in a delay tolerant network, it is possible that, during some intervals, origin and destination are close and the communication may occur directly, or similarly to communication in traditional wireless networks; Synchronicity measures how long this situation where classical communication is possible.
- Simultaneousness: This criteria measures the contact durations, i.e. the time intermediate nodes are in the same area.
- Higher-order simultaneousness: Simultaneousness is computed hop-by-hop. However, the same concept may be applied to a series of nodes. Higher-order simultaneousness is the application of the simultaneousness criteria to k consecutive nodes that are part of the complete path.
- Discontinuity: Discontinuity is the normalized duration of packet storage through the path.

Routing strategies

Recently, Shen, Moh and Chung [95] presented a compact and interesting list of routing strategies for DTNs. Like Mundur and Seligman [79] Shen, Moh and Chung [95] also divide the routing protocols in two families; flooding and forwarding. Flooding strategies are the ones where nodes create copies of the packet and forward to more than one node. Forwarding strategies use the knowledge of the network to select the best paths. A comparison between the generic behavior of flooding and forwarding strategies is depicted in Figure 3.2. Note that flooding strategies result in a significantly higher number of messages compared to forwarding.

Flooding based strategies

One of the simplest possible forwarding strategies is called Direct Contact. In this strategy the node waits until the source comes in contact with the destination before forwarding the data. Jones [67] considers direct contact as a degenerate case of a forwarding strategy. Even though this strategy does not multiply messages, it is considered flooding. The reason is that it does not make use of any topology information the nodes possess. The strategy is simple and presents low resource consumption; however, if the contact

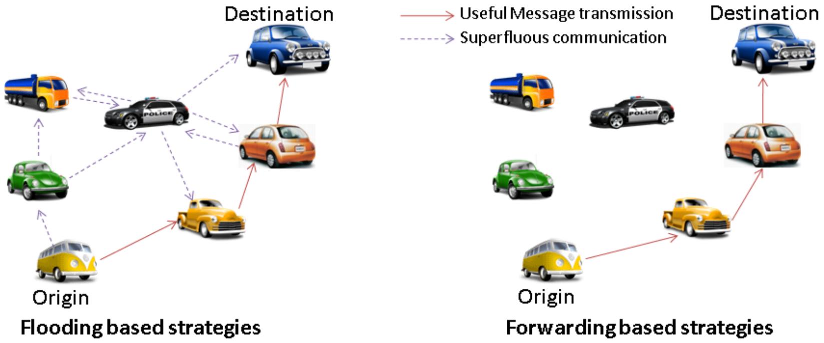

Destination
Useful Message transmission
Superfluous communication
Destination
Origin
Flooding based strategies
Origin
Forwarding based strategies

Figure 3.2: Message transmission example comparing flooding and forwarding based strategies

opportunities between source and destination are low, then the delivery rate can also be low.

In the Two hop Relay strategy [67], the source copies the message to the first n nodes that it contacts. These nodes relay the message until they find the destination, it is similar to direct contact, but now not only the source keeps the message, but also n copies of the message are spread among other nodes. With this we increase the required resources, but also the expected delivery ratio. Figure 3.3 illustrates both techniques.

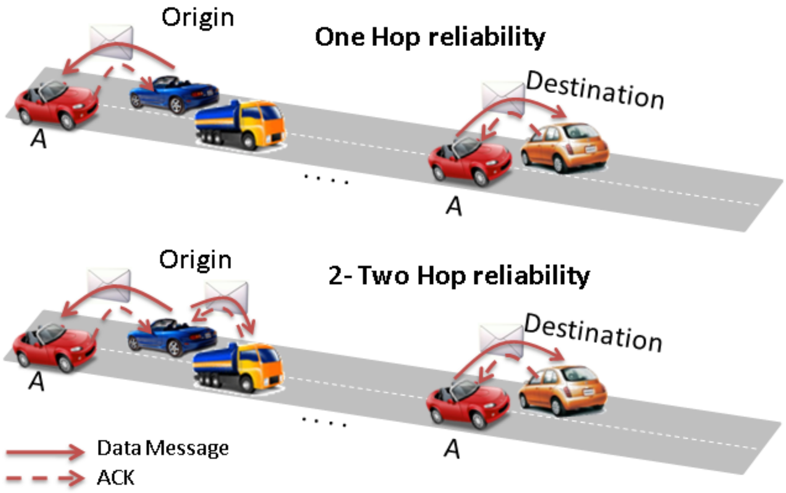


Figure 3.3: One hop reliability and two hop reliability techniques

The tree based flooding strategy of [67] extends the idea of direct contact further in the sense that now all nodes that receive the message may create n copies of it. The message tends to propagate through the network in a controlled flooding that resembles a tree.

Epidemic routing [105] consists of the spreading of the message similarly to that of a virus in an epidemic situation. Each node that receives the message rebroadcasts it to every other node it encounters. The contaminated nodes just keep one copy of the message. This approach is extremely effective, but presents a high resource consumption rate.

Ramanathan et al. [87] present a prioritized version of epidemic routing. This technique imposes a partial ordering on the messages based on costs to destination, source, and expiry time. The costs are derived from link availability information. The technique successfully maintains a gradient of replication density that decreases with increasing distance from the destination. Even though it is also a resource intensive technique it presents lower costs and higher delivery rates than simple epidemic routing.

Forwarding based strategies

Location based routing [67] techniques use geographical information, such as Global Positioning System (GPS) data, to forward data. This strategy is the forwarding one that demands the smallest amount of knowledge of the network structure. With the position information they can estimate the costs and direction to forward the messages.

Source routing strategies calculate the whole path at the origin, prior to sending the packet. This kind of strategy needs to have a fairly consistent view of the network to work properly. On the other hand, in per-hop routing [67], the decisions of which path to take are done on a hop-by-hop basis when the message arrives at each hop. Instead of computing the next hop for each message the per-contact routing technique recomputes its routing table each time a contact arrives and its knowledge of the network increases.

Instead of routing with global contact knowledge, Liu and Wu [71] propose a simplified DTN model and a hierarchical routing algorithm which routes on contact information with three combined methods.

3.3.2 Data dissemination

Data dissemination refers to data-centric communications protocols. The Data Mule project [94] and the Message Ferrying scheme [103], are two of the most well-known data dissemination algorithms for DTNs. They were designed for sensor networks. They propose the use of mobile nodes to collect data from the sensors, buffer it, and deliver the collected data to a sink.

The MULEs (Mobile Ubiquitous LAN Extensions) and ferries utilize nodes navigating through the sensor network to collect data in 'mobile caches'. According to the Data Mule project, all the nodes are fixed and only the cache is mobile. Message Ferrying [103] also considers mobile nodes, but in this approach the nodes are required to follow specific paths and even move in order to help message delivering.

The SPAWN protocol introduced by Das et al. [37] and Nandan et al. [80] discusses how vehicles should interact to accommodate swarming protocols, such as BitTorrent traffic. In SPAWN, the nodes passing through Access Points (APs) collect data that they subsequently exchange with nearby nodes. Nodes are often required to carry traffic useless to them and the BitTorrent protocol is bandwidth intensive, however, swarming protocols is an interesting and effective way for message dissemination among nodes in VDTNs.

3.3.3 Transport issues

The greatest part of the research for DTNs has focused on routing and data dissemination algorithms. However, many other aspects present interesting and valuable challenges. The transport layer is certainly one of the layers that need special attention. Most of the services offered by existing transport layer protocols, such as TCP, have been ignored. For example, end-to-end connections, sequencing, congestion control and reliability are some of the most important features of the TCP protocol. Some of these services may be easily implemented in DTNs while others will require a fair amount of future research. We will focus here on reliability approaches to ensure message delivery on the DTNs.

Hop-by-hop reliability [42] is the most basic and simple reliability strategy to ensure data delivery in DTNs. Each time a node receives a message, it sends an acknowledgement (ACK) of its reception and after that assumes the responsibility for this message across a defined region. For this case an end-to-end ACK is not possible, unless it is a completely new message generated by the destination. The lack of end-to-end reliability of the hop-by-hop approach may be a problem for a series of applications. One way to overcome this problem is the use of Active Receipt [52]. Active receipt is basically an end-to-end acknowledgment created by the destination, addressed to the source of the original message. The receipt is actively sent back through the network. In truth it is a new message that is propagated through the network. Active receipts solve the problem of end-to-end reliability but the price to pay for it may be too high in some situations.

Passive Receipt [52] is another method created to provide end-to-end reliability at a lower cost. The high price of the Active Receipt comes from the generation of two messages in the network instead of just one. To use the terminology of epidemic routing, now we have two messages infecting nodes instead of just one. In this case what Passive Receipt introduces is exactly the concept of an implicit receipt, instead of an active one. The destination, instead of creating a new active receipt, creates an implicit kill message for the first one. The kill message works as a cure for the infected nodes, when they receive this message they know that the message arrived to the destination and that they do not need to rebroadcast the original message anymore. This can be observed in Figure 3.4 - Passive receipt, where the police car does not rebroadcast message 1 after having received message 2. The message is rebroadcast only if the cured nodes meet other node that is re-broadcasting the original message, which is the case of the truck and all previous nodes on that specific path of Figure 3.4. This technique presents a lower flux of messages than the one generated by the active receipt, and the end-to-end reliability is guaranteed, since eventually the source will also receive the passive receipt.

An interesting solution for end-to-end reliability is also proposed by [52] and takes advantage of the number of multiple network infrastructures available nowadays. On the Network-Bridged Receipt approach the nodes may use a different medium access mode to deliver ACKs. For example, while the cell phone network may not present the required data rate for a specific application, or even present a high cost. The cell network may present more than reasonable bandwidth, at a cost effective, to send small ACK messages.

Figure 3.4 presents a schematic description of the reliability approaches presented here. We can see that the number of messages and nodes involved in each one of the techniques vary considerably.

3.4 Modeling techniques for VDTNs

Analytical studies perform an important role in the evaluation and, in consequence, in the development of protocols in every area. Vehicular delay tolerant networks are no different. However, as the constraints of DTNs are somehow particular, compared to traditional wired and wireless networks, the same analytical models and constraints used for the latter may not hold for a DTN environment. An analytical model, or study, "is a proven approach for studying system performance, revealing underlying characteristics, and evaluating communication protocols" [107]. Theoretical works, like the one

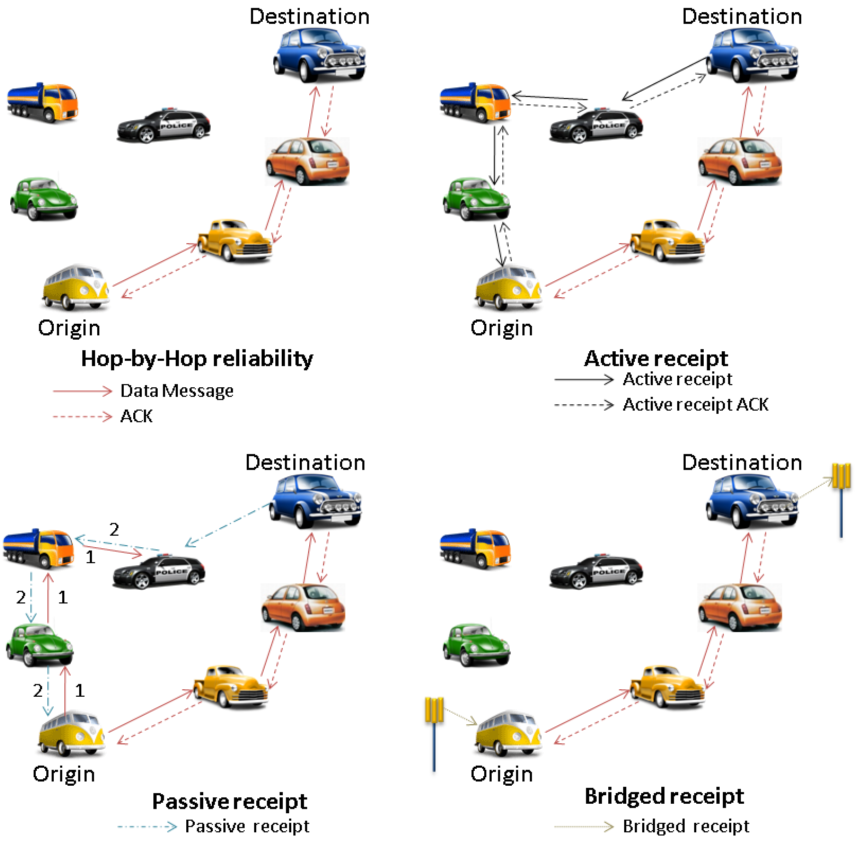


Figure 3.4: Comparison among the reliability approaches messages

of Niyato, Wang, and Teo [83], provide the indication and comparison basis for other simulation or test-beds experiments. Many factors may influence the analytical results of an experiment, e.g. node density, capacity, physical and medium access control characteristics. However the three main factors are: mobility model, data delivery scheme and queue management [107].

3.5 Mobility models

Different DTNs may have different mobility models and mobility directly influences the network structure. The way nodes move, or do not move, may affect: the retransmission delays, frequency of contacts among nodes and energy decay. Mobility can either provide the opportunity for new high quality contact or lead to the breaking of links already established.

Apart from static placement of nodes, probably the simplest mobility model is the Random Walk-based model [117]. In this mobility model nodes choose random points in the area considered and move towards these points at random speeds. The three basic steps for a random way point algorithm, as described by Bettstetter et al. [15] are: first the node chooses randomly a destination, after that it goes towards that destination at a random speed, and finally it waits for a random period of time at the destination point. Some minor variants of this process are also possible, for example Spyropoulos et al. [100] consider random directions instead of positions, but in the end the basic concept is the same.

Some techniques use different well known distributions to control the movement of the nodes. The main advantages of using these distribution based mobility models are that, not only the mathematical model of a well known distribution is easy to implement, but also it is easy to analyze the network behavior afterwards. For example, knowing the nodes distribution makes it easy to calculate the probability of a node crossing a specific network area. Some commonly used distributions are: Normal, poison and exponential.

Markovian mobility models are also a popular choice to model mobility. The main goal of using Markov chains is to create more realistic movement models [32] [22] with real drivers actions, such as motion in the same direction and in adjacent directions, acceleration, stops and sharp turns.

Another model designed to provide realistic mobility patterns, introduced by Haerri, Bonnet and Filali [51] is Kinetic Graphs. This method tries to capture the dynamics of mobile structures and accordingly develop an efficient maintenance for them. Unlike static graphs, kinetic graphs are assumed to be continuously changing and edges are represented by time-varying weights. Kinetic graphs are a natural extension of static graphs and provide solutions to similar problems, such as convex hulls, spanning trees or connected dominating sets, but for continuously mobile networks. This mobility model is implemented in a tool called VanetMobiSim [45], that can generate realistic mobility patterns.

3.6 Delivery schemes

Direct transmission and flooding [106] are two of the most simple delivery schemes possible. In direct transmssion a node simply transmits the message directly to the destination. In flooding schemes it transmits the message to all other nodes it may encounter. The analysis of both schemes is simple since the node behavior is straightforward to predict.

Epidemic dissemination schemes are also extremely popular for VDTNs. For example, the Shared Wireless Infostation Model (SWIM) presents an epidemic Markov dissemination scheme [98]. The scheme is further analyzed and refined in [99]. Wang et al. [107] present a more diverse description of dissemination models.

3.7 Queue management

The way nodes manage their queues is also a determining component in the performance of algorithms for VDTNs. The way one models the queues determines, among others, the way nodes will discard old messages and this in consequence will, possibly, affect the network delivery ratio. The generic queuing analytic framework introduced by Wang et al. [107] is a good starting point for a simple queue model for VDTNs. The models described by Wang have either infinite or finite buffer space. For the infinite buffer space the node's queue is considered to have infinite length. For the finite buffer space it is assumed that each node may hold at most k messages in the queue.

Niyato et al. [83] present an analytical queuing model based on discrete time Markov chains. This work also proposes models for queue performance measures for VDTNs. The proposed performance measures are: Average Number of Packets in Queue of a Mobile Router, Throughput and Average Packet Delivery Delay.

3.8 Applications

One of the main focuses of research in VDTNs in the last few years has been the use of VDTNs in road safety applications. Research such as Xu et al. [111] evaluates the feasibility of using dedicated short range communication to warn vehicles about road accidents. Yang et al. [113] propose the use of V2V to warn vehicles about road conditions and demonstrate the potential of DTNs for real life applications.

3.9 Conclusions

DTN is a young and expanding field. VDTN has also a huge potential because of the imminent appearance of vehicular devices capable of wireless communications. These will operate in a very demanding environment, with intermittent connectivity, where an end-to-end path may not always be present. Even though routing and data dissemination have been the focus of research, areas such as security, topology management, transport layer issues, and higher protocol level concerns are equally important. They present problems that will need to be addressed in the near future. DTN and in particular VDTN is an attractive research field exactly because, in order to achieve the envisioned future of ubiquitous connectivity, we need a solution for these open problems.

Chapter 4

Virtual Access Points for Mobile Communication

This chapter presents a simple yet efficient dissemination algorithm called Virtual Access Points (VAPs). This work focuses on the problem of data dissemination in Infrastructure-to-Vehicle (I2V) and Vehicle-to-Vehicle (V2V) communication modes. The main objective of the technique, that can be used to spread public safety warning messages, is to extend the I2V network to areas where regular access points are not deployed. The technique is based on the DTN concept and the nodes exchange messages in an opportunistic way. When a vehicle moves near an Access Point, and receives a message, this vehicle becomes responsible for re-broadcasting it over the uncovered areas. This behavior is exemplified in Figure 4.1, where node A receives a message from the AP and afterward rebroadcasts it in a non-covered area.

4.1 Introduction

In the future pervasive wireless world, all roads and cities will be covered by roadside base stations and access will be provided to both pedestrians and vehicular users. However, for the moment, roadside units (RSUs), or Access Points (APs), are not always present, or may have been damaged as a result of a disaster. Furthermore, ”historically, major disasters are the most intense generators of telecommunications traffic” [7]. The public communication

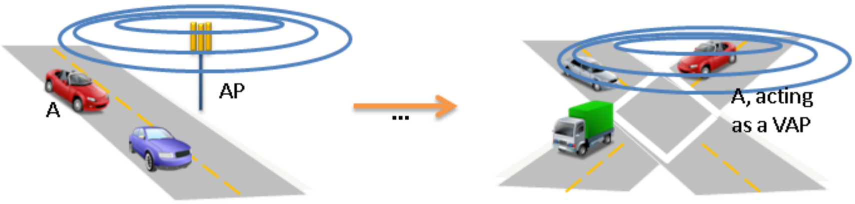


Figure 4.1: The VAP data dissemination technique

networks, even when available, may fail not only because of physical damage, but also as result of traffic overload. Therefore, the regular public networks alone are often not sufficient to allow rescue and relief operations [7].

For these reasons new and specific purpose mechanisms are required to ensure communication during catastrophic situations. With the occurrence of uncovered areas, the only possible communication mode is from one vehicle to another. This work relies on the existence of infrastructure-to-vehicle (I2V) and V2V communication to spread public safety messages among users over a defined region.

As introduced in Section 3.1, the next generation of cars will have radio capabilities. The method proposed here intends to take advantage of such capabilities to extend the coverage of emergency alert systems. Emergency warning messages are not frequent, but when they are issued they must be spread as fast as possible to all the people in the affected region. In this situation all the available means should be used to increase the awareness of the population regarding the imminent threat. We propose here that the available RSUs/APs act in partnership with regular vehicles to help on the spreading of messages that could be, for example, EAS warning messages in case of an emergency.

The proposed technique is called Virtual Access Points (VAPs) and it is a simple, yet powerful, technique to extend coverage to nodes outside covered areas. We consider a system like the one proposed by the RATCOM project [88], depicted in Figure 2.2. In the next generation of EAS, sensors will capture data and, if a real anomaly is detected, warning messages will be distributed automatically over the endangered region.

The RATCOM alert system is composed of two main components: one ascendant and one descendant. The ascendant component is responsible for sensing the related data, filtering false positives and retransmitting the relevant collected information to the coordination center. The descendant component is responsible for spreading the information of the imminent dangerous situation among the authorities and population in general. This work focuses on this last phase: we try to increase the awareness of the general population of the imminent danger using the wireless medium and V2V communication.

4.2 Virtual Access Points for mobile communication

4.2.1 Protocol explanation

The main focus of the Virtual Access Point technique is to decrease the areas not covered by roadside APs so as to minimize the problem of intermittent access to mobile nodes. If we are able to decrease this problem, then even stream traffic for mobile users may be enabled. This work is based on opportunistic node contact. The proposed protocol prime for the simplicity as the duration of the contact opportunities between mobile nodes tends to be small. Chaintreau et al. points that for human mobility patterns the contact duration follows a heavy tailed distribution [27] [28]. They observed that the fast contacts are the most common ones among nodes in real world mobility patterns.

The protocol can be summarized as follows. Each node, after receiving a message, caches it and can thus later become a VAP, acting in a similar way to a relay node. Note however that, instead of just resending the messages, the VAP stores the message and may send it more than once or not at all depending on the caching strategy and depending on the locations has it passed by. VAPs strive to supplement the lack of real APs in a given area broadcasting messages received previously from other AP or even VAPs. A node acts as a VAP if it is neither in the range of an AP nor of a VAP and its distance from the nearest AP is $2r$, where r denotes the AP transmission range. This in practice means that a node is allowed to act as a VAP only when it is at a distance where its MAC layer does not detect any APs above a very low SNR and where it will not interfere with the signal of other APs. We also assume that the MAC layer takes care of solving conflicts and of treats the medium access problem. This application is just one of possibly many others running in the network: this is why the number of messages of the stream application is controlled.

In case a node senses another node acting as VAP in the same region, it gives up being a VAP, even if it lies in an area where it could act as one. Therefore, the first node to broadcast VAP messages in a given region becomes the VAP for that time interval. Nodes are not allowed to act as VAPs during two consecutive time intervals. The high level VAP algorithm is presented in Algorithm 1.

Algorithm 1 - The VAP high level algorithm, from the point of view of a mobile node that can act as VAP

```
// At each time interval
if (Received a message && message is from an AP/VAP) then
    Stores the message in the cache;
    if (cache is full) then
        Throws away the oldest message;
        Stores the new message;
    end if
end if
// Verifies if will act as a VAP or not
if (node has messages in the cache && node is in a position where it could became
a VAP && node was not a VAP in the last round && it did not receive any message
from other VAPs this round) then
    Randomly chooses either to becomes a VAP or not;
    if (node become a VAP) then
        Chooses, from the cache, the message(s) to rebroadcast;
        Rebroadcasts the chosen message(s);
    end if
end if
```

Figure 4.2 shows a typical scenario where a vehicle A acts as VAP providing access to vehicle C. Vehicle D that is receiving a new message from the AP will also, at some point in the future, rebroadcast this received message to the nodes spread over the uncovered area. For all practical purposes we consider that there is no difference between the messages received from a road side AP or a VAP. The propagation mechanism is cooperative and transparent, from the point of view of the receiver. The system is a best effort one; there are no guarantees that every node will receive all stream packets, but using VAPs, we aim to increase the chances for timely reception.

Even in case of a severe catastrophe, or a huge terrorist attack it is unlikely that all the RSU's would break down at the same time. We consider that some RSU will be able to rebroadcast the warning message to the population. After that, the vehicles that received the warning will also be able to spread this information to the other vehicles on their path, which in their turn may do the same. As explained in Sections 3.3.1 and 3.3.1, this kind of propagation scheme is normally referred in the literature as epidemic and nodes act in a *store-carry-and-replicate* paradigm [99].

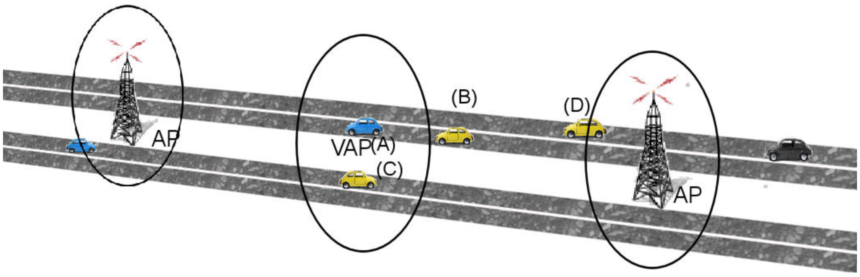


Figure 4.2: The VAP technique on a road coverage vision

To decrease the waste of resources and avoid medium access problems, vehicles act as VAPs only when they are out of the range of a real AP and if they have not received any communication from another VAP during this time slot. In the case of a disaster scenario, this kind of cooperative behavior may be the only way to disseminate useful and general information through the network.

4.2.2 Analysis

As we will see in Section 4.3 the technique successfully decreases the uncovered areas, but it has a cost. The cost can be measured in terms of the increase in the number of messages sent through the network. Consider the target message as a limited size stream being generated at a constant bit rate (CBR): this means that during each second n packets, from the total message size (η), are generated from a source and spread through all real APs. Each AP then is in charge of re-broadcasting the received message to the nodes in its area. Assuming that part of the message is transmitted from each antenna just once, the increase in the number of messages sent (im) is upper bounded by:

$$im = \alpha - (nVAP * \eta), \tag{4.1}$$

where α is the total number of exchanged messages and may be expressed as:

$$\alpha \leq \beta = (nVAP * \eta) * t, \tag{4.2}$$

where β is the maximum number of exchanged messages in each interval of time, $nVAP$ is the number of virtual roadside units, η is the size of the warning message and t is the time the warning message is propagated. The minimum possible number of packets in the network is given by the number of mobile stations in the region times the size of the message. I.e. each vehicle received the complete warning message just one time. This would be possible, for example, if the whole area was covered by RSUs. However, with a distributed communication algorithm this value is hardly achievable. However, it is clear that the number and locations of the RSUs will greatly affect the system performance. The points where vehicles will act as VAPs are directly related to the deployment of the RSUs. Well deployed RSUs can provide faster and more efficient message spreading over the target region.

Using the technique described in [19] we formally verified the VAP protocol behavior prior to its simulation. Our aim was to verify whether the protocol is loop-free or not. Surprisingly we found a number of situations where loops may occur. For example, considering Figure 4.2, the simplest loop scenario occurs in the following case: node A, acting as VAP, transmits the message M_1 that is received by node B. Suppose node B is faster than node A and starts to act as a VAP at a point ahead in the road, it can transmit message M_1, which if received by node A would characterize a loop. For this reason messages need to be equipped with unique identifiers (IDs). Once the node A receives a duplicated message, identified by the ID, it discards it, thereby preventing the loop formation.

Another type of message loop may occur, and is in fact desirable even. Again, let us consider Figure 4.2; supposing that node A acts as a VAP in *lane* 1, the message M_1 sent can reach the node C, going in the opposite direction in the *lane* 2. At some point in the future node C starts to act as a VAP and retransmits the message M_1 that is received by the node D in *lane*1. If node D does not have the message, it is stored and will be retransmitted in the future in case node D becomes a VAP. However notice that this case is not a loop in the conventional sense, since the nodes involved are different. Another point to observe is that this kind of loop is even desirable since it helps in spreading messages over the region. The buffer favors newer messages, so older messages will be ignored and removed from it.

Even though the VAPs do not transmit when they find out that there is another VAP in the same area, depending on the MAC layer protocol used, concurrent transmissions and hidden/exposed nodes problems may also occur. Here we consider the existence of a MAC layer mechanism to handle this, e.g. scheduler for IEEE 802.16 networks or CSMA/CA for IEEE 802.11 networks. However, even if collisions occur, the worst impact will be a waste of bandwidth in a region that was not previously in use anyway.

We also found out that there may be nodes in the network that never take advantage of the VAPs technique. There is no guarantee the mobile nodes will receive all the messages needed to fill their buffers, or a node traverses the entire path from one AP to the other without receiving any message from other VAPs. This will happen if the node is unfortunate enough not be inside the VAP range of other nodes acting as VAP, or when the node itself is acting as VAP for others, and thus is not receiving messages from other VAPs. These situations are more likely to occur in sparse networks.

4.3 Experiments

We now present the evaluations made to determine the impact of the VAP technique over spreading the message through the network. We have three different sets of experiments. The first one evaluates the application of the technique in stream based traffic, the second set of experiments shows the impact of VAPs over different disaster scenarios and the third set evaluates the impact of VAPs over a warning message distribution occurring over a bigger suburb-like area.

4.3.1 Environment

The simulations were programmed on top of the Sinalgo simulator [96], developed by the Distributed Computing Group at ETH Zurich. All the experiments were conducted using Linux Fedora Core release 6 in an Intel Xeon 1.86GHz machine with 16GB of RAM. The graphs are presented with a five percentile and a confidence interval of 99%. Each point is the result of the mean of at least 34 runs with different network configurations. The sizes of the target areas and the period of simulation vary according to the experiment. The APs positions are chosen randomly and the APs are static. In the typical set up, messages are spread by the available APs at a rate of 1 message per second of simulation and the same message is distributed simultaneously by all the available APs.

The scenarios follow a realistic mobility pattern generated with the Vanet-MobiSim [53] tool. All simulations keep the same basic configuration and only one of the parameters is varied: these include the number and the position of APs, the size of the available cache, the size of the message, the type of disaster scenario and the time at which the disaster occurred during the simulation.

4.3.2 Evaluated Disaster Scenarios

One of the main objectives of this work is to create techniques that can work even during severe conditions. Considering this, some experiments were conducted to determine the resilience of the VAP technique in disaster situations. Here we evaluate the impact of two kinds of disaster scenario, the first one is when the network is damaged by natural causes and the second kind is when the network is damaged by sabotage, possibly as a result of terrorist attacks. The tested scenarios evaluate the behavior of regular nodes, before and after the catastrophe. The nodes are the same and follow a realistic movement patterns. This does not mean that we claim that movement patterns will be the same before and after an earthquake, for example . However in the absence of real meaningful data, and considering nodes will still be able to move, we chose to use realistic mobility patterns as a way to test the use of the VAPs to improve the connectivity of the remaining nodes. The natural disasters evaluated here are earthquake and flooding, whereas the sabotage scenarios are power outage and network random failures. These disaster scenarios were abstracted in the simulation as follows:

- Earthquake: The network starts with all the APs and mobile nodes running perfectly. However, at some point, 80% of the existing APs are randomly damaged and excluded from the network. This abstraction permits us to evaluate the effect of the technique when a major part of the APs disappear randomly from the network without any warning.

- Flooding: The evaluated scenario is a flash flooding [35] one. This kind of flooding is common in mountain regions in spring, heavy rainfall during the tropical rainy season and in the case of dam failures. This situation is abstracted in the simulations by the random disabling of a slice of 20%, either horizontally or vertically, of the middle section of the network. All the APs in this segment of the network are disabled. This is meant to simulate a river crossing the city that flooded in a sudden way.

- Power outage: In this scenario, we divided the evaluated scenario in four quadrants. During the simulation one of the four quadrants is randomly chosen and all APs in that quadrant are disabled. Complete blackouts are rare in developed countries, but power outages in cities are relatively common if some problem occurs in a specific power station, power line or other part of the distribution system. Commonly the effect of these failures is that part of the power grid goes down leaving part of the served region without energy. Such problems could occur by accident, or as a result of sabotage.

- Random network failure: In this scenario random network APs fail and disappear from the network during the regular network operation.

The degradation of the network coverage, in this case, is gradual, in contrast to what occurs in the other scenarios. This kind of generalized and chronic failure scenario could be triggered by hacker actions or physical sabotage of the nodes to deny access to the network.

4.3.3 Stream oriented traffic

This section presents the impact of the VAP technique over stream oriented traffic. We examine two types of environments: a highway segment and a city section. The road segment considered is $5Km$ long having four lanes, two in each direction with cars going back and forth on it. For the city environment we chose a $2km^2$ area of Washington D.C. city center with cars distributed through it. The area used for the experiments is depicted in Figure 4.3. For each scenario we have 40 different configurations of 10 simulation minutes, with 200 vehicles and a transmission range of $100m$. For the city environment the nodes minimum speed is $18km/h$ and the maximum is the maximum allowed on that specific road. For the road environment the vehicles minimum and maximum speeds are $60km/h$ and $110km/h$ respectively.

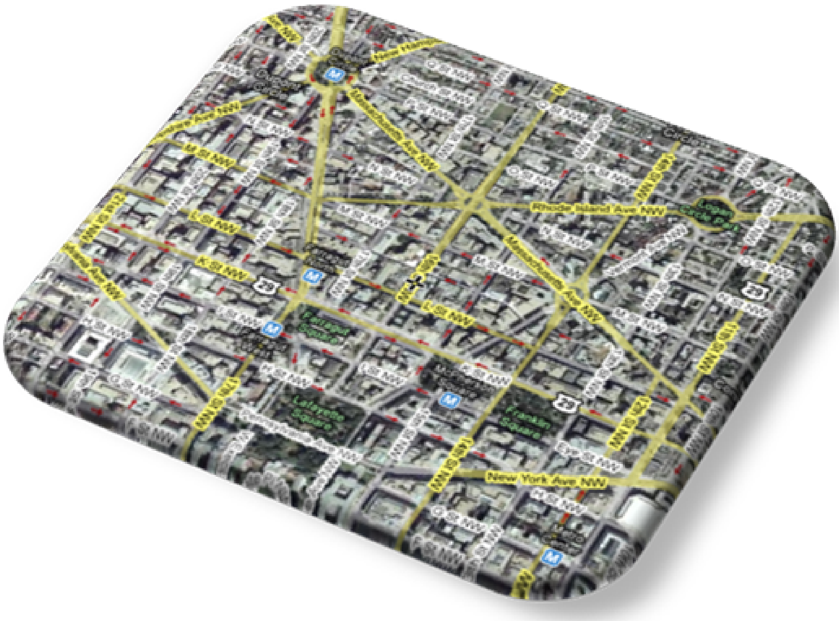


Figure 4.3: Map showing the Washington D.C. area we use for the simulations

All experiments keep the same basic configuration and a single parameter is varied in each one. The varied parameters are: the stream transmission rate, the number of static APs and the method VAPs use to select messages to re-broadcast. The source of the stream generates an ”infinite” Constant Bit Rate (CBR) traffic from 1 to 3 messages per second. We call it ”infinite” because the stream is constant and, for this set of experiments, does not repeat. It simulates a web radio broadcast, what could be an information channel news stream. Each generated scenario has a number of APs placed randomly. The number of APs tested for the city environments where 2, 25, 50 and 100. For the road environment the number of APs evaluated where 2, 5, 10 and 15. Every mobile node has a limited size buffer where it stores the last received messages. During cache replacement the oldest stream message, with lower stream ID, is discarded first, regardless of whether it was the first to be received or not. The three ways the VAPs messages are chosen to be rebroadcasted are random, oldest message first and newest message first.

The use of the VAP technique effectively allows us to increase the coverage of the real APs through the help of mobile nodes. These nodes coordinate to increase network coverage area. The graphs of Figures 4.4 and 4.5 demonstrate typical histograms of messages received in a 2Km simulated square of Washington DC and on a road segment, respectively. We can see that the mobile nodes can cache messages originated from the APs, and act as VAPs to other nodes in non-covered areas. Thus, the nodes, collaboratively, help to forward packets to areas previously uncovered and unused. The VAP technique was first designed to be used in road like environments, but as shown in Figure 4.5 metropolitan environments can also benefit from it. If we compare the plotted map with the actual area map, presented in Figure 4.3, we can even guess the roads and main intersections from it.

VAPs were first devised for road environments, however, as Figure 4.6 and Figure 4.7 show, it is valuable in both scenarios. Figure 4.6 demonstrates the behavior of the VAPs for a road environment displaying the number of unique messages received. Unique messages are defined as messages received by a mobile node for the first time. Numbers of unique messages start to decrease around the 200s because at this point the caches of the nodes start to saturate with stream messages and diversity of messages among the nodes caches decreases. This does not occur as much in the city environment as it does in rural environment of the simulated scenarios. In the road scenario the cars perpetually move along the two opposite highway directions. Thus, the nodes exchange more messages but of decreased diversity. In the city environment, however, nodes follow dissimilar paths which results in diverse cache contents. The number of lost messages decreased between 10% to 15%

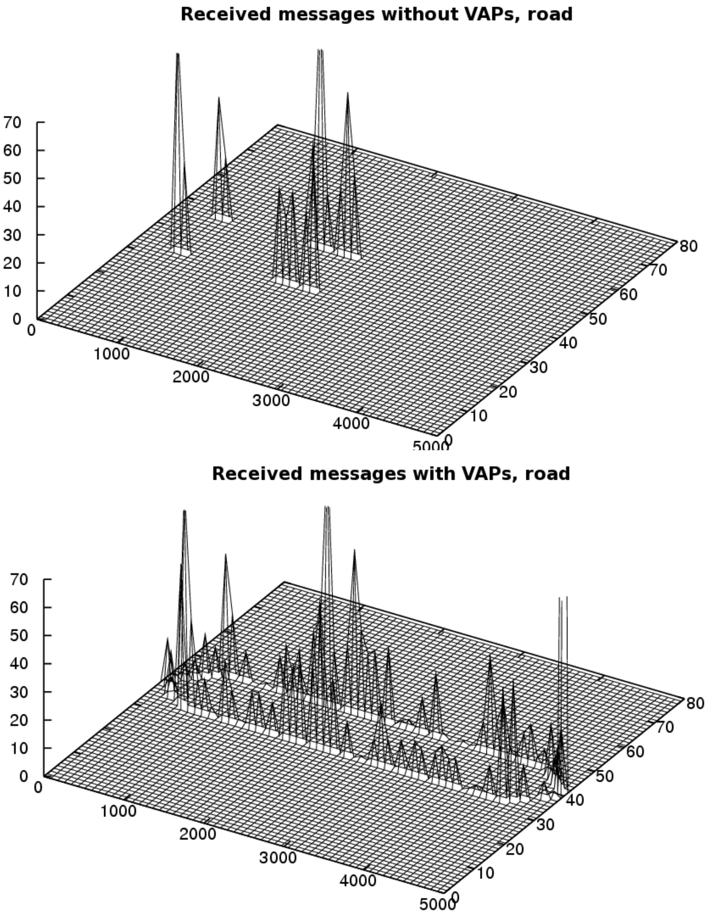


Figure 4.4: Typical histogram of the messages transmissions over the road segment observed

for city environments while for the road environment it decreased between 10% and 27.88%.

Figure 4.8 shows the difference of having 2 or 25 APs in the city scenario for varying bit rates. Both the number of APs and the bit rate influence the number of unique messages received in total. However, as expected, the number of unique messages for scenarios where VAPs are not present is nearly constant, as it only depends on the nodes passing near the APs. Even when the bit rate increases we do not observe a significant increase in the number of unique received messages. When bit rates are increased from 1 to 3 packets per second, in the 2 APs case, the result is marginal. When VAPs

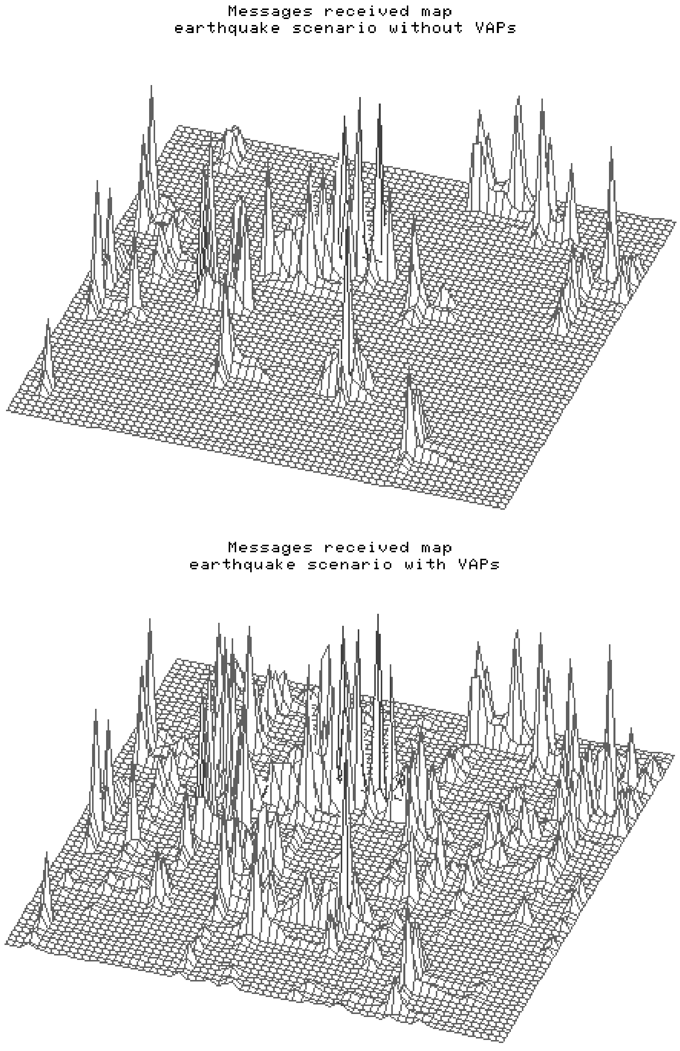


Figure 4.5: Typical histogram of the messages transmissions over the city experiment

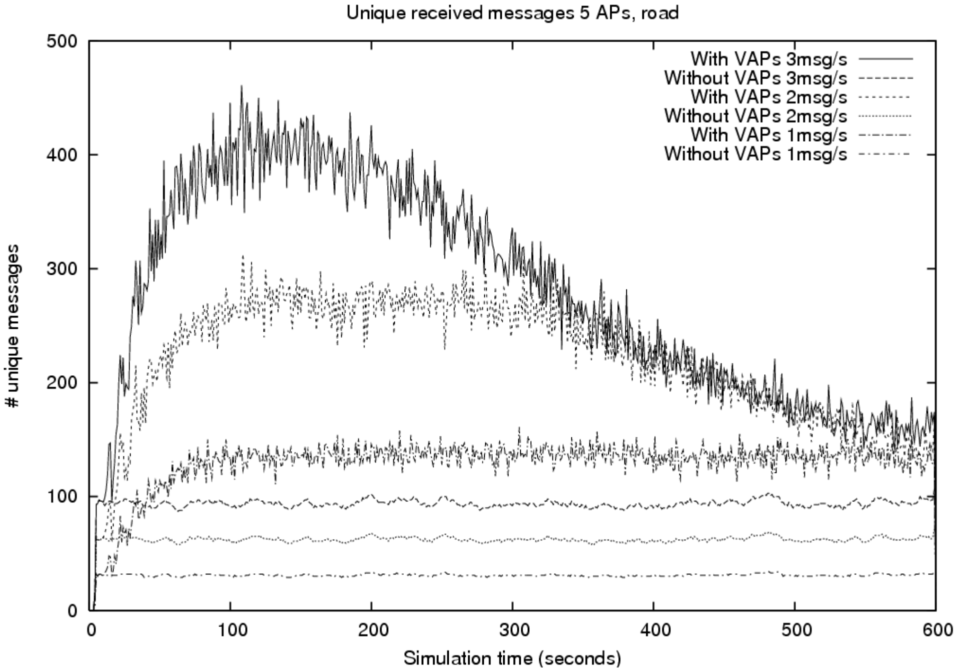


Figure 4.6: Unique received messages through the 10 mins of simulation for the road environment with different traffic rates

are enabled, the number of unique messages received significantly increases, because 2 antennas are not enough to spread the information through the entire network. The VAPs take advantage of nodes caches to propagate messages which were previously lost.

However, the larger the covered area the lower is the gain the VAP technique presents. This becomes apparent when we look at the graph of Figure 4.9. The graph shows, for the same experiments, the messages first received through APs and VAPs. As the number of APs nodes increases in the road environment, the number of messages first received through VAPs decreases. The behavior is similar for the city environment.

The use of VAPs accounts for an increase between 61.7% and 134.57% on the total traffic of the network. However, since this increase occurs only in non-covered areas, it is not creating interference or delaying the system's APs. Nevertheless, evaluating the number of repeated messages is interesting. On Figure 4.10, the number of repeated messages for the networks that use VAPs and the ones that do not use it follows the same shape. Increasing the number of messages generated by the VAPs results in more repeated

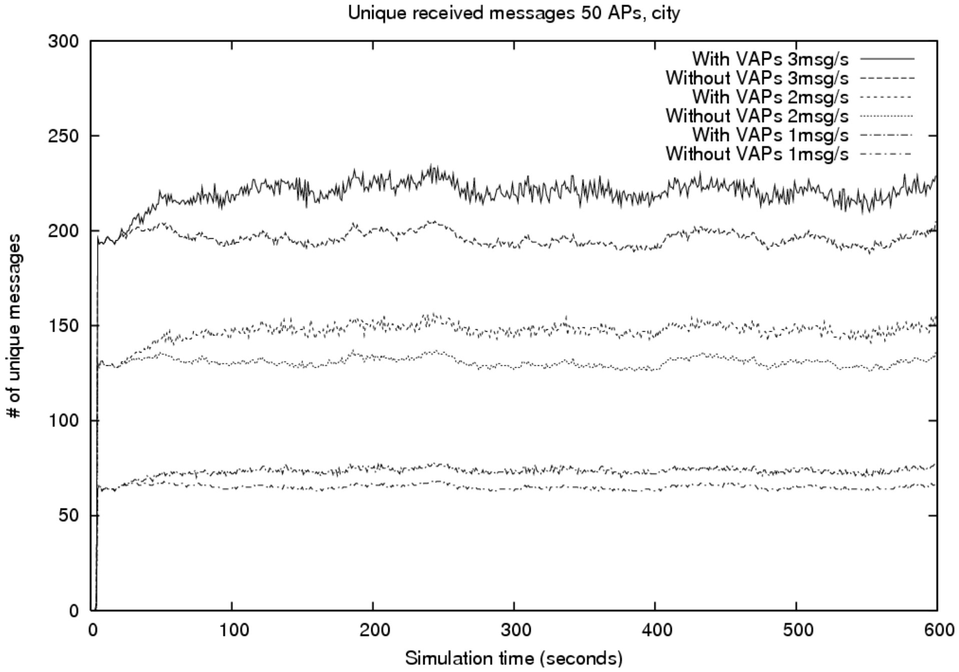


Figure 4.7: Unique received messages through the 10 mins of simulation for the city environments

messages. Figure 4.10 presents the results for different stream rates, as well as for different transmission rates for the VAPs. Each VAP node can either transmit at the same rate the stream generated or at 4 times this rate. For example, if the stream is generated at the rate of 1 message/second (m/s), the VAP can transmit cache messages either at $1m/s$ or at $4m/s$. The number of repeated messages increases based on the number of VAPs, but as the VAPs assignment is dynamic it decreases when the network coverage increases. This way the number of repeated messages also decreases, as there are less VAPs active. Ten is nearly the best number of APs for this scenario. Given less than 10 nodes, we have a lot of uncovered areas and with more than 10 the network gets so overprovisioned that APs start to interfere with each other and the number of repeated messages increase again, not because of the VAPs, but because one mobile node starts to receive messages from more than one AP.

Regarding the VAPs message spreading policies of random, older to newer and newer to older, all three presented nearly the same results. However, on

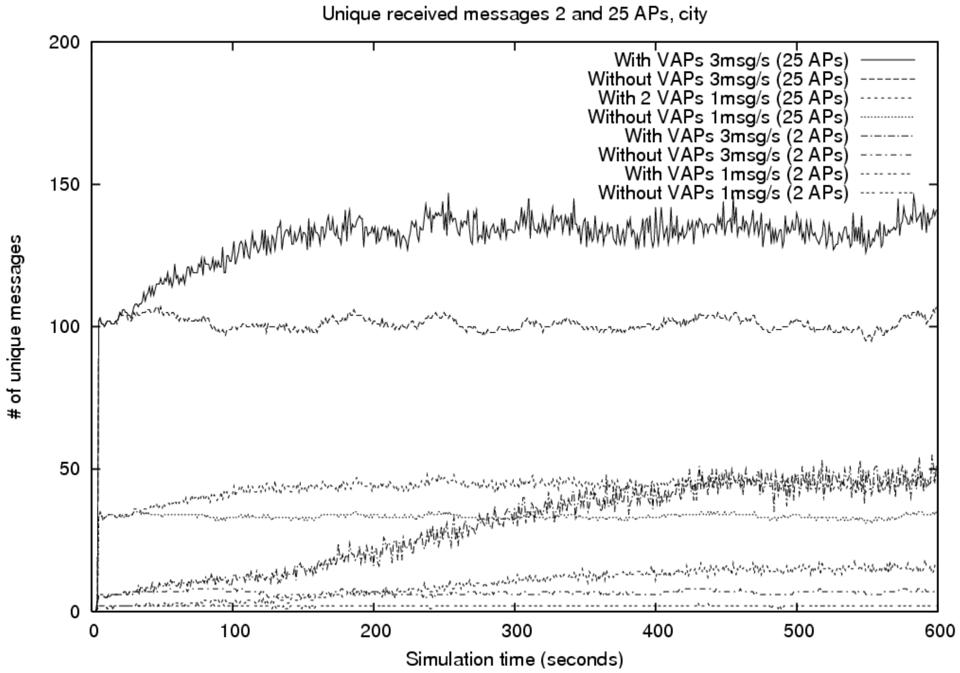


Figure 4.8: Unique received messages through the 10 minutes of simulation for the road environment with different number of APs and traffic rates

average, the random policy, i.e. the VAP node sending a random message from the cache, performed slightly better than the others.

4.3.4 Disaster resilience for stream traffic

For this set of experiments we used the same city area described in the previous set of experiments. A $2km^2$ area of the Washington D.C. city center with cars distributed over it. For each scenario we have 40 different configurations of 30 simulation minutes, with 200 vehicles and a transmission range of $120m$. For the city the nodes' minimum speed is $18km/h$ and the maximum is the maximum allowed on that specific road based on the data provided by the Topologically Integrated Geographic Encoding and Referencing (TIGER) system of U.S. Census Bureau. Each generated scenario has a number of APs placed randomly. The nodes are initially spread uniformly over the roads of the observed area and then follow the VanetMobiSim realistic mobility model. All experiments keep the same basic configuration but the number of and the locations of APs are random. On average we allocate

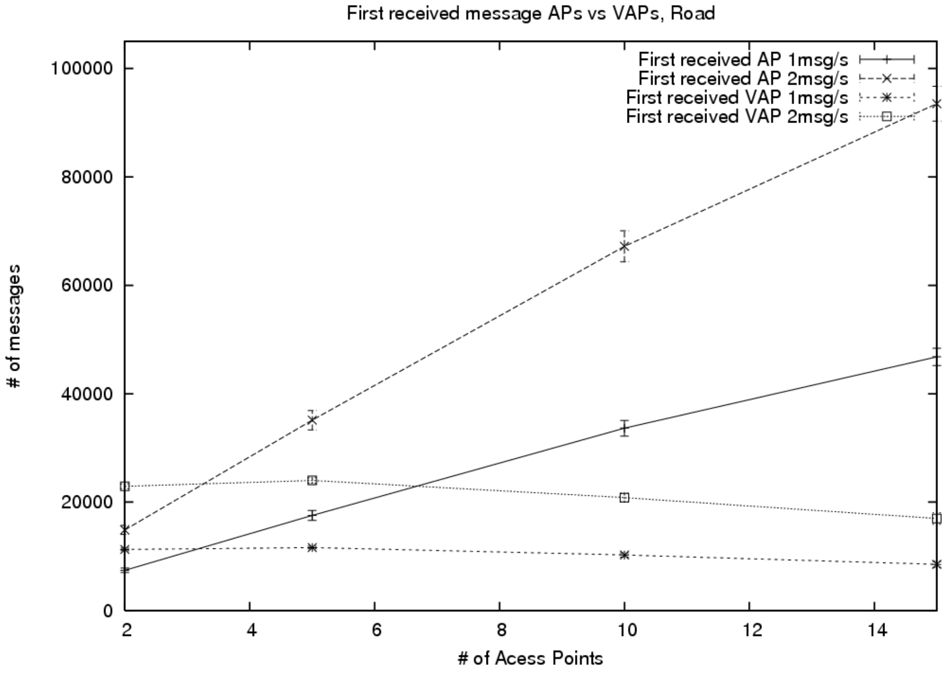


Figure 4.9: Number of messages first received from an AP and VAP

40 APs but the number varies up to 100. The source of the stream generates CBR traffic of 1 message per second, distributed simultaneously by all the available APs. We vary the number of APs, size of the cache, disaster scenario and time, during the simulation, when the disaster occurred.

Figure 4.11 shows the influence of the initial number of APs in the network on the percentage of messages received: for these simulations, the disaster occurs at the beginning of the simulation, and therefore the initial number of APs represents the number before the disaster takes place. We can observe that for all cases the VAP technique provides an increase in the number of stream messages received. The percentage of the stream traffic received is affected by the initial number of APs in the network, with larger number of APs, causing more extensive spread of information in the network. This makes the VAPs efficient for local traffic dissemination. In the best case, when no failure occurred in the network and all nodes work perfectly, using VAP technique provides an increase in the number of received messages that ranges from more than 700%, when the number of APs is two, to 16.6% when the initial number of access point is 100. Note that this ratio

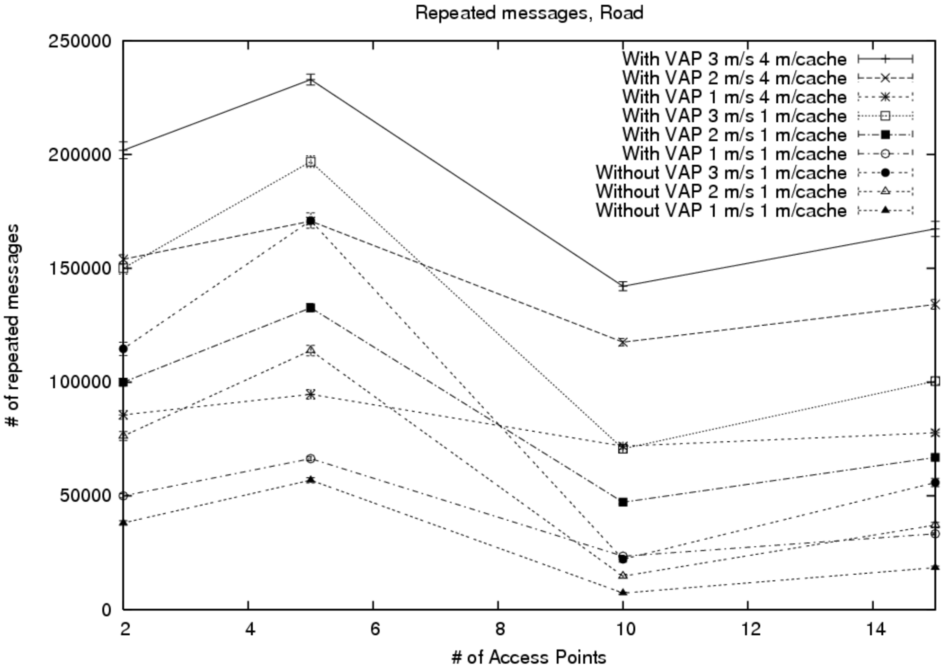


Figure 4.10: Repeated messages for the road environment

is caused by the fact that VAPs allow us to maintain communications in cases where otherwise the system would collapse.

One hundred access points represent, on average, a coverage of 58% of the total simulated area. As expected, the gain diminishes as the space covered by access points increases. This occurs because the VAPs are well behaved and, as it is an opportunistic protocol, the nodes act as VAP only when they are outside the range of any AP and any other VAP. With the increase of the network coverage by the real APs, the regions where a node could act as a VAP decrease and, therefore, the number of messages received through the VAPs decrease. For the disaster scenarios we can detect the same general behavior. Consequently, the percentage of the received streams is larger when the initial number of nodes increases. However, the corresponding gain introduced by the VAPs decreases. For the earthquake scenario the gain varies from 1615.91% to 71.95%. In this scenario 80% of the network is damaged in the beginning of the simulation, which explains the enormous gain. In this scenario, the number of actual APs is really small and almost all the delivered messages are done through VAPs. We call gain the percent

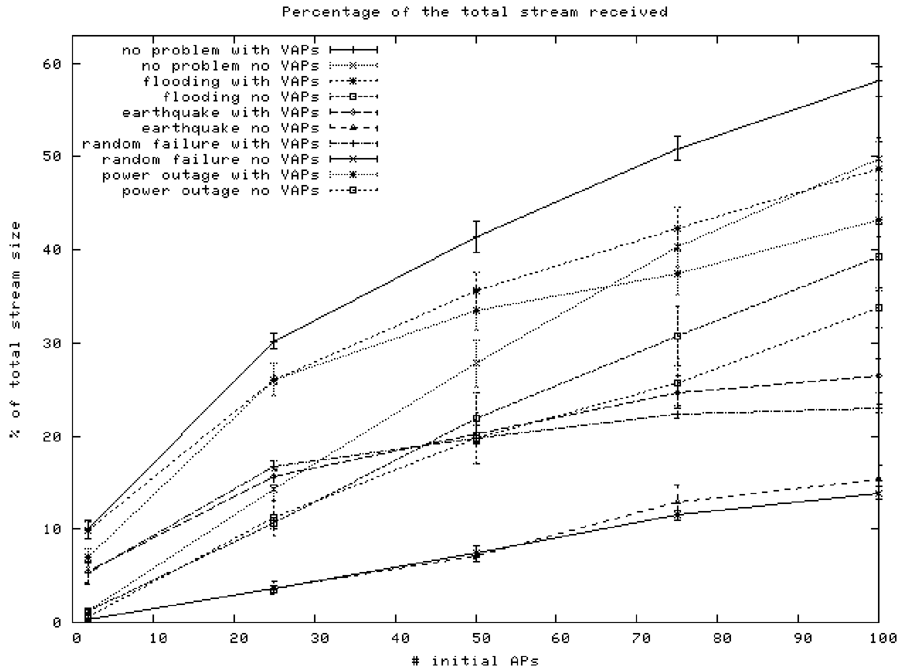


Figure 4.11: Average percentage of messages received in the network as a function of the initial number of APs for the evaluated disaster scenarios

of traffic delivered with help of VAPs over the amount initially delivered without the use of the technique. For example, if we double the number of delivered messages we say the gain attributed to the VAP technique is 100%. For the flooding scenario the gain varies from 753.88% to 24.27%. In the power outage scenario case, the gain varies between 1122.05% and 28.08%. As we can see, the gain reflects the fraction of the initial network affected by the disaster, in the flooding scenario 20% of the network is damaged and for the power outage one fourth of the network is affected. The larger the damage in the network, the more relevant the traffic received through VAPs.

For the random network failure scenario, the intervals between failures are random, distributed uniformly throughout the simulation time. By the end of the simulation only a few nodes remain functional. The damage for this scenario is not huge at first, unlike in the earthquake scenario. However the damage is constant through time. So that, by the end of the simulation, the damage caused to the network is comparable to that in the earthquake scenario. Figure 4.15 shows the behavior of the random failure and earthquake as a function of time. For the random failure, the gain varies from 1585.35% to 65.18%, close to the values estimated in the earthquake set-up.

We additionally vary the buffer size and the time the disaster occurred in the simulation. The results are basically equivalent; the only difference is a small increase in the total number of received messages, when we delay the disaster start time.

The graphs in Figures 4.12 and 4.13 show the number of duplicated messages received by the nodes during the experiments as a result of the application of the VAP technique versus the disaster start time and the size of the cache, respectively. The values for both graphs are relatively stable. This means that the duplicate messages have a low correlation with the size of the cache and the time the disasters started. As we can see in Figure 4.12 the biggest VAP overhead is around 32% of the total number of messages sent in the stream. However, on average 10% of the duplication results from nodes receiving duplicated messages from APs. So the real overhead caused, in the worst case, for the VAPs is about 22% of the network stream traffic generated. When there is no disaster, all 100 APs are working without any problem and a larger part of the stream is received by the mobile nodes from the APs. However, for the disaster scenarios, where not all the APs inject traffic into the network, the overhead varies between 9% and 16% for the flooding scenario, 16% and 19% for the random failure scenario, 24% to 26% for the flooding scenario and between 22% and 25% for the power outage scenario.

In Figure 4.14 we can observe that the number of messages received per cycle increases when we use VAPs. Using VAPs, the variability of that range increases. This is to be expected since VAPs is a best effort mechanism, and not as effective as APs would have been if they were available.

Figure 4.15 shows the number of unique messages received over time. Clearly, the use of VAPs increases the number of unique messages consistently over time. In this graph it is interesting to notice the behavior of the random failure scenario compared to the no disaster and earthquake ones. In the beginning of the simulation the random failure and the no failure results closely resemble one another. However, as time passes, the network degrades gradually in the case of the random failure scenario. VAPs decrease the impact of the APs failures, and enable mobile nodes to receive new messages even when virtually no mobile node receives messages directly from the APs. During the simulations it is guaranteed that, for any scenario, at least one AP exists and broadcasts new messages. If no VAP existed, only nodes in range of this AP would receive these new messages. Using the VAP technique these few nodes may spread the new message throughout the network.

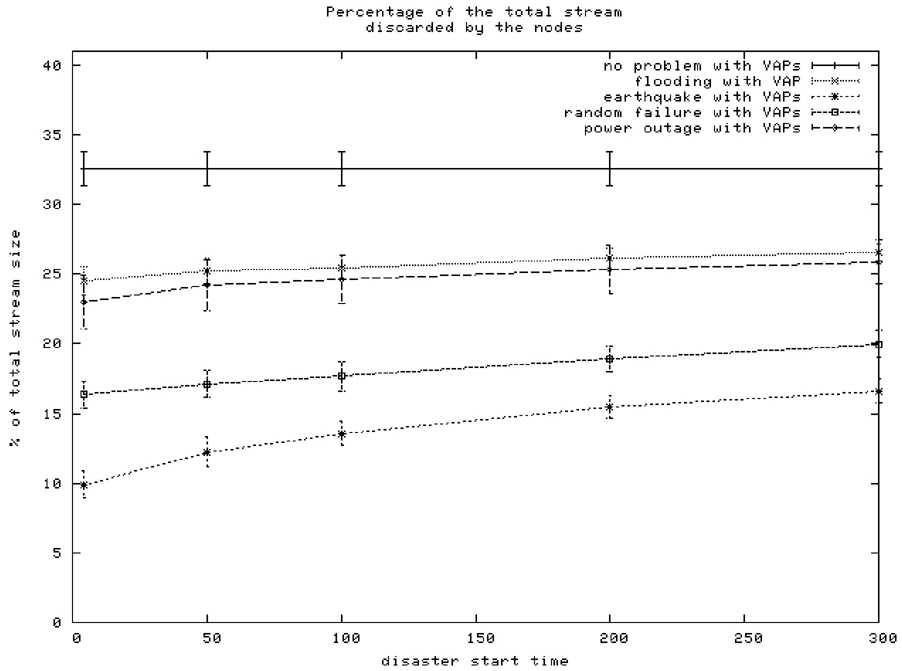


Figure 4.12: Number of duplicated messages received as a function of the initial time of each disaster

4.3.5 Warning message propagation

This set of experiments observes the use of VAPs in a suburb area. The evaluations were carried out in a $15 \times 9km^2$ area that encloses Sophia-Antipolis in the south of France, as depicted in Figure 4.16. The simulations were conducted with 1000 nodes with 200 meters communication range and speeds varying between $40km/h$ and $90km/h$. The nodes arrive randomly and are placed uniformly over the observed area.

We vary both the number of APs and the size of the messages, and analyze the impact of the occurrence of different disasters over the VAPs performance. The source of the stream generates CBR traffic of one packet per second that is distributed simultaneously by all the available VAPs. If the warning message is too big to send in one time interval, it is divided into smaller packets and these are broadcasted, one packet per second, continuously in a cyclical way. We consider transmission intervals of one second. Notice that this set-up is different from the stream-based one. Here we consider smaller messages and the same message is repeated.

The graph in Figure 4.17 shows the number of nodes that received the

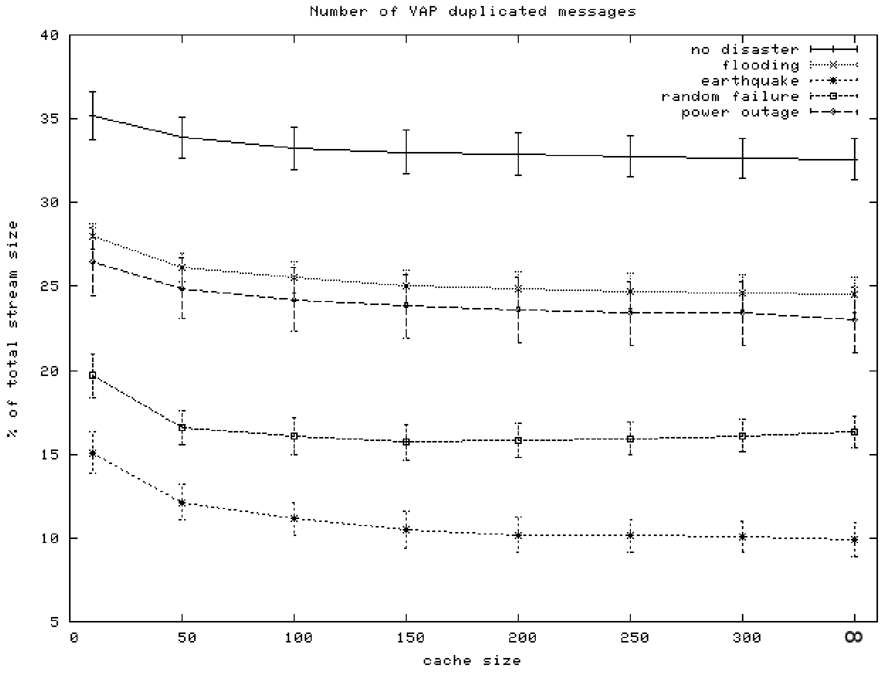


Figure 4.13: Number of duplicated messages as a function of the size of the cache with 100 nodes and the disasters occurring in the beginning of the simulation

one packet warning message for the different disaster scenarios. For all the scenarios evaluated with 10 initial VAPs, the use of VAP enabled the distribution of warning messages to all the network nodes. The most severe disaster evaluated is the earthquake one. In this scenario 80% of the initial VAPs are damaged during the experiment. However, even in this situation the VAPs delivered the warning to all the nodes in the region in less than 20 minutes. Even though the mechanism used to decrease the number of RSUs is different, for the earthquake and the random failure scenarios, their results are close. This occurs because with time the number of damaged stations in the random failure scenario increases. At the end of the simulation the number of remaining RSUs is nearly the same for both scenarios, however the smoother degradation of the random failure scenario grants it a better performance, when compared to the earthquake one. For the flooding scenario, only the nodes on the central strip of the area are removed. Although this affects the total number of nodes that received the warning message completely and slightly increases the time required to distribute the message to all the nodes in the network, the vehicle movement compensates for the

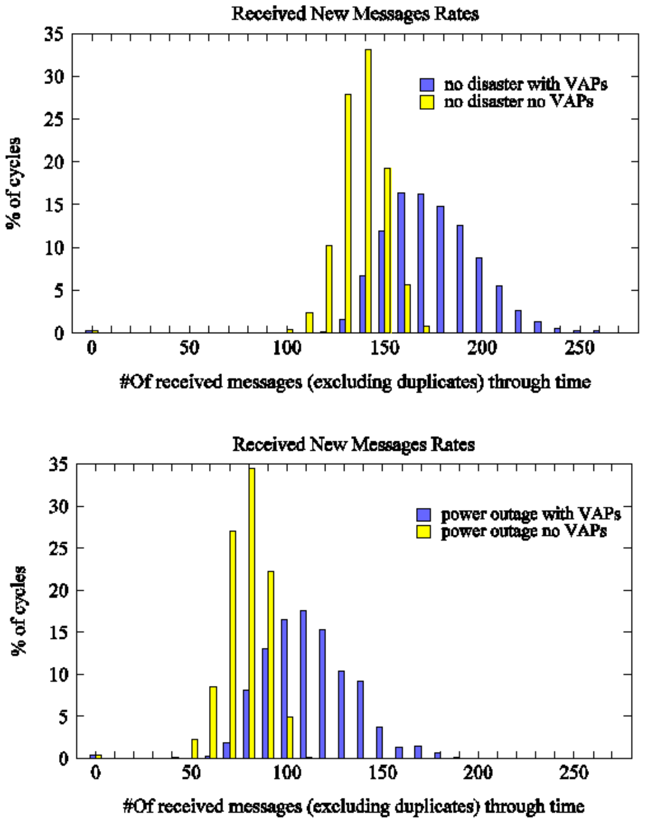


Figure 4.14: Transmission rate and variability

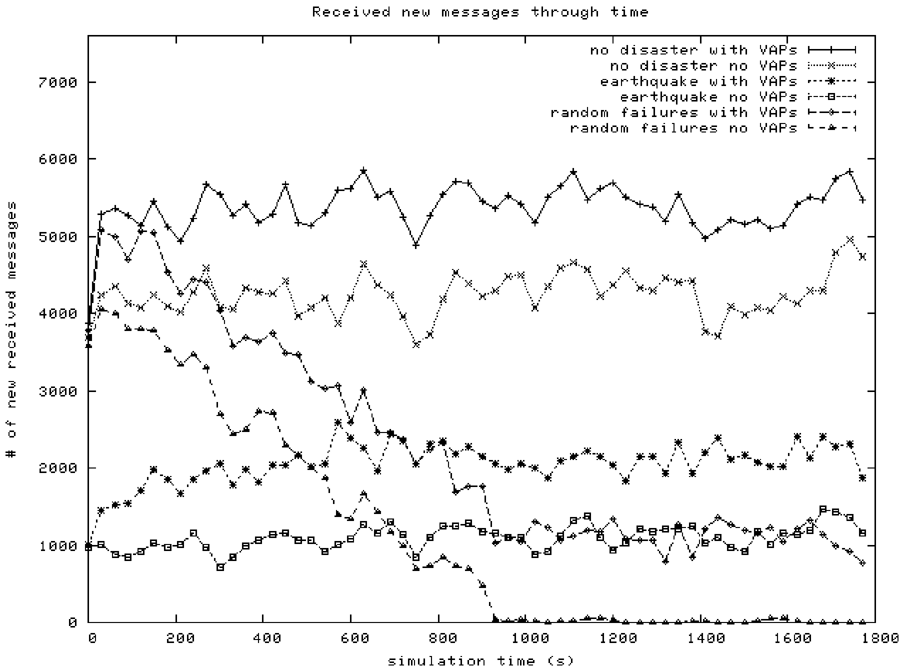


Figure 4.15: Received unique messages over time for the no disaster, the earthquake and the random failure scenarios

lack of RSUs in the central part of the area: nodes that did not receive the message because they were in that region, may later move to a region that is covered by RSUs.

We can perceive in Figure 4.17 that when no disaster occurred, the number of nodes warned is nearly 100%, regardless of whether VAPs are used or not. Indeed, the final number of nodes aware of the message is similar, when we do not consider any disaster. However the graph of Figure 4.18 shows the time it takes for all the target nodes to receive the message. We consider transmission cycles of one message per second, i.e. each second the warning message, or a part of it, is broadcasted. The plot shows the time when all nodes in the network received the warning message. Whether all nodes had received the messages or not the simulation experiment stops after 3600 seconds. If any node failed to receive the message within that interval, the registered time is 3600 seconds. Without the use of VAPs the network needs more than 200 APs to be able to spread the message to all the nodes in less than one hour. With the use of the VAPs, even in the worst case scenario of an earthquake with only two functional VAPs remaining, it takes around

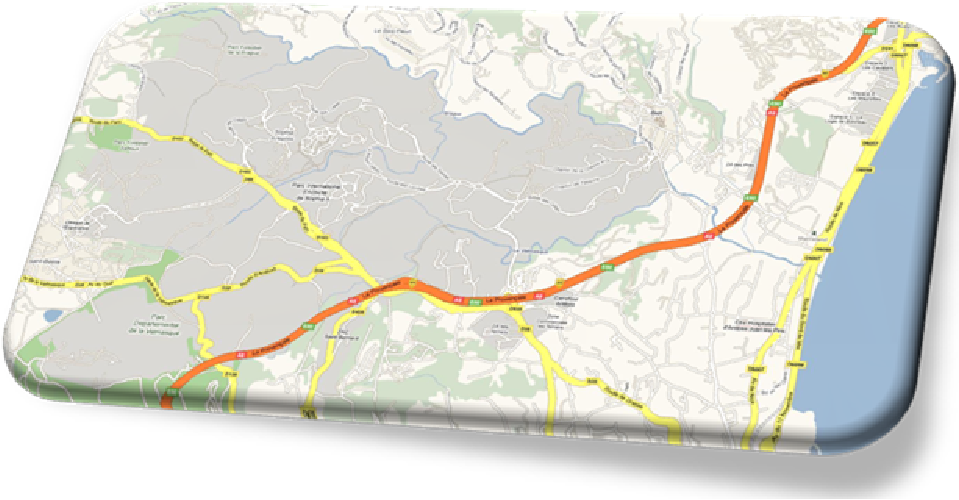


Figure 4.16: The area in Sophia Antipolis used for this set of tests

20 minutes to spread the warning message over all the nodes in the region.

The tendency is that the time required to spread the warning message decreases when the number of VAPs increases. However, the gains become comparatively smaller when number of VAPs increases beyond 50. If we consider the no disaster scenario, if we increase the number of RSUs from 10 to 50 we speed up the message distribution by 28.8%. However, when we increase the number of RSUs from 50 to 500 the gain is 29.8%. I.e. with 50 VAPs we are able to warn the whole population in 8 minutes, whereas if we increase the number of RSUs to 500, the process will take around 5 minutes. This result is interesting since it shows that the increase in the number of RSUs does not linearly impact the time needed to warn the population over a given target area. This means that we could decrease the number of RSUs, and the cost of the system deployment, without compromising significantly the quality of the service offered. This effect is also clear from the graph of Figure 4.19. From this graph we see that when we increase the number of RSUs we do not increase proportionally the number of nodes that receive the warning message. Even without the use of VAPs, the node coverage

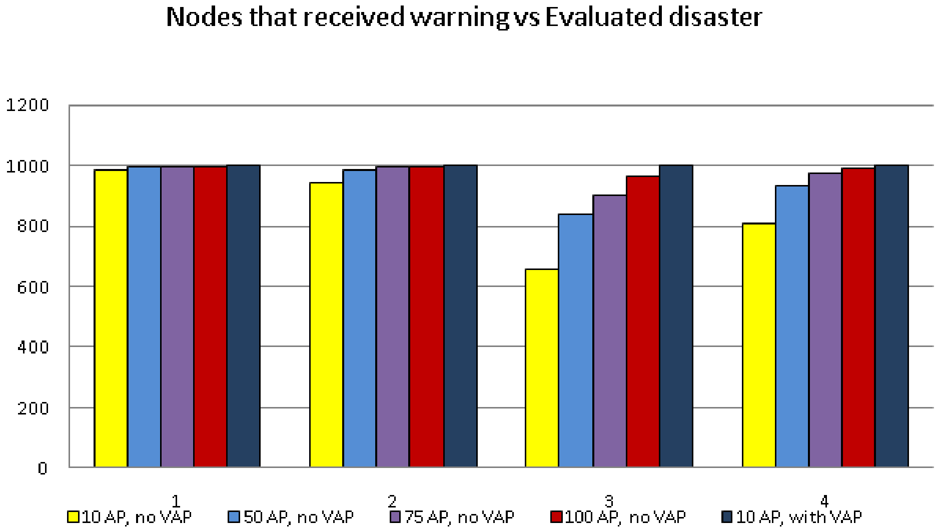


Figure 4.17: Number of nodes that received the warning message taking into account the evaluated disaster scenario

for all scenarios, except for the earthquake one, is almost 100% with only 50 RSUs. However, this value of active RSUs also holds for the earthquake scenario. In the earthquake scenario almost all the nodes are warned when we increase the number of initial VAPs to 200, i.e. when on average 40 RSUs are working during all the experiment: this is roughly the same number of nodes as in the other scenarios.

The apparent discrepancy between the graphs of Figure 4.18 and Figure 4.19 is given by only a small percentage of vehicles that did not receive the warning message during the simulation time. Because of their mobility patterns these nodes did not cross any VAPs during all the evaluated time. When we use VAPs we increase the coverage of the EAS, which permits not only to reach these nodes, but to reach them faster.

The graph of Figure 4.20 shows the percentages of messages first received through VAPs and of those received through real APs. The percentages on the graph are for the one packet size warning message and no disaster scenario. As expected when the number of APs increases the percentage of

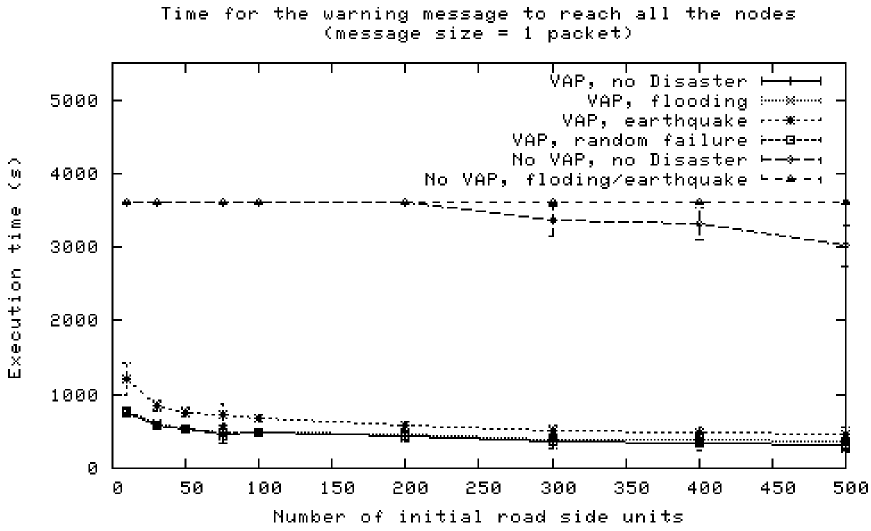


Figure 4.18: Average time for the warning message to reach all the nodes in the region. The simulation stops after 3600 seconds, this means that scenarios that had their time registered at 3600 seconds did not deliver the message to all nodes

packets delivered through VAPs decreases. Vehicles when acting as VAPs are really well behaved, if they perceive the presence of an AP or another VAP they defer retransmitting the warning messages. When we have 10 RSUs the percentage of roads covered by the VAPs is around 3%; on the other hand, when we have 500 RSUs spread randomly throughout the target area the percentage of roads covered by these RSUs is nearly 70%. This is roughly the same percentage of nodes that received the message through VAPs in the graph of Figure 4.20. It is clear that in the extreme case, if we had 100% of coverage, the VAPs would not increase the number of distributed messages. However, not only is it extremely expensive to have 100% of coverage, but also in the case of a disaster, the deployed infrastructure could be severely damaged. The main advantages of VAPs are their dynamicity and capacity to reach non covered areas.

The graph of Figure 4.21 shows the number of nodes that have received the whole message for increasing warning message sizes. As anticipated, increasing the size of the message decreases the number of nodes that receive it completely. However, the use of VAP provides an increase in the number

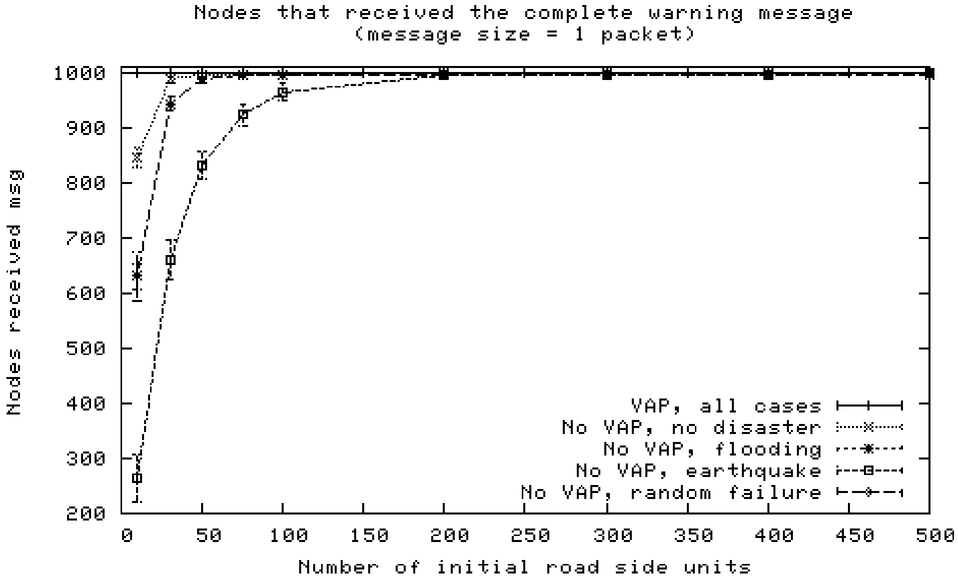


Figure 4.19: Number of nodes that received the warning message versus the number of roadside units on the network

of nodes that do so; comparing to the case without VAPs this increase varies from 14.4% to 60.8%, thus leading to a relatively stable number of warned nodes, even with the increase in the size of the message.

The experiments show that the proposed method increases the coverage and decreases the time required for all the nodes in the network to receive the message, however this has a cost. One of the ways to measure this cost is counting the number of repeated messages received by the nodes. The graph of Figure 4.22 shows the average number of repeated messages received by the nodes. The number of duplicated messages is considerably bigger when we use VAPs. The augmentation in the number of messages is also expected since the algorithm is an epidemic one. However, it is important to call attention to the fact that this traffic occurs in areas that had no communication before.

The number of duplicated messages, observed in the Figure 4.22, decreases when we increase the number of RSUs. This behavior is linked to the results observed in the graph of Figure 4.20. Again, when the area covered by the RSUs increases the areas where vehicles may act as VAPs

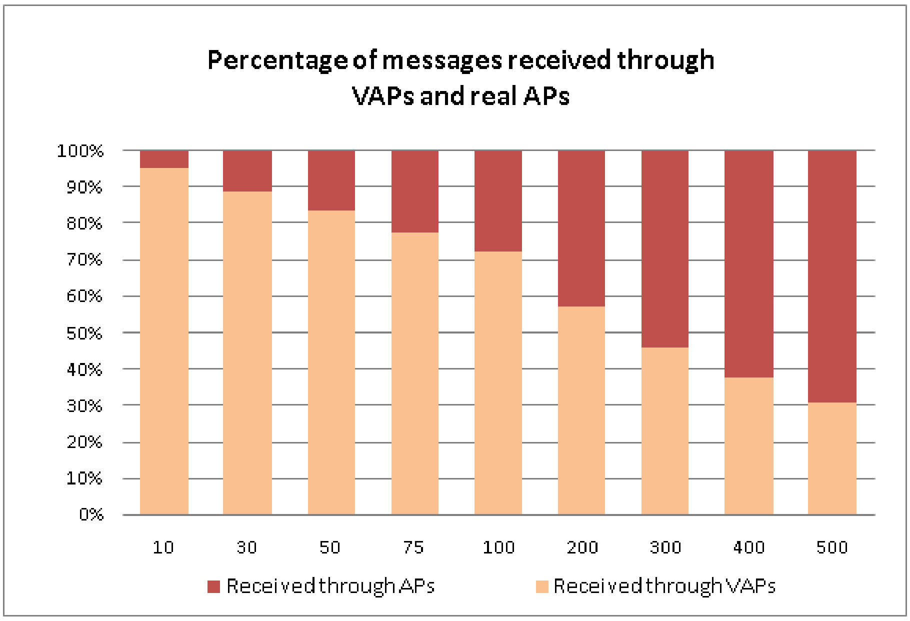


Figure 4.20: Comparison of the percentage of received messages through virtual roadside units and real road side units for one packet warning message vs. the number of road side units

decreases. From the graph in Figure 4.22 we can also observe that, apart from the earthquake scenario, the amount of traffic generated over the different scenarios does not vary significantly. As we can see in formula 4.2 the overhead is a function of the number of VAPs not RSUs. The earthquake scenario is a particular case, especially for small numbers of initial RSUs, for two reasons. First because after the disaster the number of APs is extremely small, so the area where vehicles may act as VAPs is bigger. The second factor is the small diversity of routes, when we have smaller number of APs. A vehicle only starts generating traffic after receiving the first message. When we have a small number of APs the number of sources of traffic is low, and the amount of routes nearby these APs is smaller. Nodes have then more chance of sending the message to nodes that have already received it. The nodes that really need to receive the message are the ones more distant from the AP.

The behavior of the message propagation is similar to the wave generated when we throw a stone in a lake. The wave propagates in every direction, but it takes some time to spread through all the lake and reach its borders. The warning message spreads in a similar way, reaching new nodes at each step.

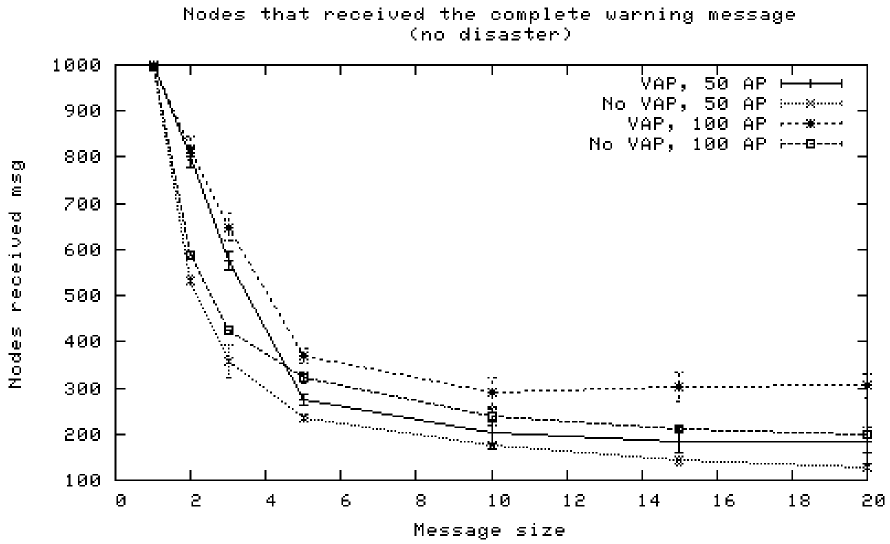


Figure 4.21: Number of nodes that received the complete warning message, vs. the size of the message

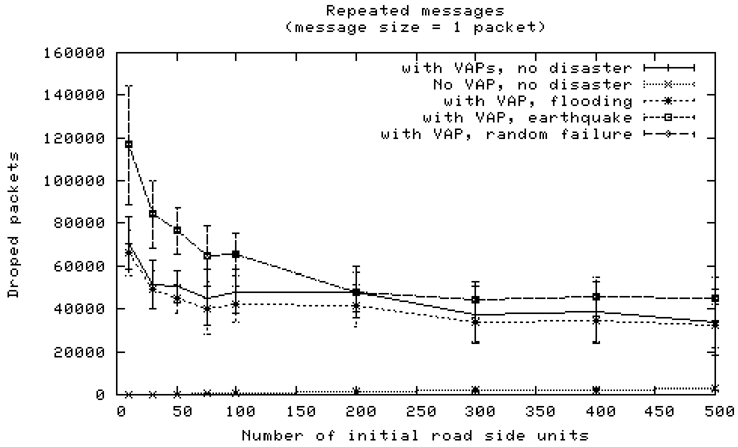


Figure 4.22: Number of repeated messages received by the mobile nodes during the simulation

If the number of VAPs is small the message wave takes more time to reach all the nodes in the network, as we can notice in Figure 4.18. The increase in the simulation time also leads to an increase in the number of messages received. However, when the number of VAPs increases the earthquake scenario starts to present a behavior similar to the one of the other disaster scenarios. None of the other scenarios presents such a severe loss in terms of APs. Even the random failure, which in the end loses a similar amount of APs as the earthquake scenario, does it in a gradual way. For the random failure in the beginning the number of RSUs is bigger and this increases the number of cars with the information. Consequently this increases the variety of the paths followed by the vehicles. This does not occurs in the earth quake where all nodes disappear at the same time.

4.4 Conclusions

The Virtual Access Point technique was proposed to increase network coverage for stream based and warning message traffic in normal situations and disaster scenarios. VAP is a simple yet effective method to increase network coverage for non-real time traffic. As discussed in the simulation results, we observe that the number of received messages for all the evaluated scenarios is increased, often impressively so, which is justified since our system manages to remain operational after the initial system has collapsed. Emergency alert messages are not frequent, but when issued they should be distributed as fast as possible to everyone in the affected region. Lives may depend on how fast and how broad the warning message was distributed.

The experiments show that the gain in the number of received messages may vary from nearly 1615.91% to 24.27% depending on the disaster scenario evaluated. Moreover, VAP is a valuable technique to disseminate network traffic even when no disaster has occurred and can operate transparently to the system. The gain resulting from the application of the VAP technique in the regular network scenario varies from 755.52% to 16.6%, depending on the number of APs disseminating data in the network. Since VAPs are only used in uncovered areas, the gain observed is negatively correlated to the AP coverage of an area. As a result of applying the VAP technique, the number of duplicated and irrelevant messages received by the nodes is increased. However, this traffic occurs in uncovered areas where it causes very low if any interference, and in the worst case, average traffic overhead is increased by approximately 27% in the experiments discussed.

We have also shown that even with a small amount of real access points, using the VAP concept can broaden and significantly speed up the warning message distribution process. Our experiments show that even in severe conditions warning messages can reach all the observed nodes within a reasonable amount of time. On average, sending one packet per second the message was able to reach all nodes in the observed region, 15x9km^2, in six to seven minutes.

Part III

Crisis Management Phase Support

Chapter 5

Mesh Networks

Communication backbones in PSNs are normally organized as a mesh network. However, Wireless Mesh Networks (WMN) generally require self-organization and topology control algorithms to enable its broad use [6]. Studying this problem, of self organization in Mesh networks, has lead us to the main contribution of this part of the thesis, a topology control algorithm to maintain, in an efficient way, the topology of PSNs. Note that this technique can also be applied in ad hoc networks.

Because the next part of the thesis rely on WMN concepts, before moving on to the proposed topology management algorithm, this Chapter provides an introduction to WMN. We use the IEEE 802.16 standard [2] as an example, which could also be used to organize nodes in PSN. This chapter focuses on the main characteristics of WMN, how the nodes can communicate, using the IEEE 802.16 scheduling, to avoid inter-node interference and the possible types of services that can be provided over a WMN. These aspects are relevant to PSNs since these networks must be stable, predictable and provide QoS.

5.1 Introduction

Wireless Mesh Networks have been attracting a huge amount of attention from both academia and industry in the last few years. Indeed, WMN is now emerging as a promising technology for broadband wireless access [6]

[17]. One of the main reasons for this sudden popularity of WMN is their inclusion in many of the IEEE wireless standards, e.g. IEEE 802.11 [21] and IEEE 802.16 [2]. Specifically for the IEEE 802.16 or WiMAX networks standard, the addition of the mesh mode brought a series of advantages., such as non-Line-of-Sight (NLOS) capability, higher network reliability, scaling, throughput and availability [25].

However, to become really useful and valuable for the applications running on top of them, the WMN must i) provide some level of Quality of Service (QoS), ii) be easy to use and iii) provide network self-organization and topology control [6]. To fulfill this requirement, Radio Resource Management (RRM) techniques play a major role [5]. RRM is the term used to identify a series of strategies and algorithms employed to optimize the use of the radio spectrum and the limited resources of wireless networks. RRM techniques include frequency and/or time channel allocation, transmission power adaptation, access to base stations, handover criteria, modulation schemes, error coding schemes [114]. According to [5] RRM policies, along with the network planning and air interface design, truly determine the QoS network performance at both individual user and network level. Figure 5.1 presents the RRM process. The call admission control procedure is responsible for granting/denying access to the network. The decision of which connections are accepted and which are not, is based on predefined criteria, taking into account the network status and the requirements of new calls. The admitted calls are then controlled by other mechanisms of the RRM, such as the scheduler. The scheduler is the RRM process that decides when to grant bandwidth for the admitted calls.

5.2 Main characteristics

WMNs are normally defined as consisting of two types of nodes: mesh routers and mesh clients [6]. Mesh routers are the nodes in charge of routing messages while mesh clients are the nodes that use the mesh routers' capability to connect to other mesh routers/clients or even other networks through backhauls. Backhauls are special nodes capable of interconnecting the WMN to other networks, such as the Internet. A WMN is dynamically self-organized and self-configured, and the nodes should automatically create and maintain the links among them. In opposition to ad hoc networks, where normally no organization is imposed, WMNs consist of a wireless backbone with mesh routers providing connectivity capabilities to mesh clients. The wireless backbone provides large coverage, connectivity, and robustness in the wire-

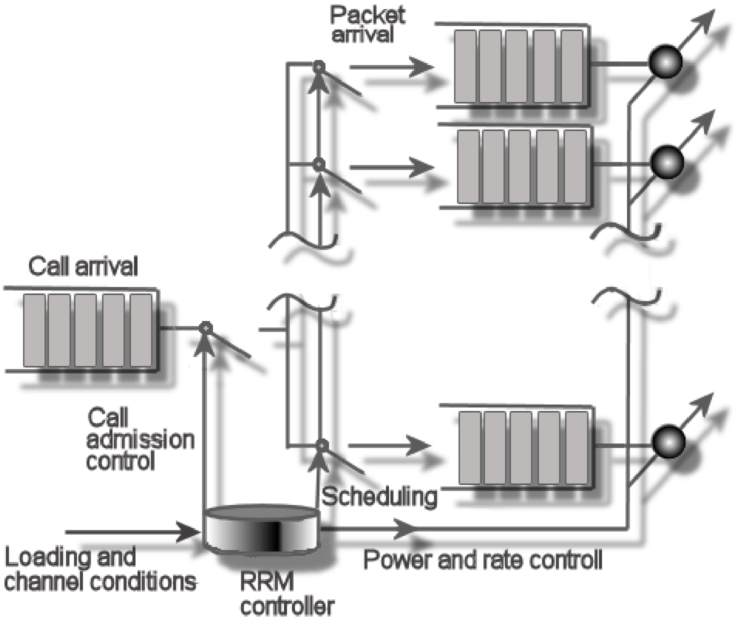


Figure 5.1: The radio resource management model [5]

less domain [6]. Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes. Another important characteristic of WMNs is their capacity of integrating various existing networks such as Wi-Fi, the Internet, cellular and sensor networks through gateway/bridge functionalities in the mesh routers [6].

In contrast to ad hoc networks, where the connectivity depend on the individual contributions of end-users which may not be reliable, WMNs rely their connectivity on trustable mesh routers with, typically, low mobility and higher capacity. For both, WMNs and ad hoc networks the capacity of the network decreases as the density of the network increases. To minimize this effect a node should only communicate with nearby nodes, and nodes can be organized into clusters interconnected by relay nodes [6].

We need to remember that, in principle, the wireless medium is a broadcast one where, at any time, a number of different stations are accessing the channel concurrently. The main problem with this is that, if concurrent transmissions occur on the same carrier frequency at the same time, this may result in mutual destruction of the transmitted signals. Unfortunately the interference range is greater than the transmission one. The receiver can only decode or sense the message if the Signal-to-Interference-and-Noise-Ratio (SINR) is above some level. For example, in Figure 5.2, node D can have its signal jammed by the signal sent from B to C and may not be able to actually decode the signal. The interference range means that any transmission made from A, which is in the interference range, can damage the signal between B and C. These different ranges can lead to a number of different scenarios, among them the hidden and exposed node problems, common in IEEE 802.11 networks. For WiMAX networks, scheduling and CAC are the techniques used to avoid the interference problems. However, regardless of the claims that WiMAX networks are free from such problems, Zhu and Lu [116] show they can also occur in WiMAX environments.

5.3 WiMAX Mesh Mode Overview

The WiMAX mesh mode, introduced in the standard by the IEEE 802.16a amendment [3], supports two different physical layers: $WirelessMAN-OFDM^{TM}$, operating in a licensed band, and $WirelessHUMAN^{TM}$, operating in an unlicensed band. Both of them use 256 point FFT OFDM TDMA/TDM for channel access and operate in a frequency band below 11GHz.

Even though the standard permits both Time Division Duplex (TDD)

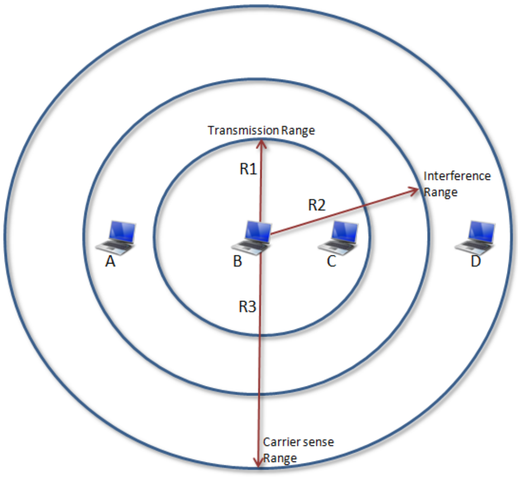


Figure 5.2: Different ranges in the nodes communication

Message Type	Name	Description	Connection Mode
39	MSH-NCFG	Mesh Network Configuration	Broadcast
40	MSH-NENT	Mesh Network Entry	Basic
41	MSH-DSCH	Mesh Network Distributed Schedule	Broadcast
42	MSH-CSCH	Mesh Network Centralized Schedule	Broadcast
43	MSH-CSCF	Mesh Network Centralized Schedule Configuration	Broadcast

Table 5.2: Mesh MAC Management Messages.

and Frequency Division Duplex (FDD) as access schemes, for the mesh mode only the TDD is allowed [2]. This means that the uplink and downlink transmissions share the same frequencies and, doing so, they must occur at different times. However, for IEEE 802.16j, the upcoming part of the standard related to relay networks some people proposed the use of FDD [101].

The Mesh frame is divided into control and data sub-frames. There are two types of control sub-frames: schedule control and network control sub-frame. The network control sub-frame provides basic functionality for network entry and topology management. The schedule control sub-frame controls the transmissions. The scheduling is done by negotiating minislot ranges for the traffic demands of each link. All the communications are done in terms of the links established between nodes. All data transmissions between two nodes are done through one link and the QoS is provisioned over links on a message by message basis. Upper layer protocols are in charge of the traffic classification and flow regulation.

5.3.1 Scheduling policies

In Mesh mode *all* transmissions have to be scheduled: not even the Mesh BS can transmit without having its transmission coordinated with other nodes [2]. To organize the medium access, the standard defines three different scheduling mechanisms: coordinated centralized scheduling, coordinated distributed scheduling and uncoordinated distributed scheduling. These three scheduling policies can be either used alone or together in the same network.

According to some authors the centralized schedule should be used for external traffic and the distributed schedule for intra network traffic [25] [30]. This is due to the fact that the centralized scheduler relies on a mesh BS, which is a backhaul responsible for acting as a gateway between the internal and external network traffic. Table 5.2 presents the messages used by the CAC and scheduling mechanisms in the WiMAX mesh mode.

Centralized scheduling

For Centralized Scheduling, the mesh BS schedules all network transmissions, even the mesh BS ones. The resource request and the mesh BS assignments are both transmitted during the control portion of the frame. The centralized scheduling coordinates the transmissions and ensures that they are all collision-free. Once the BS has the knowledge of the entire network, it is typically more efficient at using the spectrum than the distributed forms.

The MSH-CSCH message has two variants, MSH-CSCH Request and MSH-CSCH grant. With the MSH-CSCH Request each node estimates and reports the level of its own upstream and downstream traffic demand to its parent. This demand comprises also the demands reported by the node's children. With the MSH-CSCH Grant the mesh BS propagates down, through the routing tree, the levels of flows and grants to each node in the network. Fig. 3 shows an example of message flow for the centralized schedule.

All MSH-CSCH Grant messages contain information about all network grants, since all nodes need the complete information for the schedule computation. Upon receiving any message in the current scheduling sequence and assuming that nodes have up-to-date scheduling configuration information, any node is able to compute locally the schedule for all transmissions, including its own. Besides the mesh BS, a node should not transmit any downstream centralized scheduling packet without receiving a MSH-CSCH message from a parent. Also, a node should not send any centralized scheduling packets, if its MSH-CSCF information is outdated. Figure 5.3 presents an schematic example of the message flow in the centralized scheduling scheme.

In terms of eligibility to send and receive MSH-CSCH messages, all nodes are eligible to retransmit the grant schedule, except those with no children. For transmitting MSH-CSCH grant messages, all nodes with children are eligible. For transmitting MSH-CSCH request messages, all nodes, except the mesh BS are eligible.

Distributed scheduling

In both coordinated and uncoordinated distributed scheduling mechanisms, all the stations in the two-hop neighborhood must have their transmissions coordinated to avoid collision. The coordinated distributed scheduling uses the control part of the frame to transmit its own traffic schedule. Both scheduling schemes, centralized and distributed, may coexist at the same time in the same network.

The uncoordinated distributed scheduling is a simpler version of the dis-

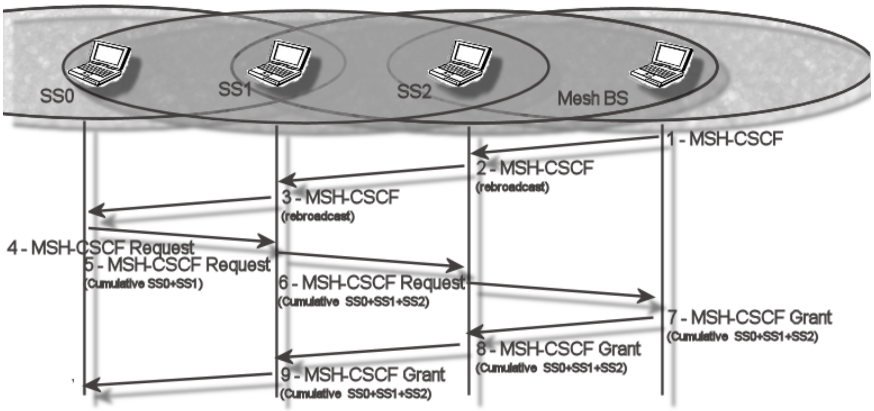


Figure 5.3: A message flow example for the centralized scheduling scheme

tributed scheduler and may be used for fast ad-hoc setup of schedules in a hop-by-hop basis. The uncoordinated schedule is basically an agreement between two nodes and should not cause collision with the data and control traffic scheduled by the coordinated schedules. Both coordinated and uncoordinated distributed scheduling employ a three-way handshake to setup the connection.

The first message in the three-way handshake is a MSH-DSCH request. The transmission is scheduled using a random-access algorithm among the ”idle” slots of the current schedule. If the attempt was unsuccessful a random backoff is used to avoid new collisions. Figure 5.4 shows schematically the messages in the distributed schedule three way handshake.

The MSH-DSCH Grant can be issued by any neighbor that hears the MSH-DSCH Request. The grant message contains the list with the subset of the resources awarded. The first granter node may start its grant transmission in the immediately following base-channel idle minislot. More than one granter may also respond to the request.

The requester node sends the same received MSH-DSCH Grant message in confirmation. This ensures the requester’s neighbors become aware of the grant awarded. The grant confirmation is then sent in the first available minislots following the minislots reserved for the grant opportunity of the last potential granter.

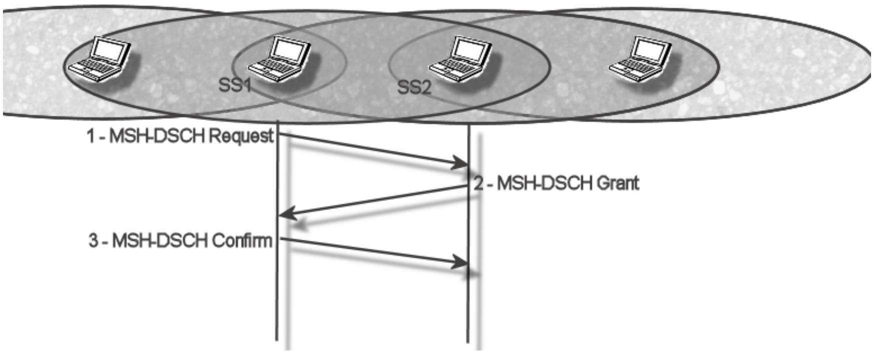


Figure 5.4: Distributed scheduling three way Hand Shake

5.3.2 Network configuration

Two more messages, responsible for creating and maintaining the network configuration, may be transmitted in the network control sub frame: Mesh Network Configuration (MSH-NCFG) and Mesh Network Entry (MSH-NENT).

A new node that wishes to join the mesh network needs to wait until it hears a MSH-NCFG message. When the new node receives this message it is able to synchronize with the mesh network. In reality it should decide which node will be the best sponsor for its communication, so the new node may wait for more than one MSH-NCFG message to arrive. When the sponsor node is chosen, the new node sends through the sponsor a MSH-NENT message to the mesh BS with its registration information. The sponsor node then establishes a quick scheduling, through the uncoordinated scheduler process, and communicates it to the new node. The new node confirms the schedule and sends the required security information. Finally, in the last step, the sponsor node grants the new node access to the network.

5.4 Quality of Service over IEEE 802.16

The IEEE 802.16 standard defines five different scheduling types of services: Unsolicited Grant Service (UGS), Real-time Polling Service (rtPS), Extended Real-time Polling Service (ertPS), Non-real-time Polling Service (nrtPS), and Best Effort (BE). Table 5.4 summarizes the main characteristics of these five types of services.

- Unsolicited Grant Service - UGS: Designed to support real-time data streams where packets are generated at a fixed data rate, for example, VoIP connections without silence suppression. The mandatory QoS parameters for this service are Maximum Sustained Traffic Rate, Maximum Latency, Tolerated Jitter, Uplink Grant Scheduling Type and Request / Transmission Policy. Once the data rate is constant, if present, the Minimum Reserved Traffic Rate parameter should have the same value as the Maximum Sustained Traffic Rate parameter, since the data rate is constant. The grants for this service are issued periodically and without any explicit request. The main advantage of this is that it eliminates the overhead and the latency of the subscriber station, (SS) issuing for new grants for this specific traffic.

- Real-time Polling Service - rtPS: The Real-time Polling Service is designed to support the same kind of traffic that UGS does, but with variable data rate, e.g. MPEG video. The mandatory QoS parameters are Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Maximum Latency, Uplink Grant Scheduling Type and Request/Transmission Policy. Differently of the UGS flow, this service offers periodic unicast request opportunities for the SS to adjust the size of its grants.

- Extended Real-time Polling Service - ertPS: The extended rtPS service, introduced at a later stage into the standard [1], is a service based on both UGS and rtPS. For ertPS the flow has some amount of resources reserved in an unsolicited grant way, but the allocation may change if the SS requests it. In other words, the allocation is dynamic and depends on the needs of the SS, but once set, it works in a similar way as the UGS type. The key service information elements are the Maximum Sustained Traffic Rate, Minimum Reserved Traffic Rate, Maximum Latency and Request/Transmission Policy. The extended rtPS is designed to support real-time service flows that generate variable size data packets on a periodic basis, such as Voice over IP services with silence suppression.

- Non-real-time Polling Service - nrtPS: The nrtPS is designed to support delay-tolerant data streams consisting of variable-sized data packets that require variable data grant on regular basis. FTP (File Transfer Protocol) is an example of application that could use this kind of service. The mandatory QoS parameters for this scheduling service are Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Traffic Priority, Uplink Grant Scheduling Type and Request/Transmission Policy. The advantage of this kind of service is that it can support data streams even in very saturated network conditions. The mesh BS provides SS the opportunity to request bandwidth using unicast and contention period. In addition, piggyback request opportunities are also available.

- Best Effort Service - BE: Best Effort service is intended to be used for any other kind of traffic that does not have any significant QoS requirements and that can be handled on a space-available basis, e.g. http and e-mail traffic. The mandatory QoS service flow parameters for this scheduling service are Maximum Sustained Traffic Rate, Traffic Priority and Request/Transmission Policy.

Characteristic —————— Scheduling type	Max Sustained Traffic Rate	Min Reserved Traffic Rate	Max Latency	Tolered Jitter	Traffic Priority	Req./ Transm. Policy	Piggy Back Request	Bandw. Stealing
UGS	M	O	M	M	X	M	NA	NA
rtPS	M	M	M	O	M	M	A	A
ertPS	M	M	M	M	M	M	A	NA
nrtPS	M	M	X	X	M	M	A	A
BE	M	X	X	X	M	M	A	A

M - Mandatory, O - Optional, X - Not Available, A - Allowed, NA - Not Allowed

Table 5.4: WiMAX services and their main parameters and characteristics.

5.5 Further reading

For future reading, among many other related works, we may highlight the survey presented by Kuran and Tugcu [69] in general dealing with emerging broadband wireless technologies. For a general survey of mesh networks the Alkydiz et al. work [6] presents a good overview of many aspects of the mesh networks, discussing how these aspects affect the entire network stack. The problem of CAC mechanisms in general is discussed in [5]. A broad view of the problem of distributed medium access control for mesh networks can be found in [31]. Zhao presents a consistent view of the problem of distributed coordination in mesh networks in [115]. For a deeper discussion, more specifically for 802.16 mesh networks centralized scheduling algorithms, see [39]. In [89] Redana and Lott present an analysis of the overhead caused by the control messages on the IEEE 802.16 mesh mode and show that, for multihop networks, the centralized approach have a better performance than the distributed one. For an analysis of the times involving the phases of the distributed scheduler mode see [23] and [24].

Chapter 6

Topology Management

As stated in the previous chapter, one of the premises to enable the full utilization of the WMN potential is self-organization. The network must be able to have mechanisms to control its behavior and adapt to new situations. This chapter introduces the network topology control that is a key aspect on wireless mesh and ad hoc networks. Control and maintain a defined and stable topology simplifies the tasks of the other layers algorithms. These algorithms are expected to work autonomously and adapt themselves to different situations maintaining the defined network structure.

6.1 Introduction

Topology management, or topology control, algorithms are used to reduce the initial topology of the network to save energy, increase the lifetime and improve stability of the network. The main goal is to maintain a desired topology, normally aiming to reduce the number of active nodes, and/or links, save resources and organize the network.

Topology control algorithms select the communication range of a node, and construct and maintain a network topology based on different aspects such as node mobility, routing algorithm and energy conservation [11]. For Santi [92] topology control is also about dynamically changing nodes' transmit power to achieve a specific goal, from the network perspective, while decreasing the power consumption. However Santi highlights that power control alone is not enough to define a topology control algorithm. Power control algorithms normally focus on the best power choice for a single channel, or transmission, while topology control mechanisms have a more systemic view as they aim to optimize the *whole* network.

Wightman and Labrador [109] consider topology control to be composed of two subproblems: topology construction and topology maintenance. Topology construction is the phase where the initial deployed nodes are first organized. In the beginning there is no control over the position of the nodes and their interconnections. Some areas may be over populated or have too many between nodes, while other areas may be poorly covered and connected. The objective of the topology construction phase is to minimize these discrepancies while organizing the network within the specified constraints. Topology maintenance is the process of maintaining the reduced topology with the desired characteristics. This process is required since after some time the established topology may change, for example, nodes may move or run out of battery.

6.2 Topology Formation

6.2.1 Neighbor Discovery

The performance of both ad hoc and mesh networks depend on the interaction among communicating entities in a given neighborhood. Thus, in general, before a node starts communicating, it must discover the set of nodes that are within its direct communication range. Once this information is gathered, the node keeps it in an internal data structure so it can be used in different networking activities such as routing. The behavior of an ad hoc node depends on the behavior of its neighboring nodes since it must sense the medium before it starts transmitting packets to nodes in its interfering range, which can cause collisions at the other nodes.

Node discovery can be achieved with periodic transmission of beacon packets (active discovery) or with promiscuous snooping on the channel to detect the communication activity (passive discovery). In probe-based distributed protocol for knowledge range adjustment (PRADA) [75], a given source node periodically sends a discovery packet to its neighboring nodes, to which the latter reply with a location update packet (that might include, for instance, the node's geographical location). PRADA adjusts dynamically its communication range, called topology knowledge range, so it leads to a faster convergence of its neighboring nodes.

6.2.2 Packet Forwarding Algorithms

An important part of any multi-hop network is the packet forwarding algorithm that chooses which neighboring node is going to be used to forward the data packet. It does so following a forwarding goal, having the shortest average hop distance from source to destination for instance. In this case, the set of potential nodes may include only those within direct communication range of the current node or also all nodes along the route to the destination. The forwarding goal may also include some QoS parameters such as the amount of energy available at each node.

The following forwarding algorithms consider only nodes that are in direct communication range of the node that has a data packet to be forwarded, as depicted in Figure 6.1. The Most Forward within Radius (MFR) forwarding algorithm [86] chooses the node that maximizes the distance from node S to point p. In this case, as depicted in Figure 6.1, it is node 1. On the other hand, the Nearest Forward Progress (NFP) forwarding algorithm [102] chooses the node that minimizes the distance from node S to point q. In this case it is node 2. The Greedy Routing Scheme (GRS) [55] uses the nodes' geographical location to choose the one that is closest to the destination node D. In this case it is node 3. The compass selected routing (COMPASS) algorithm [44] chooses the node that minimizes the angle α but considering the 4 nodes that are closest to node D. In this case it is node 4. The random process forwarding algorithm [81], as the name suggests, chooses a random node that is in direct communication range from S.

The Partial Topology Knowledge Forwarding (PTKF) algorithm [75] chooses a node using a localized shortest path weighted routing where routes are calculated based on the local topological view, taking into consideration the transmission power needed to transmit on that link.

6.3 Classification

Broadly speaking, topology control algorithms for ad hoc networks can be classified as having a hierarchical or clustering organization, or a power-based control organization [11] [110]. Furthermore, these algorithms can be either centralized, distributed, or localized.

6.3.1 Clustering Algorithms

The clustering process consists in defining a cluster-head node and the associated communication backbone, typically using a heuristic. The goal is to

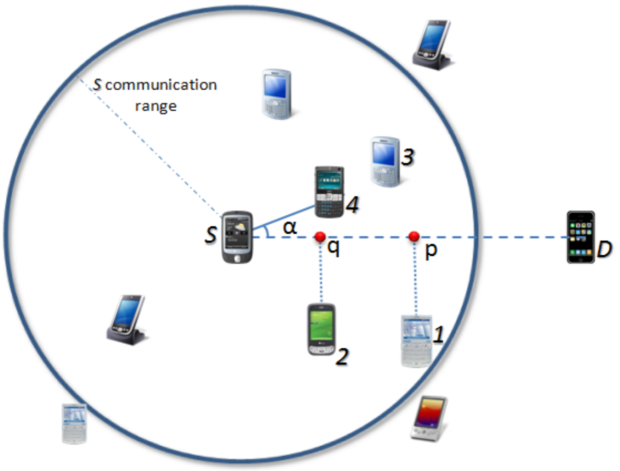


Figure 6.1: Strategies used by some forwarding algorithms

avoid redundant topology information so that the network can work more efficiently. Clustering algorithms are often modeled as graph problems such as the Minimum Connected Dominating Set (MCDS) [49]. This problem asks for the minimum subset of nodes V' in the original graph $G = (V, E)$ such that V' forms a dominating set of G and the resulting sub-graph of the MCDS has the same number of connected components as G. In other words, if G is a connected graph, so is the resulting sub-graph. MCDS is a NP-complete problem [48], and thus, we must look for approximate solutions [11]. In the case of the clustering algorithm, nodes in the dominating set represent the cluster-heads and the other nodes are their neighbors. An inherent characteristic of an ad hoc network, which makes this problem much more difficult, is that its topology is dynamic. The cluster heads can be selected using either deterministic or non-deterministic approaches:

- A deterministic solution is similar to a distributed synchronous algorithm in the sense that it runs in rounds. In this case there is just one round, and after finishing it the cluster-heads are chosen. Suppose we have a node and its neighboring nodes, i.e., its one-hop neighborhood. The lowest ID solution selects the node with the lowest identifier among these neighbors to create the Minimal Dominating Set (MDS) [48], whereas the max degree solution selects the node with the highest degree [65] [97]. The MOBIC solution examines the variations of RSSI (Received Signal Strength Indicator) signal among them to select the cluster-head [13].

- A non-deterministic solution runs multiple incremental steps to avoid variations in the selection process and to minimize conflicts among cluster-heads in their one-hop neighborhood. Examples of this approach are CEDAR [97], SPAN [29], and solutions based on a spanning tree algorithm [49].

6.3.2 Power-Based Control Algorithms

A mobile node in a MANET needs an energy source (typically a battery) to be able to execute all its tasks. Batteries need to be recharged to provide a continuous energy supply for a node. To extend the lifetime of nodes in an ad hoc network, we need algorithms to determine and adaptively adjust the transmission power of each node so as to meet a given minimization goal and, at the same time, maintain a given connectivity constraint. Some possible minimization goals are control the maximum or average power and define a maximum or average connectivity degree. Some connectivity constraints are a simplex communication or

a full-duplex communication (biconnected). Ramanathan and Hain [86] propose a topology control algorithm that dynamically adjusts its transmission power such that the maximum power used is minimized while keeping the network biconnected.

6.4 Further readings

The literature on topology control is vast, eventhough it is mainly devoted to ad hoc and sensor networks. In fact, one can find a wide range of good proposals, to solve specific problems, introductory surveys and books dedicated to this subject that can give a broader and deeper view of the subject. Good surveys are the works of Rajaraman [85] and Santi [92]. Two good books devoted to topology control are the works of Santi [91] and Labrador [70].

Chapter 7

Dynamic Topology Implementation for CHORIST

This chapter presents the implementation and evaluation of a distributed topology management algorithm for implementing the CHORIST architecture. CHORIST is a European Commission project that addresses environmental risk management focusing on natural hazards and industrial accidents [33]. The CHORIST consortium defined the desired topology but this work is the first one to present an implementation of it. The proposed algorithm is able to dynamically adapt to the nodes' mobility while maintaining the desired topology.

7.1 Introduction

The deployment and management of nodes in wireless PSNs is a fundamental and challenging problem. A well-defined and well-maintained network structure is an indispensable step to enable the creation of efficient higher layer algorithms [12]. For this reason topology control becomes a basic functionality to enhance scalability and capacity for large-scale networks [91]. Unlike in other networks the main concerns in public safety networks are rapid deployment and survivability [12].

The main contribution of this chapter is the proposal of a stable and efficient solution for implementing and managing the structure designed by the CHORIST project [33], taking into account the constraints imposed by the communication model. The backbone topology, depicted in Figure 7.1, is composed of Cluster Heads (CHs), Mesh Routers (MRs) and Relay Nodes (RNs). All the nodes' roles must be defined dynamically, using only local information and following the channel model defined by the consortium [84].

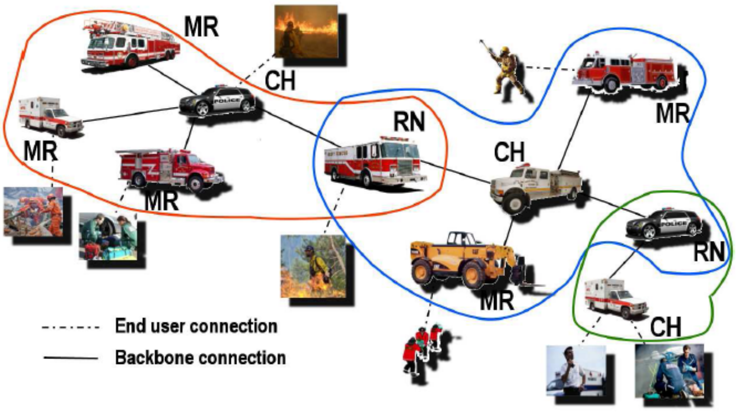


Figure 7.1: CHORIST network description and components.

The CHORIST structure was designed to be efficient and to decrease interference among nodes. Unlike other solutions, hierarchical structures are normally scalable and decrease the overall need for control messages among the nodes [14]. However, creating and maintaining such a structure has a cost. This cost can be measured in terms of bandwidth and delay. We consider that understanding the mechanics of such costs, and the tradeoffs involved, is an important step to enabling the creation of efficient and useful networks. Our proposal builds and efficiently coordinates the proposed CHORIST two-level hierarchical topology.

7.2 Chorist architecture

The core of the CHORIST network is a two-level hierarchical structure. A firefighter, for example, could use any kind of node as an access point, however, inside the proposed structure each node has its specific role. Cluster Heads (CHs) are the nodes responsible for managing the radio resources for their clusters. Relay Nodes (RNs) are the nodes that are part of two, or more, clusters and act as a bridge between them. Mesh Routers (MRs) are the nodes attached to CHs; they obey the CHs scheduling in order to communicate with other nodes. Nodes not yet attached to the network, and those that for some reason have lost their roles, are called Isolated Nodes (IN). If required, an IN may become a CH or a MR. The organization of these elements follows a well-defined and strict composition. Two CHs cannot be directly connected, neither can two RNs. For example, if a CH needs to exchange control data with another CH, the messages must be forwarded through a RN. This is done to avoid two CHs being physically located close to each other and have a more uniform cluster distribution.

The CHORIST backbone follows the channel model defined by the OpenAirInterface [84]. The main architecture of CHORIST, is derived from the OpenAirInterface adopted channel model and frequency reuse pattern. From the topology management point of view the two main constraints of the channel model are: no CH should be in the range of another CH and broadcast channels are reserved for CHs: no other node should broadcast messages. Two neighboring MRs may communicate directly, if previously agreed, but the communication must be direct, not through a broadcast channel. A MR, when inside a CH area, should be attached to it. Figure 7.2 shows all the allowed state changes for the CHORIST node status.

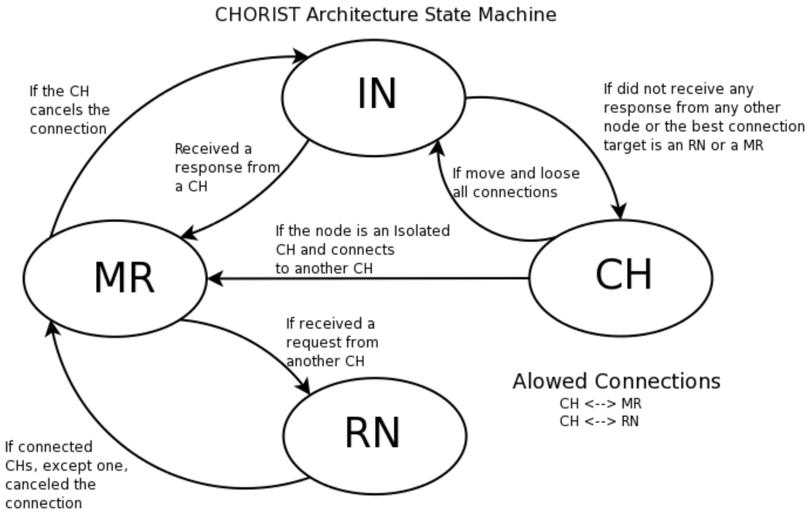

CHORIST Architecture State Machine
IN
MR
CH
RN
If the CH cancels the connection
Received a response from a CH
If did not receive any response from any other node or the best connection target is an RN or a MR
If move and loose all connections
If the node is an Isolated CH and connects to another CH
If received a request from another CH
If connected CHs, except one, canceled the connection
Alowed Connections
CH <--> MR
CH <--> RN

Figure 7.2: CHORIST state machine

7.3 Our implementation of CHORIST

Sometimes it is useful to abstract network problems as graph problems. If we consider the network as a graph, taking nodes as vertices and connections as edges we can reduce the CHORIST architecture to a two steps Weakly Connected Independent Dominating Set (WCIDS) [54].

For a given graph $G = (V, E)$ and a subset S of the set of vertices $V(G)$, S is called a dominating set if any vertex $v \in G$, v is either inside S or v adjacent to a vertex in S. In our case S can represent both the CH and the MR sets. A set S is called connected if S is a dominating set and the subgraph induced by S is connected. In graph theory a set of vertices is called independent if no two elements in it are adjacent, i.e. there is no edge that connects any pair of vertices of the set. In the CHORIST architecture we have exactly the same configuration: the CH set must be a dominating set, since all MRs and RNs should be connected to a CH. Moreover, two CHs should not be in the range of each other. It is important to notice also that the RN set also needs to be a dominating set, regarding the formed CH set. I.e. if we consider the CH set as S, then $V(G)$ would be the whole network. If we consider the MR set as S, then $V(G)$ would be the selected CH set. This makes the problem even more interesting. The minimum independent set is the one with the lowest possible cardinality. The minimum dominating set is desirable since we want to decrease, as much as possible, the number of links and signaling messages exchanged among CH nodes.

Reducing the CHORIST network structure to the solution of the WCIDS problem helps understanding the topology, but does not solve the problem. Unfortunately, both the dominating set and the connected dominating set problems are proven to be NP-Complete [34] [48]. One of the most well-known heuristics for solving the connected dominating set problem is the centralized approach proposed by Guha and Khuller [49]. Although there are distributed implementations of this heuristic [47], the CHORIST topology is not exactly the same and the distributed approach cannot be used directly in this case. Furthermore, we must also consider that, unlike graphs, that are static, a network topology is dynamic: nodes may attach and detach from the network at any time, so the graph changes constantly.

Our protocol assumes a reactive approach; nodes perceive changes in their vicinity through periodic connections update messages sent by the CHs. As a result, the delay to react to changes is linked to the frequency of the update messages. If a mobile node gets out of the CH range it takes a few seconds for the node to realize that it may be in an area uncovered by any other CH and, thus, it is its duty to become a CH. Algorithm 2 presents the protocol in further details. Figure 7.3 shows the message passing diagram for the CH discovery process and creating a RN one, the (1) sign in the diagram indicates that the communication occurs with a single message transfer.

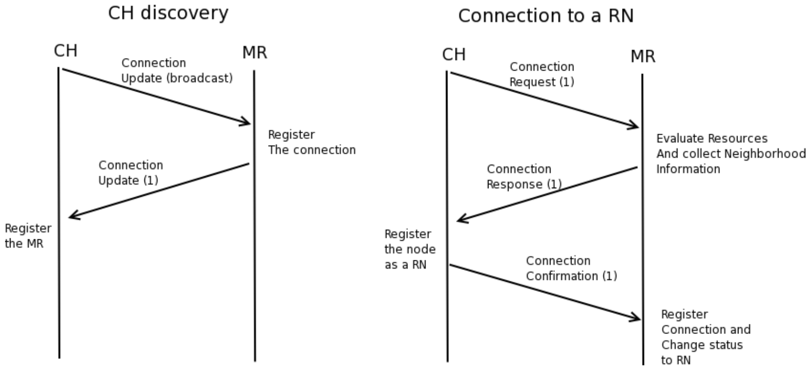

CH discovery
CH
MR
Connection Update (broadcast)
Register The connection
Connection Update (1)
Register the MR
Connection to a RN
CH
MR
Connection Request (1)
Evaluate Resources And collect Neighborhood Information
Connection Response (1)
Register the node as a RN
Connection Confirmation (1)
Register Connection and Change status to RN

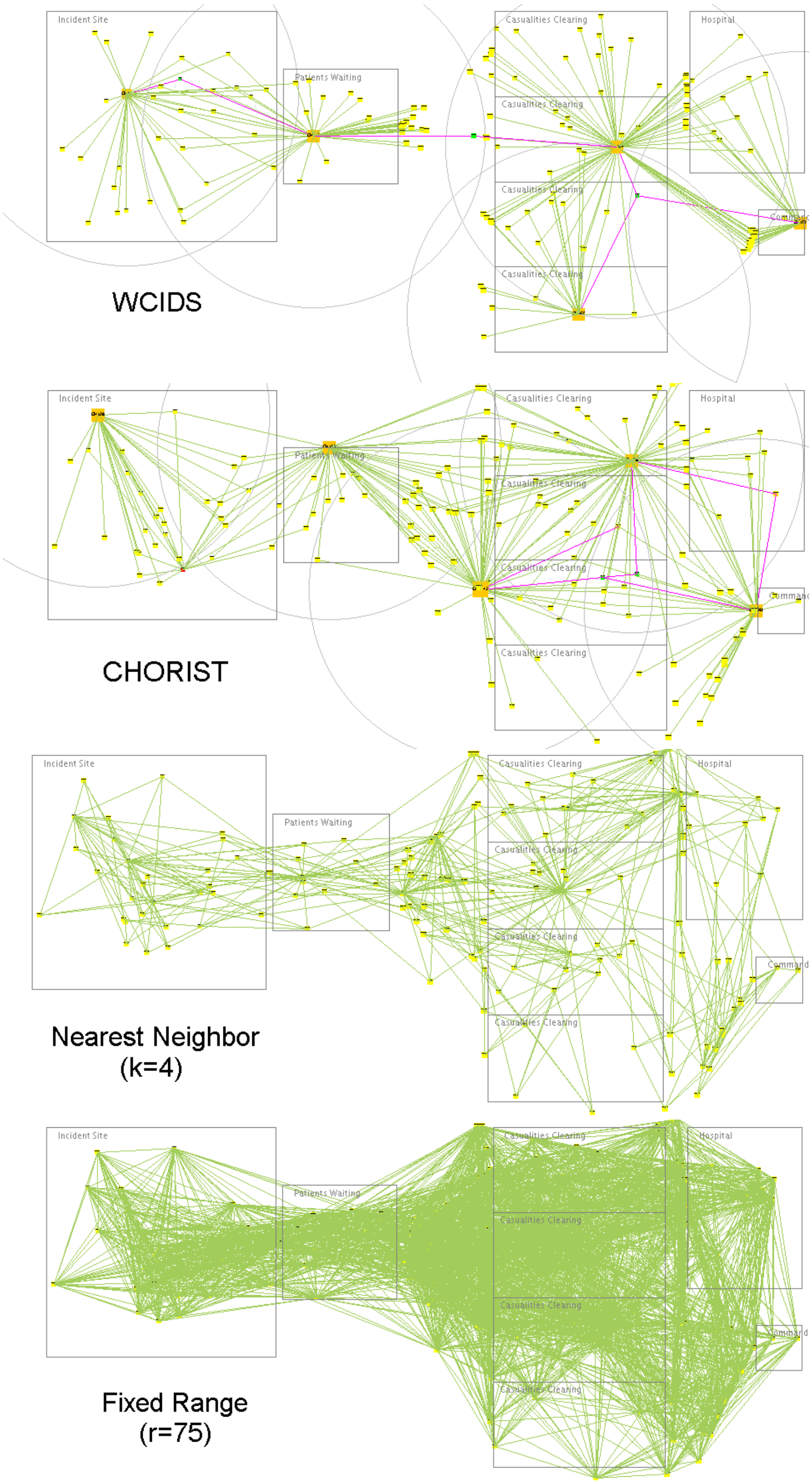
Figure 7.3: CHORIST CH discovery and RN connection request message transfer

The CHORIST hierarchy provides scalability to the network structure. In [14] Royer argues that hierarchical networks present better performance and are more robust. They enable the achievement of higher data throughputs. Another important characteristic of hierarchical networks is the decrease in the number of required links among nodes. This can be perceived from Figure 7.4, which compares the connectivity of the four evaluated methods. The number of links varies considerably among the approaches. The first diagram, WCIDS, shows the result of the application of the Weakly Connected Independent Dominating Set over the network connection graph. The second diagram shows the application of our technique over the same scenario. We can see that even though the clusters are at different positions the number of CHs, represented by bigger squares, is the same. Moreover, the number of generated edges is also nearly the same, even though for our approach they are generated dynamically and only with local information. The next two diagrams show the same nodes distribution connected through planar techniques. The number of created links, for both, is considerably bigger. In the k-nearest neighbor technique, each node connects to at least k neighbor nodes. For the fixed range technique, if two nodes are within the communication range of each other they are connected.

An important characteristic we want to emphasize about the problem is that both, RN and CH sets, should be WCIDS and as small as possible. However, both sets are not independent. The RNs selected to compose the RN WCIDS must be selected among the CH WCIDS nodes' neighbors.

Algorithm 2 - The CHORIST high level algorithm, from the point of view of the node

```
 1: Node Arrives (actual status = IN);
 2: Waits for Connection Updates;
 3: if (received an Update message) then
 4:    Sends a Connection Request to the CHs;
 5:    Evaluates responses;
 6:    Sends a Connection Confirmation to the best option;
 7:    Becomes a MR;
 8: else if (number of trials less than 3) then
 9:    Returns to 2;
10: else
11:    Becomes a CH;
12:    Broadcasts a Connection Update;
13: end if
14: Waits for messages;
15: if (received a Connection Request && node is a MR a RN or a CH) then
16:    Responds with a Connection Response informing all its neighbors;
17: else if (received a Connection Confirmation && node is a CH a MR or a RN) then
18:    Registers the connection;
19:    if (requester is a CH && actual status != CH) then
20:       Becomes a RN;
21:    end if
22: else if (received a Connection Response) then
23:    Sends a Connection Confirmation;
24:    Registers Connection;
25: else if (received a Connection Update) then
26:    Registers the Update;
27:    Registers the Neighbor;
28:    if (actual state == CH && sender == CH) then
29:       There is another CH in the range;
30:       Decides, based on the his and the sender's ranks, whether to give up being a
          CH or not;
31:       Sends an Update Message;
32:       Waits a Random time;
33:    end if
34:    From time to time Evaluate Updates to find not Connected CHs;
35: else if (received a Connection Cancel) then
36:    Removes the connection;
37:    Reevaluates actual state (may become a MR);
38: end if
39: Return to 14;
40: //From time to time evaluates the connections and sends updates
41: if (connection timeout occurred) then
42:    Removes neighbor
43:    Reevaluates state (may became a IN or a MR)
44:    if (is a IN) then
45:       Return to 2;
46:    end if
47: end if
48: From time to time sends a Connection Update for the connected nodes;
```



WCIDS

CHORIST

Nearest Neighbor (k=4)

Fixed Range (r=75)

Figure 7.4: The connectivity of the different topology control strategies for the evaluated scenario (300x200m area, 150 nodes, 75m communication range)

Our solution fulfills this and all the other requirements of the CHORIST architecture requirements.

7.4 Experiments for the CHORIST Network Implementation

7.4.1 Environment

The evaluations were made using Sinalgo simulator [96] in a $2000x2000m^2$ area for the WCIDS. When using the Aschenbrucket al. distribution model we used the same area described in [9], $300x200m^2$ area. The area is composed of one incident site, one patient waiting area, four casualties treatment areas, one hospital and one command center. Figure 7.5 presents a typical cumulative histogram of nodes distribution through the space over the simulation time. We can see that the corridors between the defined areas are the places with higher concentration of nodes. This occurs because nodes are constantly moving through these spaces to get patients from one area and move them to another area. The peaks are the entrance ports of the areas, each node should wait for a random interval in this area to get or drop patients, so these places are supposed to have a bigger concentration of nodes.

We vary the number of nodes and their communication range. All experiments were conducted using Linux Fedora Core release 6 on an Intel Xeon 1.86GHz machine with 16GB of RAM. All graphs are presented with a confidence interval of 99% and each point is the result of the mean of 34 runs of 3 hours simulation time with different network configurations and 1% of message loss. For the comparisons with the WCIDS algorithm scenarios, nodes arrive randomly and are placed uniformly over the observed area.

The centralized WCIDS implementation is an adaptation of the Guha and Khuller [49] algorithm and works directly over the connection graph. This implementation is an oracle that knows the position of all nodes and uses this information to create the minimum arrangement in an offline manner. The final result is the best possible one and is hardly achievable with distributed algorithms, where nodes have only local information and new nodes arrive at different moments throughout the network lifetime. However, it represents a base of comparison to evaluate how far our implementation is from the theoretical minimal CH/RN optimal solution.

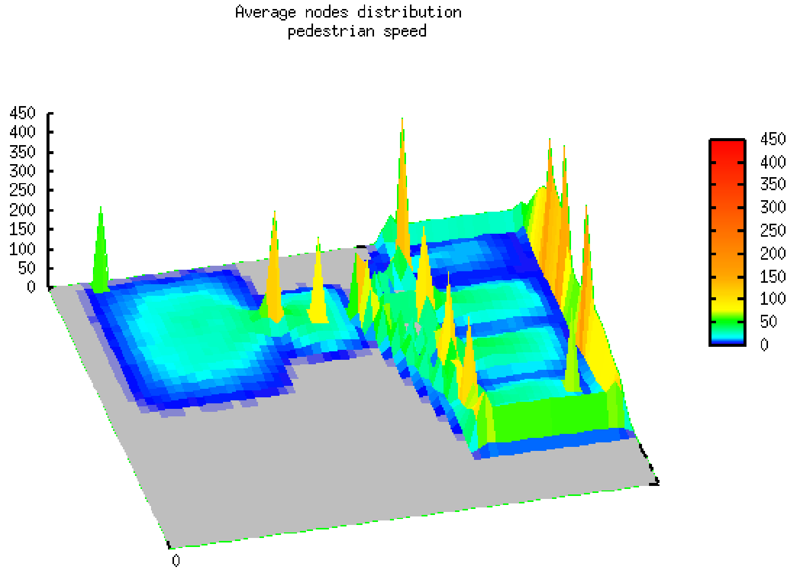


Figure 7.5: Cumulative histogram of nodes positions during a typical one hour simulation time

7.4.2 Minimum WCIDS proximity

Figure 7.6 presents a comparison between CHORIST and the offline WCIDS implementation for different density scenarios. The number of CHs created for both is close, normally with an overlap on the 99% confidence interval. This is the case even though our approach works in a distributed way, nodes just have local information and nodes arrive randomly during the network uptime. We can also perceive that the number of clusters increases sub linearly, relative to the number of nodes in the network. This indicates that for the CHORIST network the number of clusters has a closer relation to the are covered than the number of network nodes. On the other hand, the number of nodes per cluster increases almost linearly with the number of network nodes. Nevertheless the number of cluster nodes for both approaches, CHORIST and WCIDS stays basically the same for all evaluated scenarios. The number of RNs generated by our implementation of CHORIST has, on average 6.75% more RNs than the WCIDS implementation. This occurs mainly because for our approach, CHs chose their RNs in a selfish way. A CH picks the most interesting nodes, for its point of view to become its RNs, although this does not necessarily mean that these are the best nodes from the network point of view. Thus, it could happen that two CHs consider two different nodes to be relays between them, one for each CH, i.e. one RN on each communication direction. However, the increase in the number of RN has a good side since it decreases the size of the communication paths passing through the CHs.

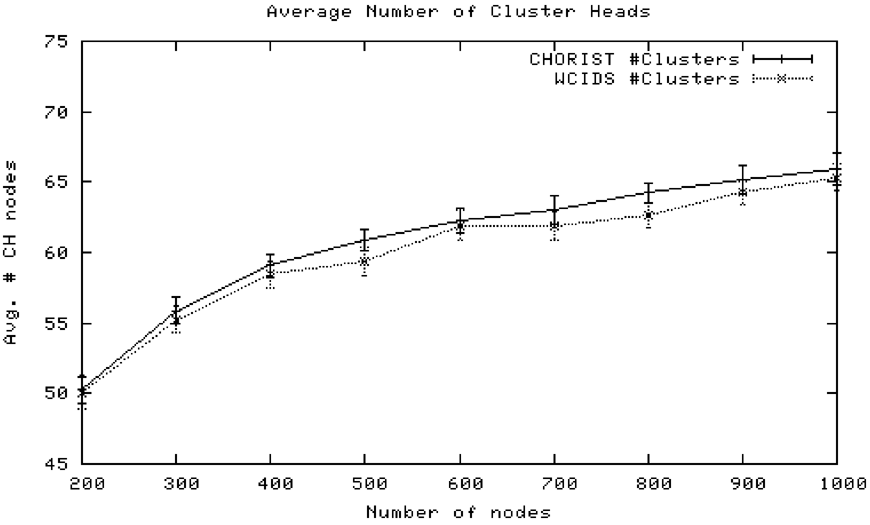


Figure 7.6: Average number of clusters on the network varying the number of nodes on the network and for 200m communication range

Figure 7.7 presents the average path lengths, between CHs, in the network. This measure is important because it reflects the traffic of control messages, e.g. scheduling, topology management, among the CHs. This traffic can be intense, so the shorter the paths the better. As we can see the size of the path for the CHORIST nodes is smaller than the ones for the WCIDS implementation. The variability given by increasing the number of CHs and RNs ensures a more diverse set of path options leading to a smaller average path length.

7.4.3 Mobility resilience

To evaluate the CHORIST network stability and availability we use the same distribution and mobility scenario proposed by Aschenbruck et al. [9]. Aschenbruck et al. propose a distribution model that divides the target area into different purpose specific sub-areas, e.g. incident location, patients waiting for treatment, hospital. Even though Aschenbruck et al. model is far

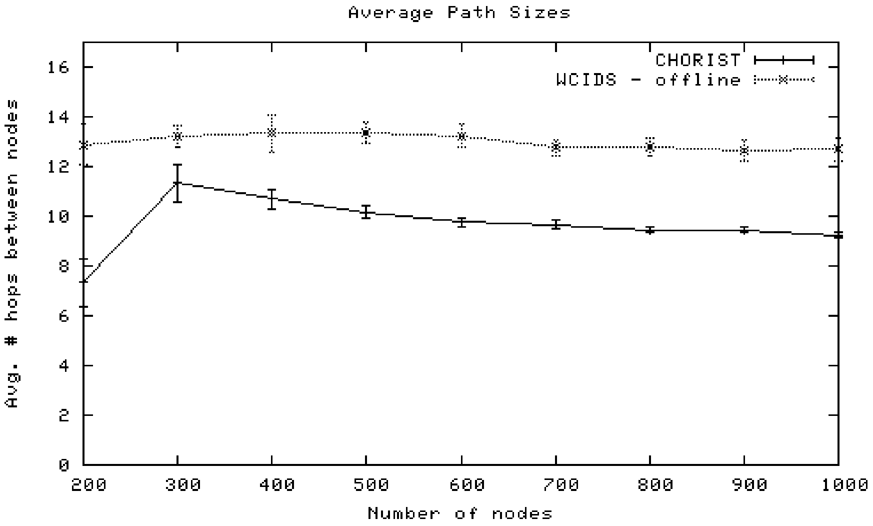


Figure 7.7: Average path size passing only through CHs and RNs, varying the number of nodes on the network and using $200m$ communication range

from covering all the possible mobility and distribution scenarios for PSNs, it is an elegant model based on a real maneuver simulation. However, instead of just evaluating the connectivity, as in [9], we implemented the protocols and compared our results with those of the other algorithms, under the same conditions.

We use the same area size, nodes distribution and organization described in [8] [9]. However, we simulated the network in two distinct situations, the first one when all nodes have pedestrian speed, ($0.5m/s$ on average and variance of $1m/s$) and another scenario where we have a mix of pedestrian and vehicular nodes. For the second scenario nodes inside the defined zones are pedestrian and nodes that travel from one zone to the other have vehicular speed (average of $40Km/h$ and variance of $4Km/h$).

The work of Aschenbruck et al. [9] does not propose a new algorithm, but compares three exiting planar proposals. No hierarchical strategy is evaluated, even though hierarchical networks are more scalable than planar ones.

One typical example of the application of the evaluated methods can be observed in Figure 7.4. In the k nearest neighbor technique, each node connects to at least k other neighbor nodes. However, one node can accept connections to other nodes that have less than k. This increases the network stability but may lead to some nodes having more than k links. The Algorithm 3 describes the technique. For the fixed range technique, if two nodes are within each other's communication range they should be connected. The protocol for both cases is nearly the same, the difference being that the fixed range does not consider the number of connections, if the node received a Connection Update it connects to the node that sent the update.

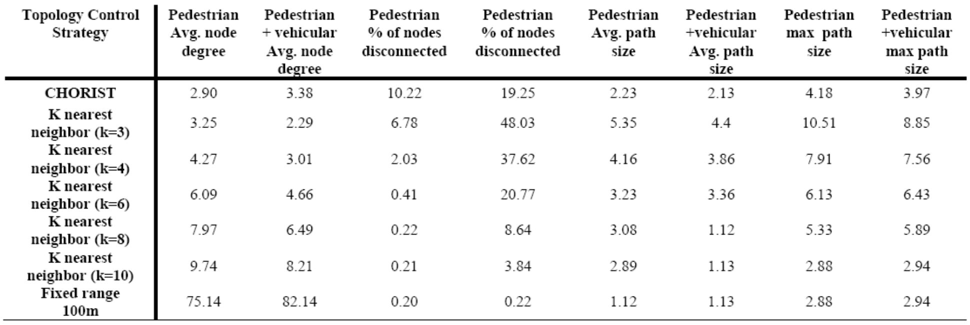
Algorithm 3 - The k nearest neighbor algorithm

```
Waits for messages;
if (received a Connection Update) then
    if (the number of connections < k) then
        Sends a Connection Request;
    end if
else if (received a Connection Request) then
    Responds with a Connection Response;
    Registers the connection;
else if (received a Connection Response) then
    Registers the connection;
end if
//From time to time evaluates the connections and sends updates
if (connection timeout occurred) then
    Removes connection
end if
From time to time broadcasts a Connection Update;
```

When exposed to higher mobility rates, transmission failures, delays, and lack of information the performance of the planar algorithms were slightly worse than those reported in [9]. Table 7.1 summarizes the obtained results. We can observe that the degrees of the nodes for the CHORIST architecture are the lowest ones, for both pedestrian and vehicular speed experiments. The percentage of nodes disconnected, columns of the table, are measured from the point of view of each node. They represent what percentage of the other nodes in the network are unreachable, from each node, at each time. For example, for an isolated node this value would be 100%, for the others, if all are connected, it would be 0.67%. Two nodes are connected only if the protocol recognizes them as being attached, and if they are indeed inside the communication range.

For all the evaluated protocols the addition of the vehicular speed nodes had a considerable impact. Every communication protocol needs a time to adapt to topology changes. As nodes are mobile, the view a node has of the topology, connectivity and other nodes' position may be outdated. Sometimes a node recognizes other nodes, which moved, as connected and at the same time may fail to recognize nodes within range as reachable. The CHORIST structure is a more sophisticated one, and it takes slightly more time for the nodes to get organized (e.g. recognize new clusters, attach to them). For this reason more nodes fail to recognize connections, when compared with the k-neighborhood algorithms. However with the increase in mobility, the k neighborhood needs considerably more resources, i.e. links, to reach the same results as those presented by the CHORIST structure.

From Table 7.1 we also have the average path length and the average longest shortest path for each node ($\forall i, j \in V(G) : ls = max_{ij} d(i, j)$), both measured in number of hops. Again, CHORIST paths were smaller than the corresponding k-neighborhood ones. The k-neighborhood algorithm needs $k = 8$ or $k = 10$ to present the same path lengths CHORIST does. However, this also means spending more resources to generate and maintain the structure.



Topology Control Strategy	Pedestrian Avg. node degree	Pedestrian + vehicular Avg. node degree	Pedestrian % of nodes disconnected	Pedestrian % of nodes disconnected	Pedestrian Avg. path size	Pedestrian +vehicular Avg. path size	Pedestrian max path size	Pedestrian +vehicular max path size
CHORIST	2.90	3.38	10.22	19.25	2.23	2.13	4.18	3.97
K nearest neighbor (k=3)	3.25	2.29	6.78	48.03	5.35	4.4	10.51	8.85
K nearest neighbor (k=4)	4.27	3.01	2.03	37.62	4.16	3.86	7.91	7.56
K nearest neighbor (k=6)	6.09	4.66	0.41	20.77	3.23	3.36	6.13	6.43
K nearest neighbor (k=8)	7.97	6.49	0.22	8.64	3.08	1.12	5.33	5.89
K nearest neighbor (k=10)	9.74	8.21	0.21	3.84	2.89	1.13	2.88	2.94
Fixed range 100m	75.14	82.14	0.20	0.22	1.12	1.13	2.88	2.94

Table 7.1: Summary of the disaster area scenario results for both pedestrian and pedestrian plus vehicular scenarios

7.5 Conclusions

This chapter presented an implementation and evaluation of the network architecture proposed by the CHORIST project. The problem was reduced to the minimum Weakly Connected Independent Dominating Set. Even though this problem is NP-complete, our solution reaches values close to the theoretical minimum, using only local information and with nodes arriving at the network at different times. From the mobility experiments we can also conclude that implementation of the CHORIST architecture is stable and able to guarantee relatively low percentage of disconnected nodes while simultaneously decreasing the average path lengths and number of links per node. The proposed topology is stable and resilient to nodes mobility.

Chapter 8

Market Based Strategy

Public Safety Networks are an extreme and challenging environment for topology management protocols. As stated in Section 2.8.1 the main concerns for PSNs are rapid deployment and survivability [12]. These concerns are also important in other networks, but are not normally the main concerns. Moreover, the network requirements for different disaster scenarios may differ greatly. This chapter describes a flexible distributed algorithm to perform network admission control and topology management for public safety wireless networks. The proposed algorithm is anot only able to dynamically adapt to different network requirements, but also to create homogeneous clusters, where the number of mobile routers attached to each cluster is roughly the same. The technique successfully creates and maintains the desired topology relying only on an elegant and customized cost function.

8.1 Introduction

The deployment and the management of nodes for wireless mesh/ad hoc networks are challenging problems and they become even more interesting when we consider them in the context of public safety networks. Not only is this kind of network, by nature, life-critical but they also have strict requirements. Moreover, these requirements may vary significantly for different disaster sites [85]. A stable network structure is crucial for enabling the creation of efficient higher layer algorithms and at the same time enhancing scalability and capacity for large-scale wireless ad hoc networks [91].

PSNs must be reliable and endure even when deployed through rough environments. The algorithms running on this kind of network should take this into account. The network organization is important to guarantee stability and provide communication even during the most severe conditions. Simple structures, such as a planar network, may be easier to deploy and to maintain, but this kind of organization is neither scalable nor appropriate for use in large scale deployments. Structured networks, on the other hand, are more scalable, but the structures must be created and maintained. This work focuses on hierarchical network topologies. Even though the proposed method is general and adapted to any wireless mesh network, we believe that we can benefit if we apply it to highly dynamic and unpredictable networks, as is the case with public safety networks.

8.2 Background

To the best of our knowledge, no other work approaches the topology adaptability problem in the same way we do. In most cases, if the topology requirement changes a completely new algorithm must be designed and deployed.

In [73], Mainland et al. propose the market-based macro-programming paradigm for controlling the behavior of the nodes in a sensor network. Even though the main focus of both works is different, both have the same inspiration. We use the free market economic concept to control the network nodes' behavior and reach stable final configurations. The first welfare theorem states that any free market system will eventually reach Pareto optimality [112]. A Pareto optimal allocation is the one where no one could be made better off without making someone else worse off. In other words, a Pareto allocation is a fair equilibrium point. It is the best allocation one can expect to reach and any change could hurt some of the participants.

Our approach consists of creating a free market environment where nodes can trade the connections freely. We consider that the quality of the service offered by two distinct providers is the same. Each node is free to set its prices, and these vary in accordance to the node load and type; however, among nodes of the same class the basic price is the same. Nodes are free to choose their provider and to change providers, if they have some gain in doing so. In our final setup no node wants to or can change providers without paying more and no provider can increase prices without losing clients. Thus this Market Based Strategy (MBS) reaches an equilibrium that is Pareto optimal.

8.3 Objectives

To accomplish the main objective of this part of the thesis, the creation of stable topologies, the algorithm proposed here has three main objectives.

1. Ensure a stable, or at least as stable as possible, network as fast as possible while respecting the desired architecture. As the target application are PSNs, the topology and mechanisms to guarantee connectivity should be stable, trustworthy and rapidly deployable.

2. Creation of homogeneous clusters. Clusters should not only have roughly the same size but it is also important to be able to control and fine tune the network shape and cluster sizes. Cluster heads must be able to optimally handle communication among nodes inside their clusters and exchange key information with neighbor nodes rapidly and efficiently. The optimal number of clusters and elements by cluster vary from one disaster scenario to another.

3. Finally, keep the number of clusters as low as possible, while keeping the clusters of a reasonable size. Having the minimum number of clusters possible not only decreases the number of required RNs but also decreases the number, and size, of control messages in the final network.

   The technique described here intends to create and maintain well-defined wireless mesh network architectures in a flexible and dynamic way. We want to be able, by just adjusting a set of parameters, to change the behavior of the whole network without deploying new equipment or protocols. The algorithm must be able to provide an easy way to change the network behavior, i.e. number and size of clusters, while respecting the topology constraints. The proposed scheme is general and can be adapted to any wireless mesh network architecture. As a proof of concept, we applied the method to three different hierarchical networks: a simple clustering algorithm, the CHORIST one and a third, more complex organization.

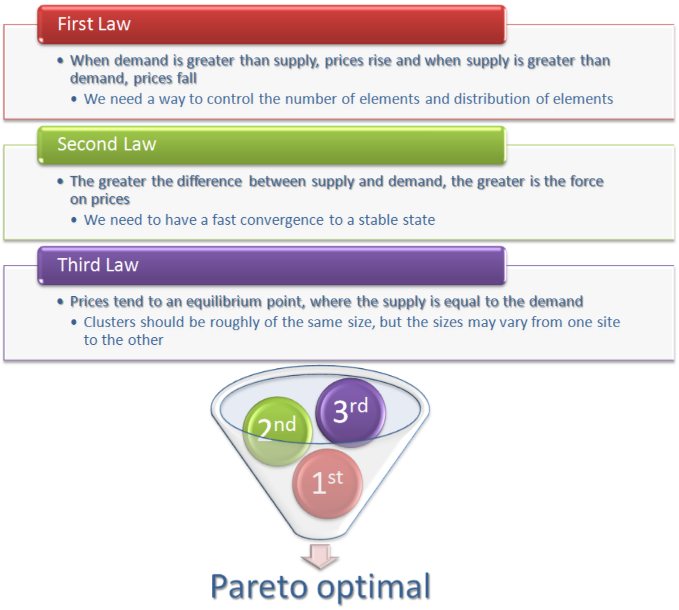
8.4 Market-based topology management

The MBS described here intends to create and maintain well-defined wireless mesh network architectures in a flexible and dynamic way. The technique in fact has the power to change the whole behavior of the network by adjusting a small set of parameters, without the need for special equipment or complex protocols.

We base our solution on the economy laws of supply and demand to dynamically organize the network. The first law of supply and demand states that when demand is greater than supply, prices rise and when supply is greater than demand, prices fall. The power of such forces, rise and fall, depends on how great the difference between supply and demand is. The second law of supply and demand, then, states that the greater the difference between supply and demand, the greater is the force on prices. The third law states that prices tend to an equilibrium point, where the supply is equal to the demand [57].

If we align our main objectives with the laws of supply and demand we will see that these three laws map perfectly to the main requirements of a topology management algorithm. We may map our need to control the number of clusters to the first law of supply and demand. Controlling the prices of each kind of service offered in the network, we can control the number of elements offering such service. The second objective is to have a fast convergence to a stable state. This requirement is met by applying the second law, since the bigger are the differences among supply and demand the faster is the convergence. Finally, recall that our third objective is to maintain an well balanced and as stable as possible network, while respecting the desired architecture. Clusters should not only have roughly the same size but we should have an easy way to control and fine tune that size. Cluster heads must be able to optimally handle the communication among nodes inside their clusters and exchange key information with neighboring nodes fast and efficiently. However, the optimal number of nodes per cluster depends upon many factors, such as number of attendees and agencies involved, kind of disaster and environmental conditions. These issues are covered by the third law, since the final topology is expected to be a Pareto optimal arrangement [112] and hence it should be stable and fair among all the participants. Figure 8.1 presents these relationships schematically.

The basic mechanism of the evaluated protocols is as follows: whenever an IN arrives in the network, it broadcasts a connection request for the nodes nearby. This request is answered by all the MR/RN/CH in the region. The neighboring nodes answer with their status, number of connections and link



First Law

- When demand is greater than supply, prices rise and when supply is greater than demand, prices fall
  - We need a way to control the number of elements and distribution of elements

Second Law

- The greater the difference between supply and demand, the greater is the force on prices
  - We need to have a fast convergence to a stable state

Third Law

- Prices tend to an equilibrium point, where the supply is equal to the demand
  - Clusters should be roughly of the same size, but the sizes may vary from one site to the other

Figure 8.1: Relation of the economic laws of supply and demand and the requirements for PSNs topology management algorithms

status. This information is used to define a connection cost to each one of the possible sponsor nodes. The information in the answer packets and the cost function determine to which node the IN will attach. The cost policy states that, considering all the given data, the lowest cost sponsor should be chosen.

To increase the network stability a node just gives up being a CH or a RN if it moves and loses all its connections, or if it moves and enters in conflict with other well established, lower cost, CH/RN in the region.

A node should always try to attach to the node that presents the lowest attachment cost. To decrease the number of CHs, the chosen basic connection costs should give greater priority to CHs in detriment of the other kind of nodes. Only if there are no CHs around or they are completely overloaded should an IN decide to attach to a MR or a RN and become a new CH. Similarly, to promote a more homogeneous load balance, the cost function guarantees that an IN node will always attach to the least loaded, or the best suited sponsor. Algorithm 4 describes in further details the method when maintaining the CHORIST network architecture.

The cost function can be as simple or as complex as one may need. For

Algorithm 4 - Market Based Strategy CHORIST topology control high level algorithm

```
 1: Node Arrives (IN);
 2: IN sends a connection request through broadcast;
 3: Waits for the responses;
 4: if (received any Connection response) then
 5:    Weights the costs of the responses;
 6:    Sends a connection confirmation to the node with the lower cost
 7:    if (connected to a CH) then
 8:       Becomes a MR;
 9:    else if (connected to a MR or to a RN) then
10:       Becomes a CH;
11:    end if
12: else
13:    if (number of trials less than 3) then
14:       Returns to 2;
15:    else
16:       Becomes a CH;
17:       Sends a connection Update;
18:    end if
19: end if
20: Waits for messages;
21: if (received a Connection Request) then
22:    Responds with a Connection Response informing all its connections;
23: else if (received a Connection Confirmation) then
24:    Registers the connection;
25:    Reevaluates state (may become a RN);
26: else if (received a Connection Response) then
27:    if ( interesting) then
28:       Sends a Connection Confirmation;
29:       Registers Connection;
30:       Reevaluates state (may become a RN);
31:    else
32:       Sends a Connection Cancel;
33:    end if
34: else if (received a Connection Update) then
35:    Registers the Update;
36:    From time to time Evaluate Updates to find not Connected CHs;
37: else if (received a Connection Cancel) then
38:    Removes the connection;
39:    Reevaluates actual state (may become a MR or a IN);
40: end if
41: Returns to 20;
42: From time to time broadcasts a Connection Update ;
```

this work our cost function considers basically the clusters' load. However, other factors could be taken into account as well, e.g. perceived quality of signal, number of blocked nodes and mobility pattern. The used function can be described as:

$$C = \beta_k + \sum_{i=0}^{n} \epsilon_i, \tag{8.1}$$

where C is the connection cost for one specific sponsor candidate and β_k is the basic connection cost for each kind of server. In a free market environment, there is no difference between the services provided by two distinct servers. For this reason the basic connection cost for all servers in the same class k, is the same. A class is a kind of of node, for CHORIST, for example, would be CH, MR or RN, n represents the number of nodes connected to this specific sponsor and ϵ_i represents the individual cost for each one of the already sponsored nodes. For the experiments we set ϵ to be one for each connection the node has, but this value can be gauged according to the topology needs. The last part of the formula provides an adaptive behavior that enables nodes to choose the best servers for their needs, i.e. the less loaded ones; however the formula could be much more complex.

The cost function calculation is a flexible way to control network connections and the topology behavior. By fine-tuning the cost function one can, for example, decrease the number of connections of each CH and increase, or decrease, the size of the clusters. This flexibility is interesting, mainly for PSNs where different disaster sites may have different needs and the network operation can be shaped as desired. By changing and broadcasting a new basic costs vector, one can even change completely the behavior of an already established network without any full software or hardware update.

8.5 Experiments for the MBS topology control

8.5.1 Environment

The evaluations were made using Sinalgo simulator [96] in a $2Km^2$ area. We vary the number of nodes and the communication range of the nodes. All experiments were conducted using Linux Fedora Core release 6 in an Intel Xeon 1.86GHz machine with 16GB of RAM. All graphs are presented with a confidence interval of 99% and each point is the result of the mean of 34 runs with different network configurations. The nodes arrive randomly and are placed uniformly over the observed area. As the experiments observed in

Section 7.4, the centralized implementation works as an oracle: its results are the best possible ones and unachievable with distributed algorithms. However, this offline implementation shows us how far the proposed algorithm is from the theoretical minimal CH optimal solution.

All experiments were conducted for different communication ranges of 50, 100, 150, 200, 250, and 300 meters. However, as the final results for these variations did not present any meaningful difference, we will present only the values obtained for the 200 meters communication range experiments. To evaluate the adaptability capacity of the proposed solution we defined different network configurations and node costs. Considering the implemented cost formula 8.1, if one needs, for example, a network with fewer CHs, it is only a matter of decreasing the basic CH connection cost and increasing the costs for other kind of nodes. In this way nodes will prefer to attach to an existing CH, as it is cheaper than to attach to other nodes to create a new CH. For each different target scenario the cost values should be adapted accordingly to the final desired network shape.

We created six different scenarios with different basic costs for each type of nodes. The basic cost configurations used in the experiments were:

- Configuration 1: favors the creation of clusters, as much as possible. It has high cost to connect to a cluster and low cost for connecting to other nodes. The basic connection cost values (β) are CH=20, MR=5, RN=1.

- Configurations 2 to 5: are variations over the standard configuration, smaller costs for attaching to CHs and larger ones for RNs and MRs. The objective of testing these configurations is to establish whether small variations of costs affect the algorithm behavior. β values are:

  - Configuration 2 CH=0, MR=2, RN=1
  - Configuration 3 CH=0, MR=5, RN=3
  - Configuration 4 CH=0, MR=7, RN=5
  - Configuration 5 CH=0, MR=20, RN=5

- Configuration 6: tries to shape the network as close as possible to the minimum WCIDS, the target configuration of the implemented offline approach. For this case values are: CH=0, MR=50, RN=45.

Configurations 1 and 6 are diametrically opposite in the sense that the first aims to stimulate the creation of CHs while the second aims to keep the number of clusters as small as possible. The differences among the configurations and the desired final network shape are expressed by the histograms in Figure 8.2. These histograms were created from typical runs of the simulation. We can observe that the technique really manages to control the network topology going from the extreme case of a nearly minimum number of CHs to the case where almost all nodes are CHs.

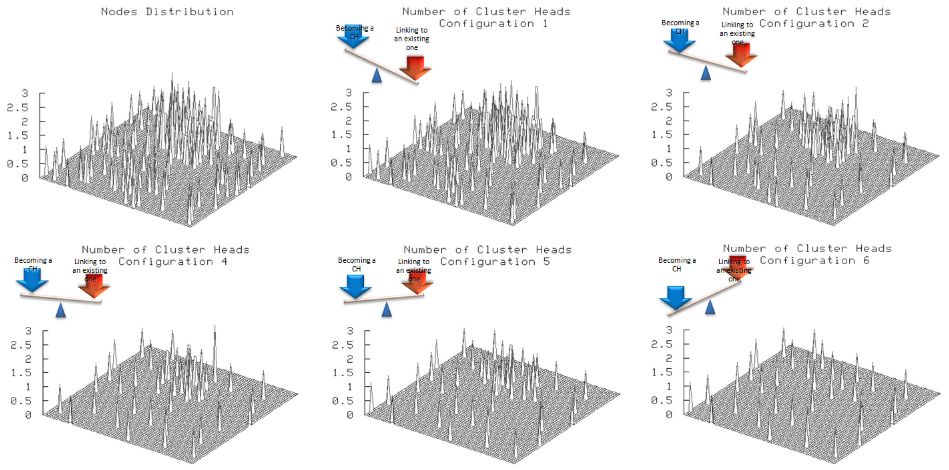


Figure 8.2: Number of cluster heads spread through the network according to the different evaluated configurations, for a 40% concentration network scenario.

To validate the technique we applied it to three different hierarchical network organizations. The three networks are a simple generic cluster, CHORIST and an interest group one. The aim here is to show that the technique is independent of the target architecture and at the same time it can shape the format of the final network topology. We will present the experiments in order of complexity of the topology protocols, from the simplest to the most sophisticated one.

8.5.2 Simple cluster experiments

The generic cluster algorithm is also a two layer one but simpler than the CHORIST architecture. CHs may be connected directly or through MRs, there is no RN role. Figure 8.3 shows an example of the expected behavior of the simple cluster algorithm. The minimum number of CHs for this scenario is also a WCIDS, where the CHs are not in the range of one another and the message exchange occurs through a common MR. Figure 8.4 shows the state machine for the generic cluster algorithm.

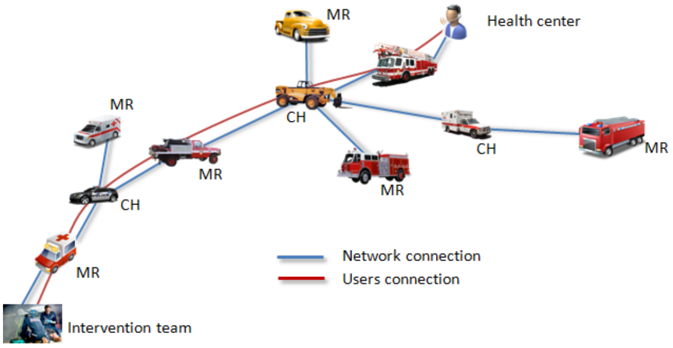


Figure 8.3: Simple cluster architecture, showing an end-to-end users communication

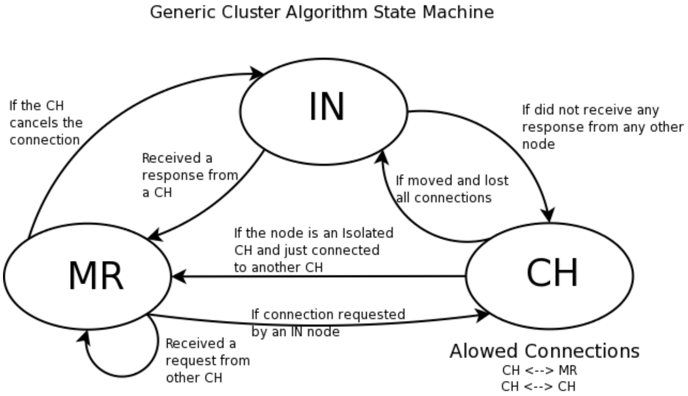

Generic Cluster Algorithm State Machine
IN
MR
CH
If the CH cancels the connection
Received a response from a CH
If did not receive any response from any other node
If moved and lost all connections
If the node is an Isolated CH and just connected to another CH
If connection requested by an IN node
Received a request from other CH
Alowed Connections
CH <--> MR
CH <--> CH

Figure 8.4: State machine for the generic cluster algorithm

The graph in Figure 8.5 shows the number of CHs for different network sizes for the simple clustering algorithm. As we can observe the number of CHs changes in the way it was expected to. The small changes in the cost values also show that using the technique one can even make a fine grain control of the network shape. With regard to the minimum CHs configuration, the values reached by Configuration 6 are quite close to the ones found by the minimum WCIDS algorithm, normally inside the 99% confidence interval range. However, it is worth reminding that the offline implementation, not only has the complete view of the network, but also works using the final configuration, while our approach, MBS, works only with local information, the CHs are assigned dynamically, the algorithm does not need to know the entire topology in advance and nodes join the network at different moments during the simulation time.

Another interesting characteristic we can notice from the graph in Figure 8.5 is the slope of the curves: for Configuration 1, where the CH attachment cost is abusive, the slope is more accentuated, and when the cost to attach to a CH decreases, the slope of the curve is given by the increase in the cost of the attachment to MRs and RNs. The differences between the two graphs are also expected since the evaluated protocols are different and have different elements. So the proportional connection costs are different.

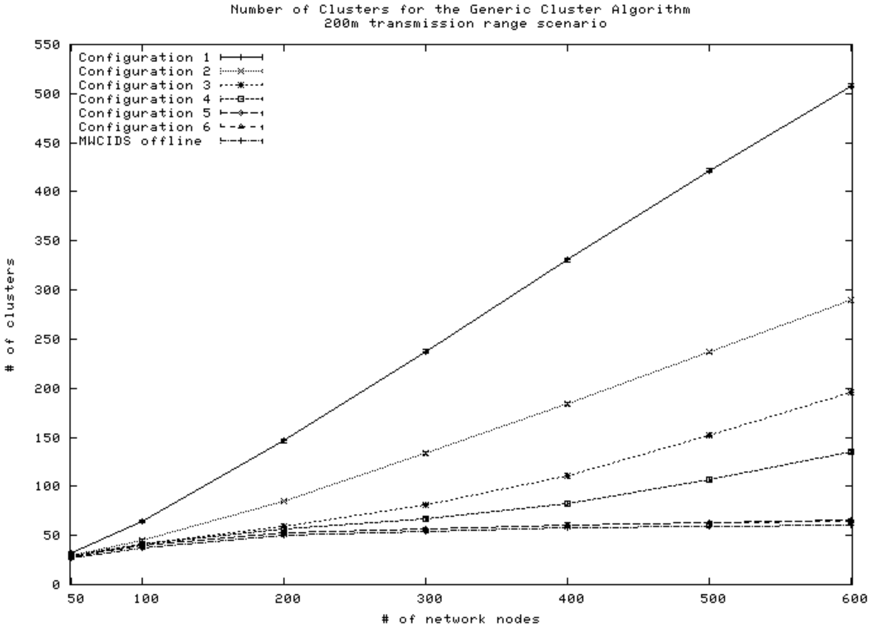


Figure 8.5: Number of Cluster Head nodes for the generic clustering topology

Figure 8.6 presents the average size ratio of clusters when the network size increases. We define cluster size ratio as: $CSR = (nMR + nRN)/nCH$, where CSR is the cluster size ratio, nMR, nRN and nCH are, respectively, the number of mobile routers, relay nodes and cluster heads of the whole network scenario. The average shown is the average over all the evaluated scenarios. From these graphs we can perceive that by fine tuning the costs we can model the clusters' behavior. The offline approach has the biggest cluster size ratio since its main goal was to reach the minimum number of clusters, so the clusters are larger. The standard deviation for the cluster sizes, for all the evaluated configurations, is typically below 0.05, this means the clusters are indeed well balanced, as we first intended. Moreover, we can control the clusters size by changing the cost function. We can perceive from the graphs that the different configurations reach a stable point in the ratio of MR + RN and CHs. Except for the configuration where we intend to increase the number of clusters as much as possible, the average cluster size reaches a saturation point and the size of the clusters stays stable independently of the number of nodes in the network.

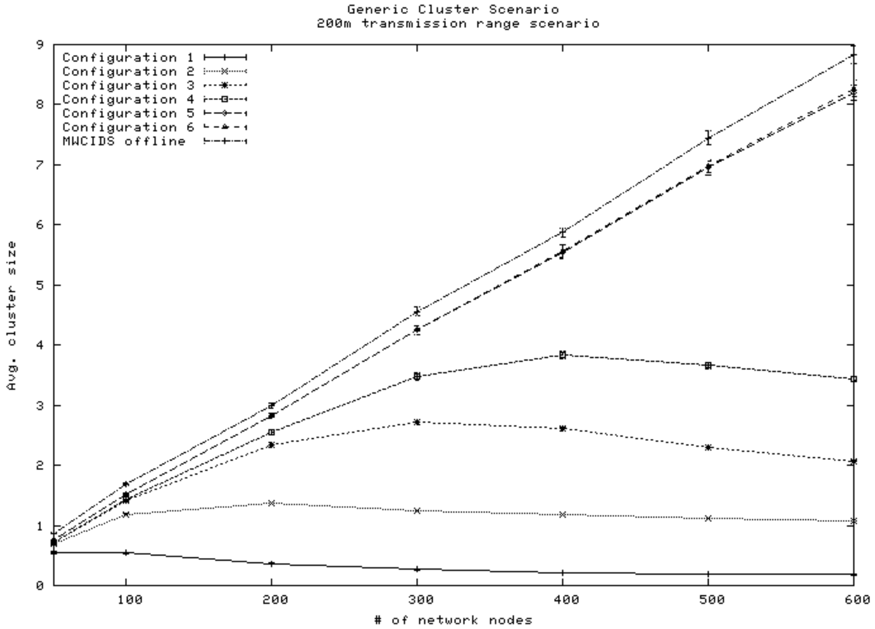


Figure 8.6: Number of nodes per cluster for the generic clustering topology

8.5.3 Relaxed CHORIST experiments

For the CHORIST experiments we have kept all the requirements and constraints described in Chapter 7, we just relaxed two constraints. First for these experiments two CHs may be in the same area, although when searching for the minimum number of clusters the WCIDS is still the target architecture. The second constraint we relaxed was that for these experiments the MR may broadcast connection updates. These two changes are required to allow the network to vary the clusters concentration. However, the state machine observed in Figure 7.2 is still valid and all the transitions are rigorously respected.

The same observations made for Figures 8.5 and 8.6 are valid for Figures 8.7 and 8.8. As expected, even though the protocol and the nodes organization are different, the technique managed to shape both architectures in the same way.

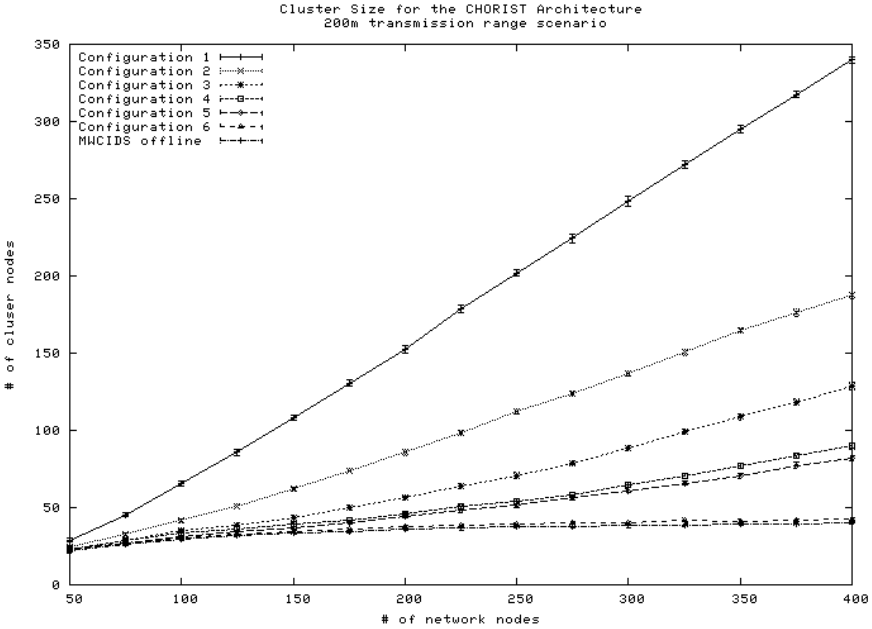


Figure 8.7: Number of Cluster Head nodes for the CHORIST topology

To simulate different disaster scenarios we varied the concentration of the network. We randomly chose a point in the defined area and evaluate different nodes densities within a 300m radius from this point. The observed concentrations were 10%, 20%, 30% 40% 50% 60% 80%. Figure 8.9 presents the Configuration 2 cluster sizes and the cluster distribution, for the different evaluated distributions. We can observe that for Configuration 2, as it was intended, the cost function increases the number of CHs in the more crowded areas while simultaneously keeping the size of the clusters under control.

The graph of Figure 8.10 shows the number of messages sent through the entire network during the simulation time for each one of the defined configurations. As expected the bigger the size of the network the larger the number of messages exchanged among nodes. However, the volume of messages shows only small variations between configurations. Even though the network shape changes considerably, the message cost to generate and

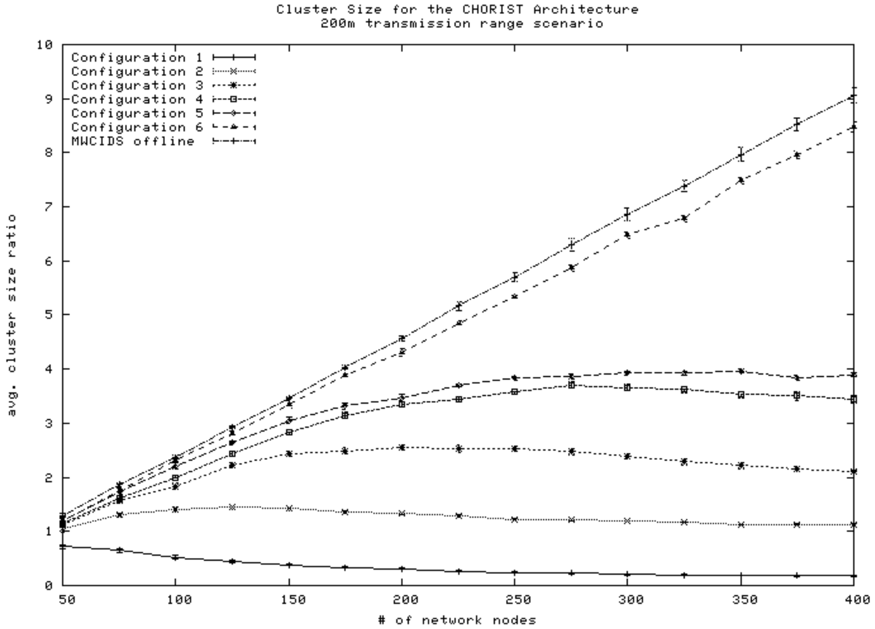


Figure 8.8: Number of Cluster Head nodes for the CHORIST topology

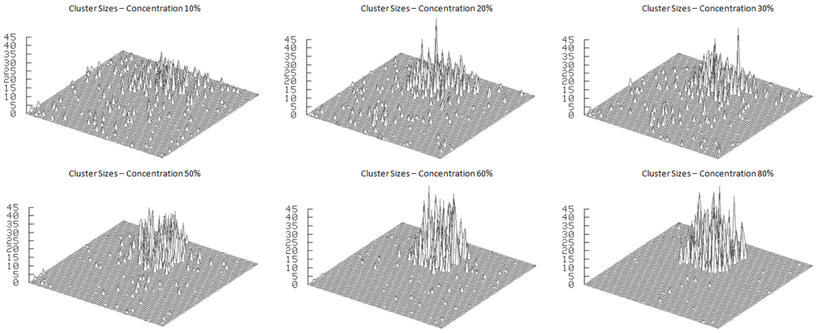


Figure 8.9: Cluster sizes for configuration 2 varying the nodes concentration.

maintain a network, with the minimum and maximum number of CHs, is basically the same. This behavior is the same for all the experiments for the three evaluated network types.

The graph in Figure 8.11 shows the number of clusters a relay usually

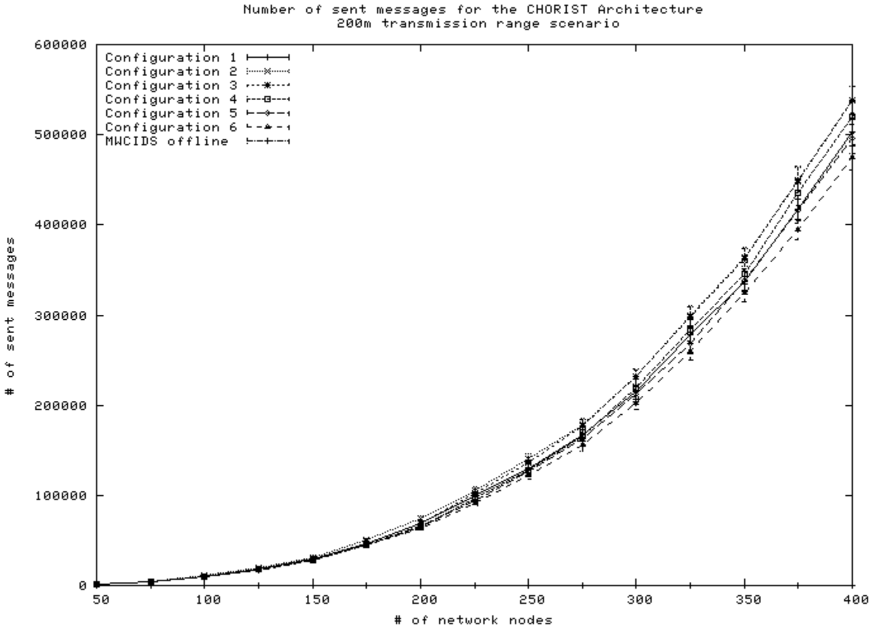


Figure 8.10: Number of sent messages through the network nodes for the CHORIST topology

connects. Comparing the graphs of Figure 8.5 and Figure 8.11 we see that the number of RN connections is directly related to the number of CHs in the network. The bigger the number of clusters the higher the load for the available RNs. When we decrease the number of clusters we also decrease the need for RNs. For the WCIDS offline implementation this value is around two, i.e. on average a RN connects only two clusters.

For all CHORIST evaluated cases, our technique increases the number of relay nodes more than the minimum value, given by the offline implementation. The first reason for this is that, the technique does not have a global view to be able to select the best global RNs. Second, as we create more clusters it is only natural to have more RNs to interconnect them. However, the most important factor is that CH nodes chose their RNs in a selfish manner. They chose the best suited nodes, from their point of view, not that of the network. Consequently, it is possible to have, for example, two different nodes acting as RN between the same two CHs, just because each CH chose their RN in a selfish manner. In this case instead of having one RN acting as a gateway between these two CHs, as it is the case in the offline approach, the network will have two RNs. Each one of them acting as a RN

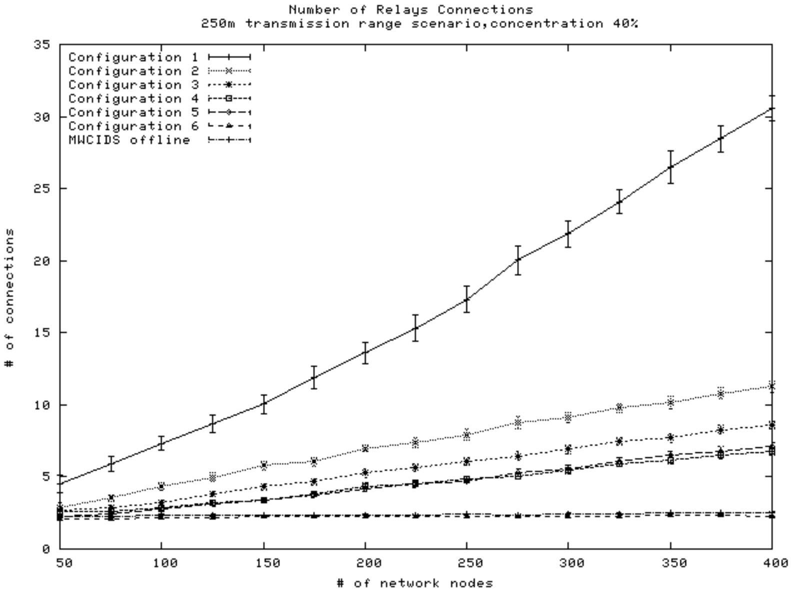


Figure 8.11: Average number of clusters connected by a RN

for one of the CHs involved. However, the increase in the number of RNs has some advantages. For example, the cost function could take into account the channel reliability and, in this case, having two RNs the network stability would increase. Another point to observe is that, as example of what already observed in our standard implementation of CHORIST presented in Chapter 7, the path sizes are smaller when we increase the number of RNs. As expected, the same occurs for this implementation. Increasing the number of RNs, also increases the paths' diversity, enabling the occurrence of smaller routes between nodes.

The graph of Figure 8.12 shows the average size of clusters for the configuration 2 network for different network sizes and concentrations. The network concentration effectively affects the size of the clusters. However, the standard deviation for the cluster sizes, in all the evaluated configurations, is typically around 0.15. This means that, even though the concentration changes, the sizes of the clusters are well balanced. Within the same scenario, the number of nodes per cluster does not present any significant variation, as we first intended.

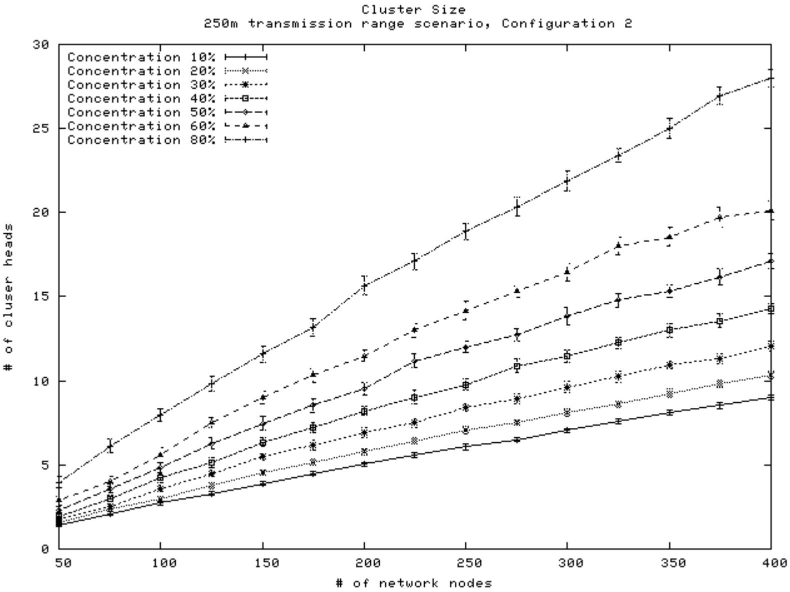


Figure 8.12: Average cluster size for different concentrations of configuration 2

8.5.4 Interest groups experiments

This observed topology management algorithm is also hierarchical, with the formation of clusters maintained by one cluster head. These experiments present mainly two distinctions when compared to the previous ones. The first difference is that here we have a set of special nodes that are declared cluster heads by default, i.e. Default Cluster Heads (DCH). These nodes maintain this status throughout the network's life. Other nodes become cluster heads (CH) only in areas not covered by these DCHs. The second difference is that the method also considers a variable number of interest groups (1 to N groups). Each interest group is defined in the network startup and must have at least one DCH to represent it. The DCH does not necessarily have to be close to all nodes in its group. This kind of behavior may be interesting for PSNs when one want to maintain the different authorities' traffic separate. For example, normally in a disaster scenario the police missions and interest differ from the ones of medical staff. So it makes sense to have different interest groups for these two distinct teams.

Interest groups may also have an important role in decreasing the amount of traffic, as observed by Hui and Crowcroft [58]. Sometimes in PSNs some messages may need to be spread to all nodes in a specific group but may be meaningless for nodes in other groups. For example, in case of an earthquake the status and conditions of nearby roads may interest police officers or ambulance drivers, but has little or no importance for the rescue teams digging for survivors. For simulation purposes, only the DCHs have a defined interest group at the beginning of the simulation, and the different groups are attributed evenly to the available DCHs. The interest group of regular nodes is defined by the DCH nearby through the periodic broadcast of connection update messages.

Apart from the CH and DCH nodes no other node receives messages from nodes from different interest groups and even CH and DCH only receive Connection Update messages from nodes in different groups. We allow this to increase connectivity and make the CH nodes aware of the number of clusters around.

Each element in the proposed solution has a connection price. The prices vary among the different nodes, and the price to pay for a connection to a CH is higher than the price to pay for a DCH. Standalone CHs/DCHs have also higher connection costs than the ones that already provide connection service to some nodes. The load of the CH/DCH also counts, as loaded the CH/DCH higher is its connection cost. The idea is to have more balanced clusters, however, the costs are attributed in a way that guarantees that all the available resources of an available DCH should be used before a new CH/DCH start to accept connections in the same region. The order of communication costs goes like this: DCH providing connection < isolated DCH < CH providing connection < isolated CH. The costs of the DCH/CH providing connection increases with the number of connections it is handling. For example, if an isolated node has two options, an CH with providing connection to 5 other nodes, and another CH providing connection to 6 other nodes, it will prefer to connect to the first one.

Interests group protocol description

Periodically CH and DCH nodes send connection update messages announcing their presence and list of connected nodes. Each connected node, MR, sends also a periodic a connection update, but only to the node it is attached to. CH and DCH updates are sent through two available interfaces. When arriving by the default interface it may change the status of the nodes that received it. If it arrives by the second interface, it is just stored as a way to build the knowledge of the clusters around. The two interfaces have different purposes, the first one could be a WiFi like interface, to organize the communication with nodes closer to the CH and the second interface could be a WiMAX kind of interface, to reach further nodes and with a broader bandwidth capacity. This interface would normally be used to transfer data between the clusters. Figure 8.13 presents an example of the interests groups setup.

If the node that received the update message, by the default interface, is a CH or a DCH, this node verifies the cost of the income message. If the node is not already connected to a DCH, the cost of this new provider is smaller than the cost of the present provider, or the node own connection cost, and the perspective provider has room to accommodate all the present connections, the node sends a connection request to the node that sent the update message. If the node is an IN (isolated node) or an isolated CH/DCH and the node that sent the message has enough space, this node sends a connection request to the node. Anything is better than stay isolated.

When a CH/DCH receives a connection request, and it has enough resources, it sends a connection response to the node that requested the connection and reserves the resources to this node. If it does not have enough resources the CH/DCH sends a connection cancel.

When an IN/MR/CH/DCH receives a connection response from a CH/DCH, it releases its resources (its connections), sends a connection confirmation to the CH/DCH that sent the message and registers this new node as the provider. Case the node is an IN/CH it changes state to become a MR. However, if the node didn't send any connection request in first place, i.e. the message was a mistake, the node sends a connection cancel to the node that just sent the connection response. Case the MR/CH/DCH receive a connection cancel in response to a connection request, it forgets the request and waits for a new opportunity to connect to another node or, if it stays as a IN for a long time, three attempts with different bakeoffs intervals, it may became a CH.

If the CH/DCH receives a connection confirmation it updates the information regarding this connection. If it receives a connection cancel, it releases the resources allocated to this connection.

For all practical purposes there is no difference from CH and DCH. The differences are in terms of connection costs, lower for DCH. Other difference is that being a CH is a transient state, a CH node may become a MR at any moment if it finds another node that has a lower cost than it has. However, a DCH is always a DCH, no matter what. A DCH continuously broadcast update messages being able even to receive connections, if some other node needs it, and is able to pay for the price. Figure 8.14 presents the state machine for the DCH node.

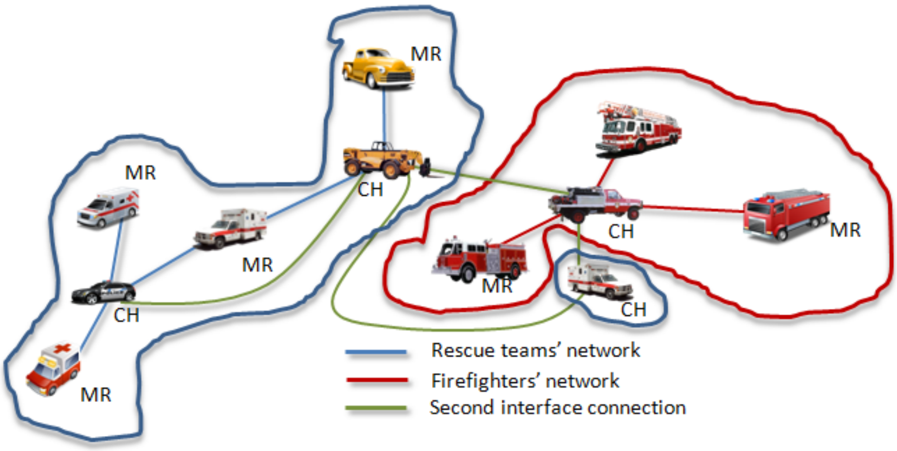


Figure 8.13: Interest groups architecture, showing two different interest groups and the second interface links

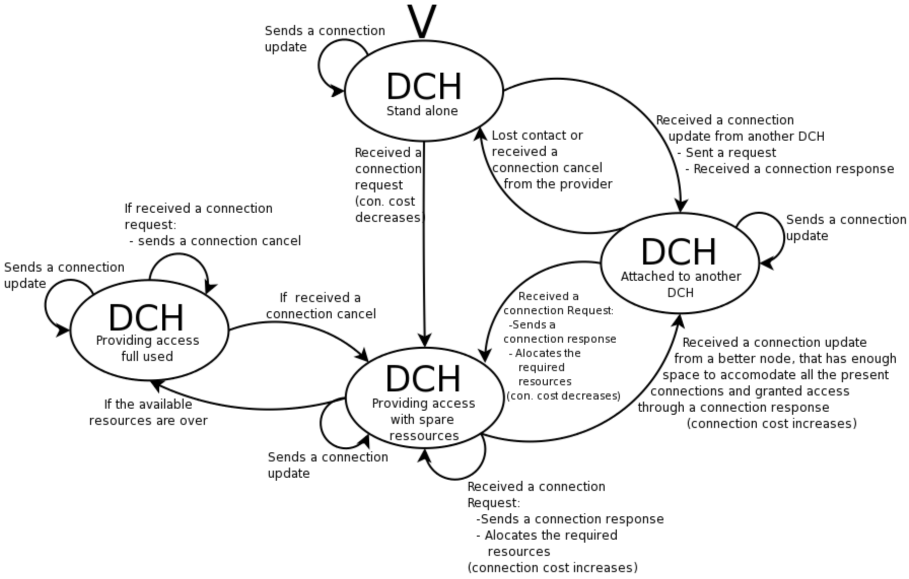

Sends a connection update
DCH
Stand alone
Received a connection update from another DCH
- Sent a request
- Received a connection response
Lost contact or received a connection cancel from the provider
Received a connection request (con. cost decreases)
If received a connection request:
- sends a connection cancel
Sends a connection update
DCH
Attached to another DCH
Sends a connection update
DCH
Providing access full used
If received a connection cancel
Received a connection Request:
-Sends a connection response
- Alocates the required resources
(con. cost decreases)
Received a connection update from a better node, that has enough space to accomodate all the present connections and granted access through a connection response (connection cost increases)
If the available resources are over
DCH
Providing access with spare ressources
Sends a connection update
Received a connection Request:
-Sends a connection response
- Alocates the required resources
(connection cost increases)

Figure 8.14: Default Cluster Head state machine

Experiments

For these experiments nodes move in a random way point fashion in a $1000 \times 1000m^2$ area for one hour simulation time. The communication range for

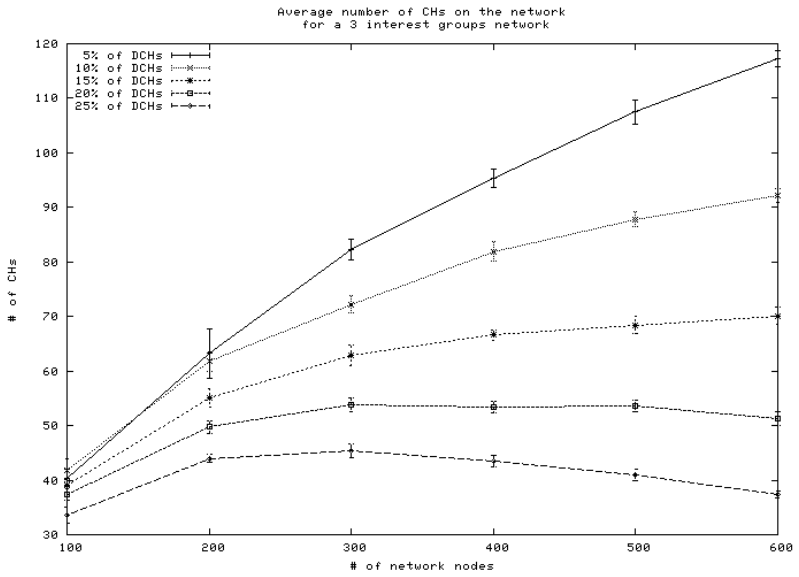


Figure 8.15: Variation of the average number of CHs in the network when we increase the percentage of DCHs

the first interface is $100m$ while for the second interface the communication range is $300m$. The used basic connection weights are: $DCH = 0$, $CH = 8$, $MR = 50$. We considered here that the maximum allowed size for a cluster is 7. We varied the number of interest groups and percentage of DCHs. The DCHs are placed randomly thought the network and the remaining IN nodes are placed in a maximum distance of $130m$ from these DCHS.

The graph in Figure 8.15 shows the average number of CHs on the network when we vary the percentage of DCHs. For this clustering algorithm CHs are created only when nodes are either outside the area of a DCH or when the DCH have not enough resources to grant the node's connection requirements. We can see that the increasing in the percentage of DCHs decreases the number of CHs. The number of CHs are more or less stable for networks with more than 300 nodes because the limit of the size of the clusters were not a problem for these experiments, and as the nodes does not have a common movement pattern, the occurrence of CHs have a closer relation to the size of the area than with the occurrence of overpopulated clusters. As the area does not change, the average number of CHs needed to cover the area also does not change significantly.

Figure 8.16 presents the average number of CHs when we vary the percentage of DCH and the number of interest groups. The graph shows the

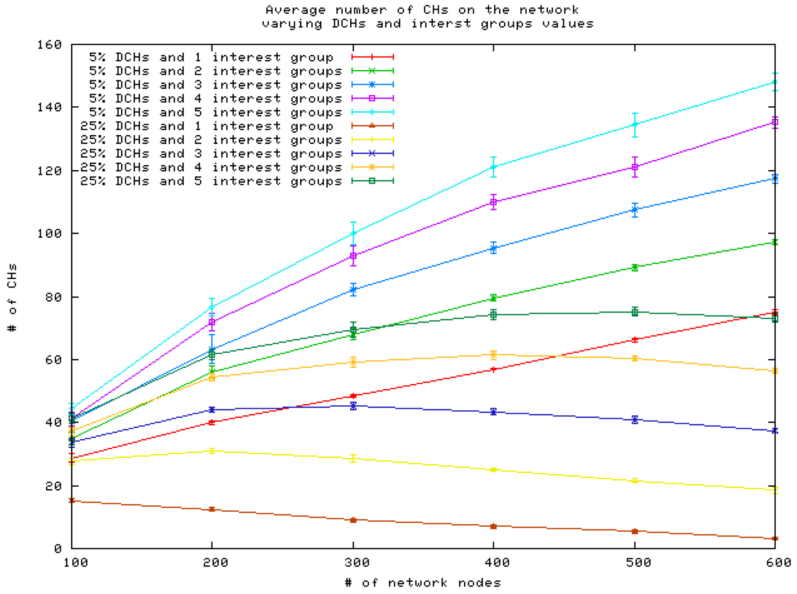


Figure 8.16: Variation of the average number of CHs in the network when we increase the number of interest groups

curves for 5% and 25% of DCHs, the minimum and maximum number of DCHs we evaluated. We can observe that the behavior is consistent for both percentages and that when we increase the number of interest groups we increase also the number of CHs in the network. This is expected since when we increase the number of groups is equivalent to split the network, the bigger the number of groups the harder is for a node to find a nearby cluster with the same interest. In this way more nodes start to become CHs. We can also observe that 25% of DCHs on the network is enough to stabilize the number of required CHs over the simulated area. On the other hand, Figure 8.17 shows that the average size of clusters decrease with the increasing in the number of DCHs and interest groups. The average cluster size, for these experiments, on average did not reach the maximum defined cluster size, which is of 7 nodes. However, when the maximum value was reached during the experiments the designed cost function could control the nodes behavior and form new clusters.

One interesting thing of the graph in Figure 8.17 is that we can observe that networks with 5% DCHs and 3, 4 and 5 interest groups have a similar behavior, in terms of numbers of nodes per cluster, than a 25% DCHs network with 2, 3 and 4 interest groups respectively. This is interesting because shows that the impact of the number of DCHs has also a relation with the number

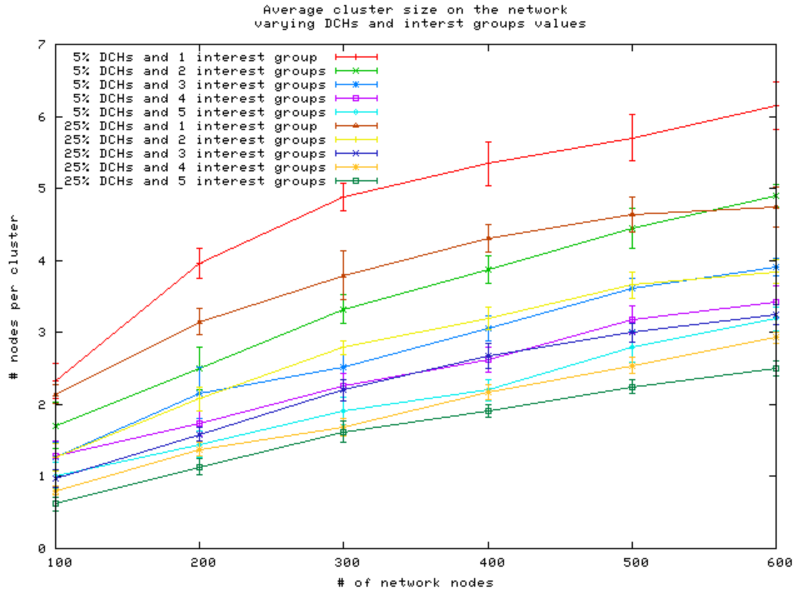


Figure 8.17: Average cluster size CHs in the network when we increase the number of interest groups

of interest groups.

For these experiments we also tracked the number of times a node changed status during the simulation period i.e. CH to MR or MR to CH. Figure 8.18 show that when we increase the number of interest groups we decrease the number of changes. This relation, counter intuitive at first, comes from the fact that when we have more interest groups nodes spend more time to find another cluster with the same interest, so they tend to became CHs and stay as CHs for more time than the nodes in environments with less interest groups. When we have less interest groups the tendency is for nodes that become a CH to find faster another cluster, thus changing states more frequently. Even though the number of changes for the 25% DCH network is smaller, we can observe that the behavior does not change significantly when we change from 5% to 25% the number of DCHs on the network. Not only the shape of the curves is similar, but also the values themselves are close. This means that the number of changes has a small dependency to the percentage of DCHs on the network. It is more related to the mobility, number of interests groups and area coverage than with the number of DCHs in the network.

The graph in Figure 8.19 shows the average number of standalone clusters during the whole simulation time: we consider as standalone clusters

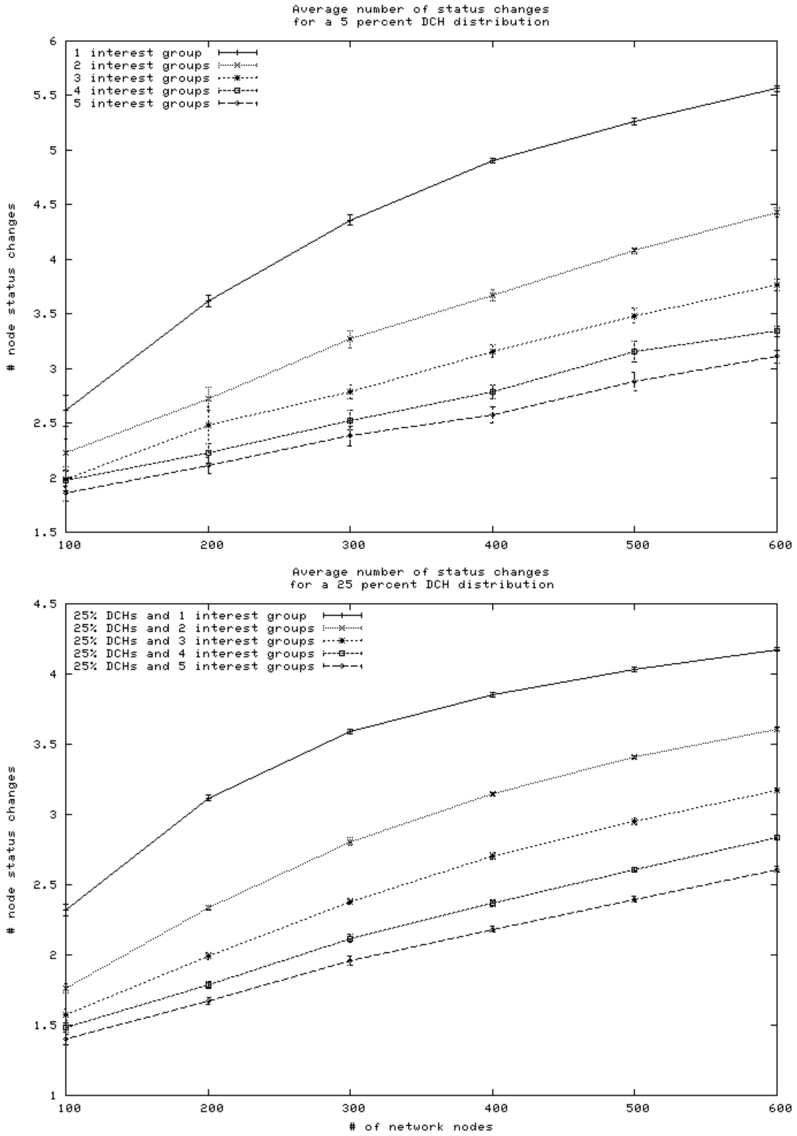


Figure 8.18: Average number of status change for 5% and 25% DCHs networks

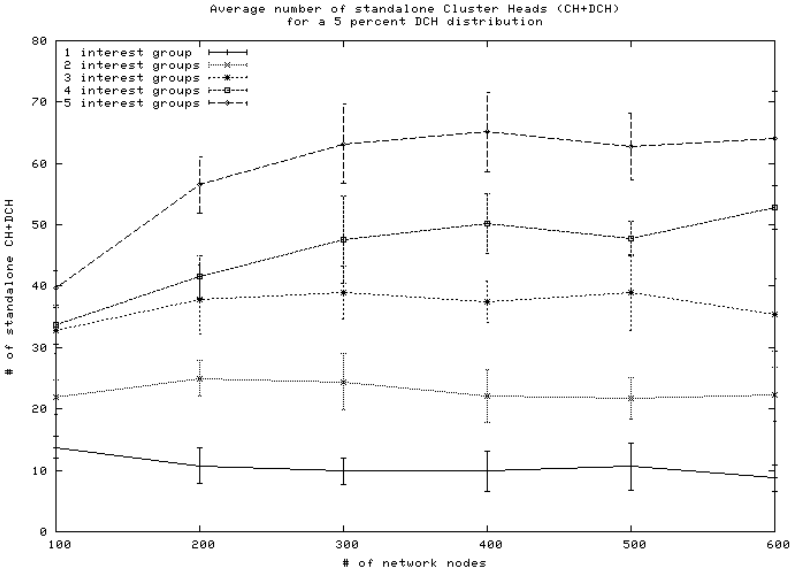


Figure 8.19: Average number of standalone clusters when we increase the number of interest groups

those that just have a single member, either a CH or a DCH. The bigger this value the worse it is for the network. This means that the network is more fragmented and more control messages will be required to maintain the structure, as can be observed in Figure 8.20, i.e. the cost of the network is higher and less bandwidth will be available for data traffic. Another thing we can observe is that the average number of standalone clusters is stable and independent of the number of nodes in the network. Again, the increase in the number of interest groups contributes to the occurrence of standalone clusters.

The higher the number of interest groups the bigger the number of control messages exchanged during the simulation period. Figure 8.20 shows that when we increase the number of interest groups the number of exchanged messages also increases. Even though the difference is relatively small, the graph only considers the messages exchanged to maintain the network. More clusters also means more connectivity changes that can affect other protocols, for example routing or peer discovery processes: In other words, the increase in the number of clusters and the over-segmentation of the network may lead to a ”domino effect”, where the other layers protocols will also need to exchange more control messages making the difference between the curves larger.

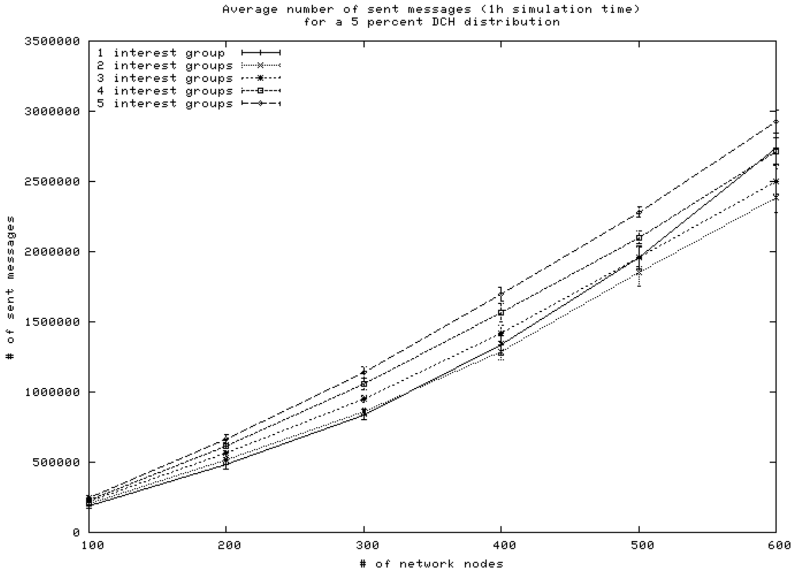


Figure 8.20: Average number of sent control messages when we increase the number of interest groups

8.6 Conclusions

This chapter presented a technique to perform network admission control and topology management for structured mesh networks. The results show that by handling only local information and without the complete final configuration, the proposed method guarantees the correct clustering formation and role attribution to the nodes. The technique is also able to shape fairly distinct final network configurations. For example, just controlling a vector of cost functions one can go, in a distributed way, from a completely clustered network to the one that has the minimum possible number of clusters.

The cost function, responsible for modeling the network shape, can be as simple or as complex as one needs it to be. For the results presented here, we chose to focus on the number of clusters, however, other factors could be taken into account. The important point to consider is that cost function calculation is a flexible way to control the network topology behavior. This flexibility is an interesting asset for networks such as public safety networks where different disaster sites could have different network requirements and the network operation can be shaped as desired. The cluster sizes are homogeneous; the technique enables a load balance among clusters in a dynamic and simple way.

Part IV

Conclusion

Chapter 9

Conclusion

This thesis proposes some new techniques to enable PSNs communication during the warning and crisis handling phases. Even though the techniques presented here are general and valuable for other environments, PSNs present an extreme case where stable and efficient mechanisms may save lives. Another point to observe is that two different disaster sites may have completely different requirements, and this makes PSNs a challenging field because any solution should be flexible enough to foresee and adapt to different scenarios. The two main parts of this thesis, Alert Phase Support and Crisis Management Phase Support, present, respectively, a DTN based solution to spread warning messages and a topology control mechanism, the former aimed at enabling the CHORIST architecture and the latter being able to adapt to the needs of different PSNs sites.

The Virtual Access Point technique, presented in Chapter 4, improves the performance of stream traffic and independent warning messages enabling the transmission of warning messages in areas without network coverage. The method is simple yet effective in increasing network coverage. The method is best effort based in DTNs and epidemic data delivery, which means that there are no guarantees all target nodes will receive the message and that there is an increase in the number of sent messages. However, the increase in the number of transmitted messages occurs in areas that had no communication before: the generated traffic is therefore not interfering with other communications. Even though the method does not guarantee data delivery the increase in the percentage of messages received is impressive and may reach 1615.91% depending on the evaluated case. This can be explained by the fact that our system manages to remain operational even after the traditional, RSUs only based setup, has collapsed. However, to be effective a number of real APs, even though small, must be active. This is a limitation but we believe that, even in a severe incident, not all the RSUs will be damaged at once. Even if that occurs, we can consider that a Risk Management Centre will be deployed by the authorities to manage the rescue operations. This centre could work as an AP to broadcast the warning message. From this point the mobile nodes could spread the message over the target region.

Chapter 7 presents a proposal to build the CHORIST project proposed network. The architecture was reduced to the solution of the minimum WCIDS problem, which is an NP-Complete problem. Our solution is capable, using only local information and in a distributed way, to present a performance comparable to the ones reached by the centralized implementation of the minimum WCIDS. Moreover, the results show that even with mobility our implementation of the CHORIST architecture is stable.

The market based technique, presented in Chapter 8, is a flexible and efficient way to perform network admission control and topology management for structured mesh networks. The results show that by handling only local information and without the complete final configuration, the technique is able to shape fairly distinct final network configurations. The cost function is a key part of the method and can be as simple or as complex as needed. This flexibility enables the method to shape the network as desired and may consider a large set of parameters on the network composition. The technique also enables the creation of homogeneous cluster sizes.

9.1 Remarks and future work

This thesis summarizes part of what I have been researching during the last few years but as the Appendix A shows, other works were not included here.

The natural next steps for this work would be implementing the proposals in a real environment to evaluate how they would behave in a real world trial. This work is only based on simulations what give us a good view of the potential and expected scalability of the techniques, but gives us no insights about potential real world problems. Even a small test bed implementation using, for example, WAVE protocol, IEEE 802.11p [60], would give us valuable insights regarding the deployment of the techniques in real environments.

For the market based topology control algorithm, one valuable and interesting extension would be the use of other parameters in the cost calculation. This should lead to a more accurate calibration of the cost function and a finer and more precise control of the number and quality of the elements on the network architecture e.g. CHs and RNs. Some initial experiments also showed us that it is possible to have different cost functions for different defined areas. This would enable that parts of the same network could have different topology configurations. For example, imagine a huge disaster, such as a large scale earthquake. In such a scenario, it may be possible that while in one place firefighters are trying to control a building in fire, as a result of some gas leak, close by rescue teams are digging trying to find survivors. These two situations have different network requirements, and it could be interesting to have two distinct organizations for them.

For the PSNs environments we consider here, with the nodes being in vehicles, connectivity is a more important factor than energy saving [104]. The vehicles should be able to generate enough energy to keep the communication equipment running during the assigned missions. For this reason we did not vary the transmission power of the nodes, even though smart radio techniques may play an important role in future wireless communications and should be evaluated in the future. This is especially true if one plans to apply the proposed algorithm to other environments such as sensor networks, for example. We also assumed that the VAPs were vehicles, so that energy efficiency was also not a critical aspect there. However, it would be interesting to consider, as an extension to this work, how to increase energy efficiency when the nodes are carried by humans.

Appendix A
Publications

List of publications during the Ph.D.

1. Daniel Câmara, Nikolaos Frangiadakis, Christian Bonnet, Fethi Filali, Vehicular Delay Tolerant Networks, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010

2. Giuliana Iapichino, Daniel Câmara, Christian Bonnet, Fethi Filali, Public Safety Networks, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010

3. Ikbal Chammakhi Msadaa, Daniel Câmara, and Fethi Filali, Mobility Management in WiMAX Network, WiMAX Security and Quality of Service: Providing an End to End Explanation, Wiley, accepted for publication, to appear in late 2009

4. Daniel Câmara, Antonio A.F. Loureiro, and Fethi Filali, Formal Verification of Routing Protocols for Wireless Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Chapter 8, Springer, January, 2009

5. Daniel Câmara and Fethi Filali, Scheduling and Call Admission Control A WiMax Mesh Networks View, Guide to Wireless Mesh Networks, Chapter 17, Springer, January, 2009

6. Azzedine Boukerche, Daniel Câmara, Carlos M.S. Figueiredo, and Antonio A.F. Loureiro, Algorithms for Mobile Ad Hoc Networks, Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, Chapter 1, edited by Azzedine Boukerche, John Wiley and Sons, ISBN: 0470383585, October, 2008

7. Daniel Câmara, Christian Bonnet, Fethi Filali, Propagation of Public Safety Warning Messages, IEEE Wireless Communications & Networking Conference (WCNC) 2010, Sydney, Australia, 18-21 April 2010

8. Ikbal Chammakhi Msadaa, Daniel Câmara, and Fethi Filali, Scheduling and CAC in IEEE 802.16 Fixed BWNs: A Comprehensive Survey and Taxonomy, IEEE Communications Surveys & Tutorials, to appear late 2009

9. Erlon R. Cruz, Daniel Câmara, Hï£¡io C. Guardia, Providing Billing Support in WiMAX Mesh Networks, The 5th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2009), IEEE, Marrakech, Morocco, 13-14 October 2009

10. Daniel Câmara, Christian Bonnet, Fethi Filali, Implementation and Dynamic Topology Maintenance for the CHORIST Network, The 20th Personal, Indoor and Mobile Radio Communications Symposium 2009, PIMRC'09, IEEE, Tokyo, Japan, September 13-16, 2009

11. Daniel Câmara, Christian Bonnet, Topology Management for Public Safety Networks, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany, June 21-24, 2009

12. Daniel Câmara, Nikolaos Frangiadakis, F. Filali, A. A. F. Loureiro, Nick Roussopoulos, Virtual Access Points for Disaster Scenarios, IEEE Wireless Communications & Networking Conference (WCNC) 2009, IEEE, Budapest, Hungary, April 5-8, 2009

13. Daniel Câmara, Daniel T. Fokum, Eric Anderson, Hassan Ghasemzadeh and Yong Liu, Report from HotMobile 2009, IEEE CS, PERVASIVE computing, 1536-1268/09, AprilJune 2009

14. Daniel Câmara, Christian Bonnet, Fethi Filali, Dynamic Topology and Communication Control for Highly Dynamic Wireless Mesh Networks, A Public Safety Network Point of View, Tenth Workshop on Mobile Computing Systems and Applications (HotMobile 09), Doctoral Consortium, ACM Sigmobile, Santa Cruz, CA, February 23-24, 2009

15. Daniel Câmara, Nikolaos Frangiadakis, F. Filali, A. A. F. Loureiro, Nick Roussopoulos, Virtual Access Points for Stream Based Traffic

Dissemination, 2008 IEEE Asia-Pacific Services Computing Conference, IEEE, Yilan, Taiwan, December 9-12, 2008

16. Hicham Anouar, Cristian Bonnet, Daniel Câmara, Fethi Fillali , Raymond Knopp, OpenAirInterface Simulation Platform, International Conference on Measurement and Modeling of Computer Systems, SIGMETRICS 2008, ACM, June 2-6, 2008, Annapolis, Maryland, USA

17. Nikolaos Frangiadakis, Daniel Câmara, Fethi Filali, Antonio Alfredo FLoureiro, Nick Roussopoulos, Virtual access points for vehicular networks, Mobilware 2008, 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, ACM, February 12th-15th, 2008, Innsbruck, Austria

18. Daniel Câmara, Antonio Alfredo F. Loureiro, Fethi Filali, Methodology for formal verification of routing protocols for ad hoc wireless networks GLOBECOM 2007, 50th IEEE Global Communications Conference, IEEE, November 26-30, 2007, Washington, USA

Appendix B
Résumé Étendu en Français

Cette thèse propose un ensemble de techniques visant à améliorer la couverture et l'organisation des réseaux mobiles dans le contexte de la sécurité publique.

Les réseaux de sécurité publique (RSP) sont des réseaux établis par les autorités afin d'avertir les populations d'une catastrophe imminente ou alors afin de coordonner le travail des équipes d'intervention durant les phases de crises et de normalisation.

Une catastrophe, telle que perçue par les personnes affligées, pourrait être définie comme un évènement extrême causant des dommages et/ou des pertes humaines.

Les RSPs jouent un rôle primordial pour assurer la communication et la coordination des opérations de sauvetage.

Les catastrophes peuvent être classées en deux catégories: les catastrophes naturelles (ex. les volcans, les inondations, les tremblements de Terre, et les épidémies), et les désastres causes par l'homme (e.g. les accidents nucléaires, les accidents maritimes, et les attaques terroristes.

Dans les deux cas, des vies humaines sont en danger et l'infrastructure de télécommunication pourrait être sérieusement endommagée. Voire même carrément "hors service".

La gestion du désastre est requise pour gérer les dégâts. Elle consiste en trois phases:

- la phase de préparation,
- la phase de crise,
- et le retour a une situation normale.

Ces trois phases sont illustrées dans la Figure 9.1. Ce travail s'intéresse à cette phase de crise. Cette phase s'étale de du point de déclenchement, quand les autorités décident de prendre les choses en main et de répondre a un évènement spécifique jusqu'a l'après désastre ou les conséquences immédiates du désastre sont encore présentes et tant que des vies humaines peuvent encore être sauvées.

Cette phase de crise pourrait être subdivisée en deux sous-phases:

- La phase d'alerte,
- Et la phase de gestion de la crise.

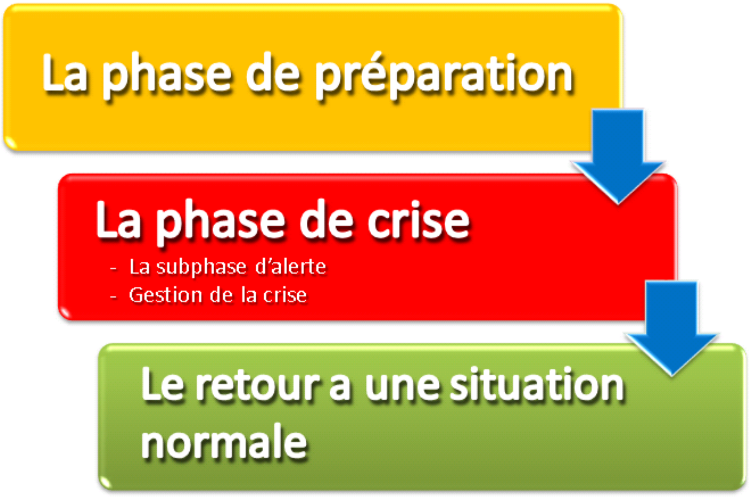


Figure 9.1: Les trois phases de gestion du désastre

La phase d'alerte correspond à la phase au moment de laquelle la population devrait être informée d'une menace imminente ou d'un désastre bel et bien existant. "Crisis handling" consiste en l'ensemble des mesures entreprises par les autorités afin de gérer le désastre.

Cette thése se propose de contribuer au niveau de ces deux phases d'alerte et de gestion de crise.

La phase d'alerte est importante dans la mesure où, si elle est gérée d'une manière efficace, pourrait sauver des vies puisque la population serait alertée à temps pour éviter la zone de danger. Plusieurs méthodes telles que les sirènes, la tv et la radio pourraient être utilisées. Cependant ces méthodes supposent l'existence d'une infrastructure pré-déployée et que la population aura accès à cette infrastructure. Le problème qui se pose en comptant sur une structure existante est que, dans le cas d'une catastrophe, cette structure est très probablement endommagée. L'autre problème qui se pose en considérant la deuxième hypothèse est que les gens pourraient ne pas être en train de regarder la TV ni d'écouter la radio comme ils pourraient être dans une zone non couverte par des sirènes.

Et ceci est d'autant plus vrai quand les personnes sont en déplacement (en voiture, en train de marcher, etc.). Ce travail propose de diffuser cette information et d'en étendre la couverture d'une manière transparente et discrète.

La solution proposée dans cette thèse pour aider dans la phase d'alerte est basée sur les réseaux opportunistes et utilise des équipements a la portée de la population et qui seraient disponibles même en voiture ; et ce afin de pallier au problème de portée limitée.

Cette technique, que l'on nomme technique de Points d'Accès Virtuels (ou VAP pour Virtual Access Points), crée une mémoire cache distribuée et coopérative entre les différents noeuds mobiles qui se trouve dans a zone affectée par le désastre. En utilisant la technique de VAP, les noeuds opèrent comme des noeuds virtuels en rediffusant les messages préalablement reçus et qui sont stockes dans leur propre cache : ils adoptent la technique Store-and-Forward. Ceci aide à diffuser les messages à des noeuds qui n'y avaient pas accès avant. Les principaux avantages de la technique proposée est qu'elle ne se base sur aucune caractéristique spécifique du réseau, elle est transparente et améliore d'une manière significative une dissémination efficace du message en question.

La phase de gestion de crise présente également de nouveaux défis et présente un terrain fertile pour la recherche. Le problème auquel on s'adresse ici est le problème de gestion de la topologie et de gestion du contrôle d'admission. Nous proposons des solutions pour construire des structures de réseaux stables et fiables, des caractéristiques cruciales à la coordination des équipes de sauvetage durant les phases les plus critiques.

La gestion de la topologie dans les réseaux RSPs est particulièrement complexe pour diverses raisons. D'abord, les deux principaux défis des réseaux RSPs sont la serviabilité et le déploiement rapide. Ensuite, ils doivent faire preuve d'une grande flexibilité et d'adaptabilité dans la mesure où ils peuvent être déployés pour scenarios de catastrophes très différents. Par exemple, le nombre de noeuds, les nombre de personnes servies, le modèle de mobilité, ainsi que l'environnement de déploiement d'un site incendié est complètement différent d'un site ayant subi un tremblement de Terre.

Néanmoins les personnes amenées à intervenir dans les deux cas sont les mêmes et possèdent en général les mêmes équipements.

Ce travail présente non seulement une solution pour l'établissement et le maintien de l'architecture de certains RSPs proposes dans le cadre de projets gouvernementaux, mais encore une nouvelle technique pouvant répondre, d'une manière simple et efficace les différents sites de désastre. La technique proposée prend en considération les concepts économiques d'offre et de la demande. L'approche permet ainsi une adaptation dynamique des la topologie aux besoins des différents sites cibles et permet rend possible la réorganisation d'un réseau déjà établi.

Les de sécurité publique représentent un cas extrême ou la zone de couverture, les mécanismes dynamiques et auto-adaptatifs deviennent d'une haute importance. Les techniques exposées dans cette thése sont appliquées aux RSPs ; néanmoins, ils sont assez génériques et peuvent être étendus à bien d'autres cas tels que les réseaux de capteurs ou les réseaux véhiculaires.

Cette thèse présente des solutions aux problèmes survenant durant les phases d'alerte et celle de gestion de crise ; les deux étapes formant la phase de crise. Pour détailler notre travail, nous avons organisé le manuscrit en quatre parties.

- La première partie présente une introduction au thème général avec une vision approfondie du domaine de réseaux de sécurité publique (RSPs).

- La deuxième partie décrit notre contribution à l'amélioration de la communication durant la phase d'alerte et évalue les résultats obtenus en utilisant cette technique.

- La troisième partie détaille notre contribution relative à la gestion de la topologie afin d'aider les RSPs durant la phase de gestion de la crise.

- Finalement, la dernière partie représente une conclusion de la thése ainsi que de ces contributions. Elle met également l'accent sur les éventuels travaux futurs et sur les différents axes de recherche dans ce domaine.

La section qui suit présente les différents chapitres de la thése, ainsi qu'un bref résumé de chacun d'entre eux.

Résumé des chapitres de la thèse

Chapitre 2 : Les réseaux de sécurité publique

Dans ce chapitre introductif, nous présentons un résumé des propriétés fondamentales des RSPs. La majeure partie du travail décrit dans cette thèse est relatif a l'application des techniques développées dans des environnements de réseaux de sécurité publique. L'objectif principal de ce chapitre étant de fournir une vue globale du domaine des RSPs, en présentant les différentes phases de gestion des situations d'urgence, des besoins des RSPs et des défis qui leur sont associés.

Certaines parties de ce chapitre ont été publiées dans :

- Giuliana Iapichino, Daniel Câmara, Christian Bonnet, Fethi Filali, Public Safety Networks, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010.

Chapitre 3 : Les réseaux vehiculaires tolérants aux délais (VDTNs)

Certaines des techniques présentées dans cette thèse utilise le concept de réseaux tolérants aux délais (DTNs) et plus particulièrement les réseaux véhiculaires tolérants aux délais (VDTNs) afin de résoudre certains des problèmes relatifs a l'amélioration de la couverture et a la diffusion de messages d'alerte dans le cas d'un désastre.

Les réseaux tolérants aux délais, appelés aussi tolérants aux délais ou encore réseaux opportunistes, ont été établis dans le but de mettre en place des modèles d'architecture tolérants aux longs délais et/ou a la présence de partitions, lors de la transmission des données a la destination.

Nous présentons dans ce chapitre les caractéristiques des DTNs et certaines des techniques développées afin d'assurer l'expédition de paquets dans ces réseaux.

Certaines parties de ce chapitre ont été publiées dans :

- Daniel Câmara, Nikolaos Frangiadakis, Christian Bonnet, Fethi Filali, Vehicular Delay Tolerant Networks, In Handbook of Research on Mobility and

Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010.

Chapitre 4 : Les points d'accès virtuels pour les communications mobiles

Dans le future, dans un monde sans fil omniprésent, toutes les routes et les villes seront très probablement couvertes par des stations de base de bord de routes (roadside units ou encore RSUs) et l'accès a ces réseaux sans fill sera aussi bien fourni aux piétons qu'aux conducteurs et passagers. Cependant, jusqu'à ce jour les points d'accès (APs) et les RSUs ne sont pas présents partout et même s'ils le sont, il y a de fortes chances qu'ils soient endommages lors d'un désastre. La conséquence principale et directe à ce genre de situation est la présence de zones non couvertes ou le seul moyen de communication est celui entre les véhicules. De plus, équiper les routes avec chaque nouvelle technologie d'accès nécessite du temps pour un déploiement à large échelle. Dans un future proche, la mise à jour et le rajout de nouvelles options aux équipements destinés aux utilisateurs serait plus facile que pour le cas de l'infrastructure de bord de route. Ce chapitre présente une technique simple, néanmoins puissante, qui permet d'étendre la portée aux nIJuds en dehors des zones de couverture. Nous nous intéressons plus particulièrement aux messages d'avertissement et à la dissémination de données en streaming.

Certaines parties de ce chapitre ont été publiées dans :

- Daniel Câmara, Christian Bonnet, Fethi Filali, Propagation of Public Safety Warning Messages, IEEE Wireless Communications & Networking Conference (WCNC) 2010, Sydney, Australia, 18-21 April 2010
- Daniel Câmara, Nikolaos Frangiadakis, Fethi Filali, Antonio Alfredo Ferreira Loureiro, Nick Roussopoulos, Virtual Access Points for Disaster Scenarios, IEEE Wireless Communications & Networking Conference (WCNC) 2009, IEEE, Budapest, Hungary, April 5-8, 2009
- Daniel Câmara, Nikolaos Frangiadakis, Fethi Filali, Antonio Alfredo Ferreira Loureiro, Nick Roussopoulos, Virtual Access Points for Stream Based Traffic Dissemination, 2008 IEEE Asia-Pacific Services Computing Conference, IEEE, Yilan, Taiwan, December 9-12, 2008
- Nikolaos Frangiadakis, Daniel Câmara, Fethi Filali, Antonio Alfredo Ferreira Loureiro, Nick Roussopoulos, Virtual access points for vehicular networks,

Mobilware 2008, 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, ACM, February 12th-15th, 2008, Innsbruck, Austria

Chapitre 5 : Les réseaux maillés (mesh)

Durant les derrières années, les réseaux sans fil maillés WMNs ont été l'objet d'une grande attention aussi bien du coté académique qu'industriel. En effet, ces réseaux apparaissent comme une technologie prometteuse pour l'accès sans fil à large bande. Dans les réseaux WMNs chaque noeud se comporte comme un routeur indépendant et ce indépendamment du fait qu'il soit ou non connecter à un autre réseau. En général, dans les environnements à surface limitée, le déploiement de réseaux complètement maillés est le moyen le plus rapide et le plus facile pour la mise en place d'un réseau sur le site du désastre. L'objectif de ce chapitre est de présenter et de discuter ce type de réseaux étant donné que les réseaux de gestion de crise se basent sur une structure maillée pour fournir des moyens de communication aux équipes présentes sur le terrain.

Certaines parties de ce chapitre ont été publiées dans :

- Ikbal Chammakhi Msadaa, Daniel Câmara, and Fethi Filali, Scheduling and CAC in IEEE 802.16 Fixed BWNs: A Comprehensive Survey and Taxonomy, to appear in IEEE Communications Surveys & Tutorials, No4, 2010

- Erlon Rodrigues Cruz, Daniel Câmara, Hélio Crestana Guardia, Providing Billing Support in WiMAX Mesh Networks, The 5th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2009), IEEE, Marrakech, Morocco, 13-14 October 2009

- Daniel Câmara and Fethi Filali, Scheduling and Call Admission Control A WiMax Mesh Networks View, Guide to Wireless Mesh Networks, Chapter 17, Springer, January, 2009

- Azzedine Boukerche, Daniel Câmara, Carlos Maurício Seródio Figueiredo, and Antonio Alfredo Ferreira Loureiro, Algorithms for Mobile Ad Hoc Networks, Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, Chapter 1, edited by Azzedine Boukerche, John Wiley and Sons, ISBN: 0470383585, October, 2008

Chapitre 6 : La gestion de la topologie

Ce chapitre présente une discussion introductive sur la gestion de la topologie et son importance dans le contexte des réseaux sans fil. Les réseaux auto-organisés représentent un facteur essentiel pour la constitution et l'utilisation de réseaux maillés.

Certaines parties de ce chapitre ont été publiées dans :

- Ikbal Chammakhi Msadaa, Daniel Câmara, and Fethi Filali, Mobility Management in WiMAX Network, WiMAX Security and Quality of Service: Providing an End to End Explanation, Wiley, accepted for publication, to appear in late 2009

- Azzedine Boukerche, Daniel Câmara, Carlos Maurício Seródio Figueiredo, and Antonio Alfredo Ferreira Loureiro, Algorithms for Mobile Ad Hoc Networks, Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, Chapter 1, edited by Azzedine Boukerche, John Wiley and Sons, ISBN: 0470383585, October, 2008

Chapitre 7 : Implémentation et maintenance d'une topologie dynamique pour le réseau CHORIST

Ce chapitre présente une proposition de solution stable et efficace pour l'implémentation et la gestion de de la structure conçue par le prjet CHORIST [33], prenant en considération les contraintes imposées par le modèle de communication. CHORIST est un projet de la Commission Eureopéen qui s'inscrit dans le cadre de la gestion des risques environnementaux et ce donc avec un interêt particulier pour les catastrophes naturelles et les accidents industriels [33].

Certaines parties de ce chapitre ont été publiées dans :

- Daniel Câmara, Christian Bonnet, Fethi Filali, Implementation and Dynamic Topology Maintenance for the CHORIST Network, The 20th Personal, Indoor and Mobile Radio Communications Symposium 2009, PIMRC'09, IEEE, Tokyo, Japan, September 13-16, 2009

Chapitre 8 : Une solution basée sur la stratégie du marché

Ce chapitre décrit un mécanisme flexible et distribue pour la gestion de la topologie et du contrôle d'admission dans les réseaux sans fils mailles/ad hoc d'une manière générale. La méthode proposée utilise les concepts économiques de l'offre et de la demande pour organiser d'une manière dynamique le réseau sans fil. Le contrôle de la topologie pour les réseaux mailles, et plus particulièrement pour les RSPs, est un problème intéressant. En effet, étant donne le fait que, même si les équipements utilises sont les mêmes, les besoins de deux sites de désastres peuvent varier d'une manière significative. Une structure de réseau qui s'apprête a un site en particulier ne l'est pas forcément pour un autre site.

Certaines parties de ce chapitre ont été publiées dans :

- Daniel Câmara, Christian Bonnet, Topology Management for Public Safety Networks, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany, June 21-24, 2009
- Daniel Câmara, Christian Bonnet, Fethi Filali, Dynamic Topology and Communication Control for Highly Dynamic Wireless Mesh Networks, A Public Safety Network Point of View, Tenth Workshop on Mobile Computing Systems and Applications (HotMobile 09), Doctoral Consortium, ACM Sigmobile, Santa Cruz, CA, February 23-24, 2009

Chapitre 9 : Conclusions et travaux futurs

Ce chapitre présente une évaluation du travail réalisé tout en mettant l'accent sur les aspects importants ainsi que les principales réalisations de cette thèse. Il donne également un aperçu sur les axes de travaux futurs et les perspectives de recherche dans les domaines s'inscrivant dans le cadre de cette thèse.

Réseaux de sécurité public

La plus grande partie de cette thèse est liée au développement des techniques pour l'amélioration des réseaux de sécurité publique (RSP).

Réseaux de sécurité publique sont établis par les autorités pour prévenir et préparer la population en cas d'une catastrophe imminente, ou de fournir l'aide pendant la crise et des phases de normalisation. Comme le montre la figure 9.2, les catastrophes peuvent varier en nature et en intensité. Les RSPs ont le rôle fondamental de fournir une communication et une coordination des opérations d'urgence. Bon nombre des problèmes du champ RSP proviennent de l'hétérogénéité des systèmes et des organismes concernés sur le site de crise et de leurs habitudes de mobilité au sein du site de la catastrophe.

Japan, ship crash - Feb/2/2009
Australia, wild fire - Feb/9/2009
France, storm - Jan/24/2009
China, flooding - June/16/2008
China, earthquake - May/24/2008

Figure 9.2: Différents scénarios de catastrophes.

Principaux aspects de les Réseaux de Sécurité Publique

Les caractéristiques et les exigences des réseaux de sécurité publique peuvent varier considérablement en fonction de leur objectif et leur placement. Toutefois, ils sont toujours essentiels à la mission. Une fois déployé, les RSP doivent être fiables, car peut-être que la vie des gens est en danger. Par exemple, les rapports du 11 de Septembre révelent que les échecs de communication ont contribué directement à la perte d'au moins 300 pompiers et ont empêché la bonne gestion des efforts de sauvetage qui a contribué à la perte de nombreuses vies, [4] [74]. Les pannes de communication ont été aussi un des obstacles à la coordination des ressources de sauvetage dans le séisme de 1995 Kobe [72]. Les problèmes de communication ont empêché les gens de ors des areas affectés de recevoir des informations sur la gravité des dommages. De cette manière les pannes ont retardé les efforts de secours qui auraient pu empêcher la perte de nombreuses vies humaines.

La fiabilité des équipements et des protocoles est une affaire sérieuse pour tout type de réseau, mais elle est encore d'autant plus importante dans le contexte de RSPs. Le maintien des possibilités de communication dans un scénario de catastrophe est un facteur crucial pour éviter la perte de vies et de dommages à la propriété [104]. Dans une catastrophe comme un tremblement de terre, une panne de courant ou des inondations, la structure du réseau sans fil principal peut être gravement affectée et "historiquement, les grandes catastrophes sont les générateurs de la plus intense vague de trafic de télécommunications" [104]. Les réseaux de communication publique, même lorsqu'ils sont disponibles, peuvent échouer non seulement en raison de dommages physiques, mais aussi en raison de surcharge de trafic. Par conséquent, les réseaux publics réguliers seuls ne sont souvent pas suffisantes pour permettre les opérations de secours et de sauvetage [104].

Cependant, des pannes d'équipement et le manque de connectivité ne sont pas les seuls problèmes rencontrés dans RSPs. Traditionnellement, les RSP sont été détenus et exploitées par les différents organismes, tels que l'application des lois, de la défense civile et des pompiers. En outre, ils peuvent appartenir et obéir à des commandes liées aux gouvernements fédéral, préfectoral ou municipal. Tous ces différents RSPs sont souvent pas interopérables, ce qui peut représenter un problème dans le cas d'une catastrophe [10]. Au cours des dernières années, certaines initiatives, telles que MESA [76], ont tenté de résoudre le problème de l'interconnectivité entre les différents organismes.

Phases de gestion des urgences

Les catastrophes peuvent être de différents types: les catastrophes naturelles, telles que las inondations, les tremblements de terre et les épidémies. Les catastrophes peuvent aussi être d'origine humaine, comme les accidents industriels et nucléaires, les accidents maritimes, les attentats terroristes. Dans les deux cas, naturels ou industriels, des vies humaines sont en danger et les infrastructures de télécommunication peuvent être sérieusement affectées.

La gestion des catastrophes comporte trois phases principales:

1. **Préparation**, à ce stade tous les équipements et les gens doivent être

prêts à entrer en action, si nécessaire. Il se compose de la formation, la maintenance des équipements et la détection des risques.

2. **Crise**, cette phase va du point de break-out (décision de répondre), à la suite de la catastrophe, où des vies peut encore être sauvées. La crise est comprise comme la réponse de la société à une catastrophe imminente, elle est différente de la catastrophe elle-même.

3. **Retour à la situation normale**, cette phase comprend la construction et l'entretien des mécanismes de communication des structures provisoires pendant que les mécanismes réguliers sont en cours de réparation ou de reconstruction.

Point d'Accès Virtuel

L'objectif principal de la technique de Point d'Accès Virtuel (VAP) est de réduire les zones non couvertes par les points d'accès en bordure de route pour minimiser le problème de l'accès intermittent aux noeuds mobiles.

Le protocole peut se résumer comme suit. Chaque noeud, après avoir reçu un message, peut devenir un VAP plus tard. Notez cependant que les VAPs pouvant renvoyer les messages plus d'une fois, en fonction de la stratégie adoptées. Les VAPs ne rediffusent les messages que dans des zones non couvertes par d'autres points d'accès ou VAPs. Le noeud est autorisé à agir comme un VAP seulement quand il est à une distance où la couche MAC ne détecte pas les transmissions des autres noeuds. Nous supposons également que la couche MAC s'occupe de résoudre les conflits et traite le problème d'accès. Dans le cas où un noeud détecte un autre noeud en qualité de VAP dans la même région, il renonce à être un VAP, même si elle se trouve dans une zone où il pourrait agir comme VAP. Les noeuds ne sont pas autorisés à agir en tant que VAPs au cours de deux intervalles de temps consécutifs.

Figure 9.3 montre un scénario typique, où un véhicule A se comporte comme VAP donne accès à un véhicule C. Le véhicule D, qui reçoit un nouveau message de l'AP, à un moment donné dans le futur, rediffuse ce message à aux noeuds sur la zone découverte. Pour des fins pratiques, nous considérons qu'il n'ya pas de différence entre les messages reçus à partir d'un point d'accés reel ou d'un VAP. Le mécanisme de propagation est coopératif et transparent, du point de vue du récepteur. Il n'y a aucune garantie que chaque noeud recevra tous les paquets, mais en utilisant VAPs, nous visons à augmenter les chances de réception.

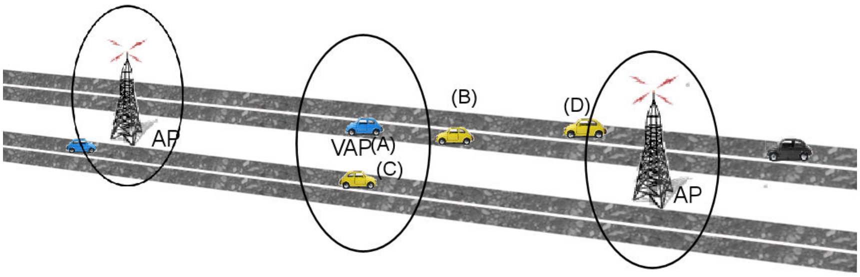


Figure 9.3: La technique VAP sur une vision de couverture de route

Évaluations

Nous présentons maintenant les évaluations effectuées pour déterminer l'impact de la technique VAP sur la diffusion du message.

Environnement

Les simulations ont été réalisées avec le simulateur Sinalgo [96], développé par le Distributed Computing Group à l'EPF de Zurich. Toutes les expériences ont été réalisées sur des machines avec Intel Xeon 1,86 GHz et 16 Go de RAM utilisant Linux Fedora Core version 6. Les graphes sont présentés avec cinq percentile et avec un intervalle de confiance de 99%. Chaque point est le résultat de la moyenne d'au moins 34 fois avec différentes configurations de réseau. La taille des zones et la période de simulation varie selon l'expérience. Les Points de Accès (PA) sont statiques et leurs positions sont choisies au hasard. Les messages sont transmis par les points d'accès disponibles à une ration de 1 message par seconde et le même message est diffusé simultanément par tous les points d'accès disponibles.

Les scénarios suivent un schéma de mobilité réaliste généré avec le logiciel VanetMobiSim [53]. Toutes les simulations gardent la même configuration de base et un seul des paramètres est varié: le nombre et positions des PAs, la taille du cache disponible, la taille du message, le type de scénario catastrophe et l'heure à laquelle a catastrophe s'est produite au cours de la simulation.

Un des principaux objectifs de ce travail est de créer des techniques qui peuvent fonctionner même dans des conditions sévères. Considérant cela, certaines expériences ont été menées pour déterminer la résistance de la technique VAP en cas de catastrophes. Ici, nous évaluons l'impact de deux types de scénario catastrophe, le premier est lorsque le réseau est endommagé par des causes naturelles et le second type, c'est quand le réseau est endommagé par sabotage. Les scénarios testés évaluent le comportement des noeuds réguliers, avant et après la catastrophe. Les noeuds sont les mêmes, et suivent des moèles de mouvement réalistes. Cela ne signifie pas que nous prétendons que la circulation sera le même avant et après un tremblement de terre, par exemple. Toutefois, en l'absence de véritables données significatives, nous avons choisi d'utiliser les schémas de mobilité réalistes comme un moyen de tester l'utilisation des VAPs pour améliorer la connectivité des noeuds restants. Les catastrophes naturelles évaluées ici sont les tremblements de terre et les inondations, alors que les scénarios de sabotage sont les panne d'électricité et un réseau de défaillances aléatoires. Ces scénarios catastrophes ont été extraites de la simulation comme suit:

Transmission stream

Cette section présente l'impact de la technique VAP plus orientée flux de trafic du type stream. Nous examinons deux types d'environnements: un segment de route et une section d'auto-route. La portion de route considérée est à $5km$ de long à quatre voies, deux dans chaque direction avec des voitures qui roulent dans les deux sens. Pour le milieu urbain, nous avons choisi a portion de $2km^2$, dans le centre-ville de Washington DC avec des voitures distribuées sur toute la surface. La superficie utilisée pour les expériences est représentée dans la figure 9.4. Pour chaque scénario, nous disposons de 40 configurations différentes de 10 minutes de simulation, avec 200 véhicules et une portée de transmission de $100m$. Pour le milieu urbain, a vitesse minimum est de $18km/h$ et le maximum est le maximum autorisé sur cette route spécifique. Pour l'environnement routier, les vitesses minimales et maximales sont de $60km/h$ et $110km/h$ respectivement.

Toutes les expériences gardent la même configuration de base et un seul paramètre varie dans chacune d'elles. Les paramètres sont variés: le taux de transmission flux, le nombre de points d'accès statiques et la méthode que les VAPs utilisent pour sélectionner les messages a rediffuser. La source du réseau génère un trafic "Constant Bit Rate (CBR)" de 1 à 3 messages par seconde. Le flux est constant et, pour cette série d'expériences, ne se répète pas. Il simule une émission de radio web, ce qui pourrait être un flux de nouvelles informations sur les canaux. Chaque scénario a génere un certain nombre de points d'accès placés au hasard. Le nombre de points d'accès testés pour les environnements de la ville est 2, 25, 50 et 100. Pour l'environnement routier, le nombre de points d'accès évaluée est 2, 5, 10 et 15. Chaque noeud mobile possède une mémoire de taille limitée où il stocke

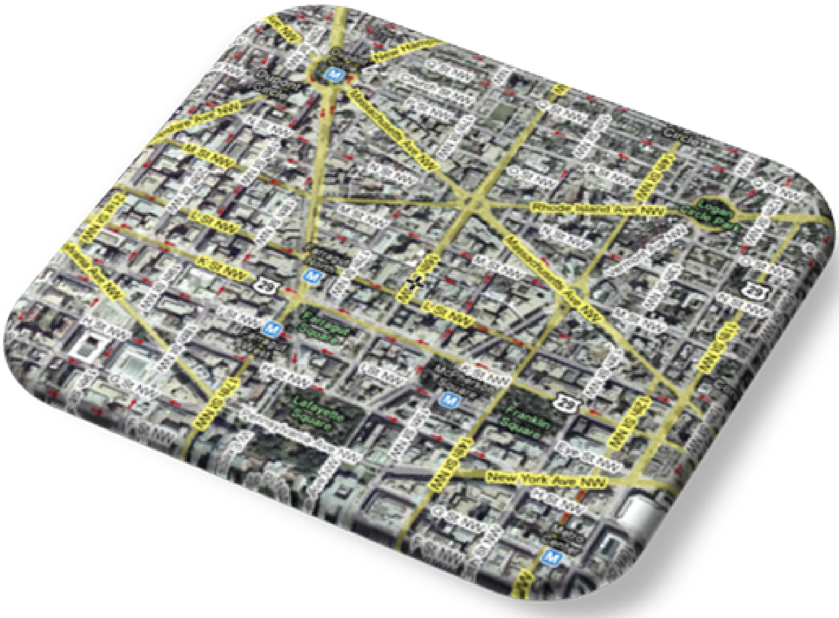


Figure 9.4: Carte montrant la région de Washington DC que nous utilisons pour les simulations

les derniers messages reçus. Lors du remplacement, le message plus ancien sont jeté pour faire de espace pour les plus nouveaux. Les trois façons les messages VAPs sont choisies pour être renvoie sont: aléatoire, le plus ancien et la plus récent.

L'utilisation de la technique VAP permet effectivement d'augmenter la couverture des points d'accès réels à l'aide des noeuds mobiles. Les graphes des figures 9.5 et 9.6 démontre histogrammes typiques des messages reçus dans un carré 2 km de simulation de Washington DC et sur un tronçon de route. Ainsi, les noeuds, en collaboration, vont aider à transmettre les paquets à des zones non couvertes. Si l'on compare la carte tracée à la carte de la région réelles, présenté dans la figure 9.4, on peut même deviner les routes et les principaux carrefours de la vile.

Les VAPs ont d'abord été conçus pour les environnements routiers, cependant, comme la figure 9.7 et la figure 9.8 montrent, ils sont est utiles dans les deux scénarios. Figure 9.7 illustre le comportement des VAPs pour un environnement routier affichant.

Le nombre de messages uniques commence à diminuer autour de 200 car à ce point les caches des noeuds commencent à saturer et la diversité flux

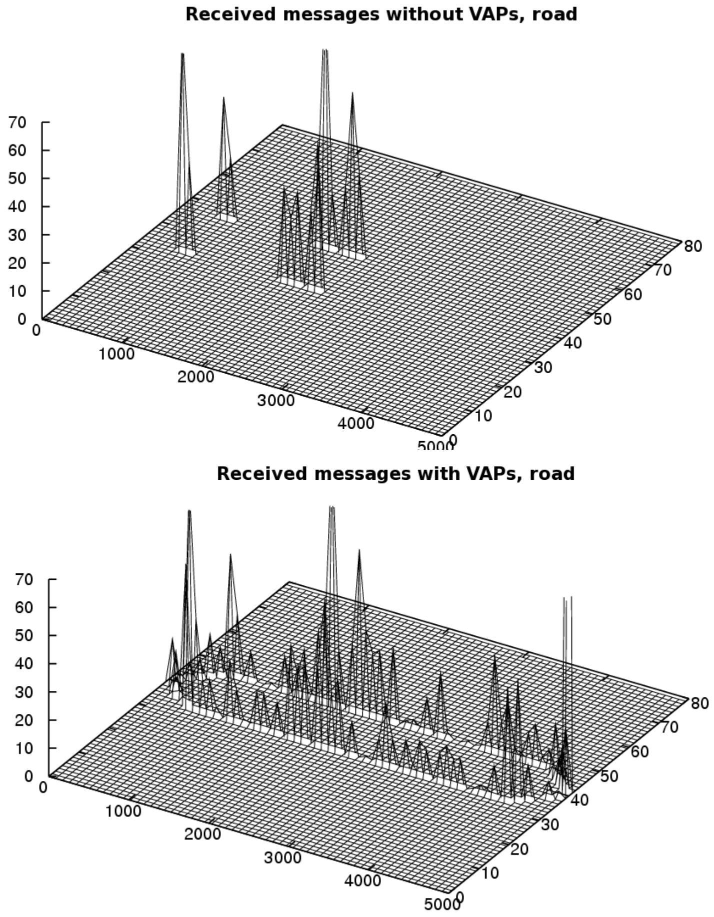
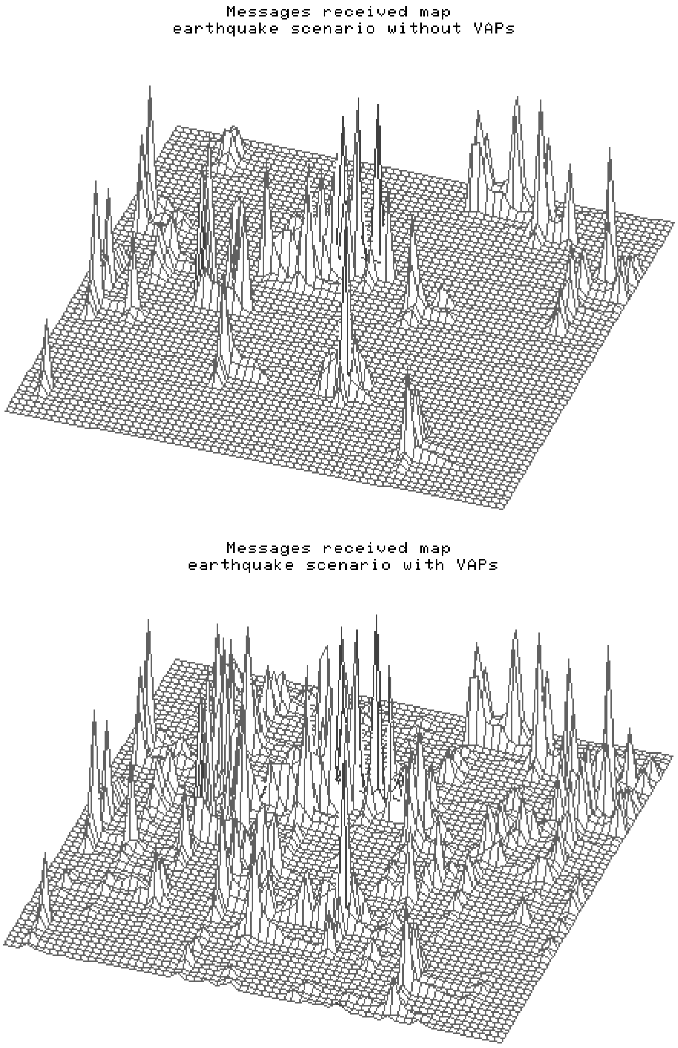


Figure 9.5: Histogramme typique des messages transmissions sur le segment de route observée

de messages entre les noeuds diminue. Cela se produit de la même façon dans le milieu urbain que sur une autoroute. Dans le scénario de la route, les voitures se déplacent perpétuellement tout au long de la route. Dans l'environnement urbain cependant le fait que les noeuds suivent des chemins différents, ça se traduit par le contenu différent dans le cache. Le nombre de messages perdus ont diminué de 10 % à 15 % pour les environnements de la ville et pour l'environnement routier, il a diminué de 10 % à 27,88%.

Figure 9.9 montre la différence entre le fait dťavoir 2 ou 25 points d'accès dans le scénario urbain en faisant varier le taux de transmission. Le nombre de points d'accès, aussi bien que le taux de transmission l'influence le nom-



Messages received map
earthquake scenario without VAPs

Messages received map
earthquake scenario with VAPs

Figure 9.6: Histogramme typique des messages transmissions sur l'expérience sur la vile

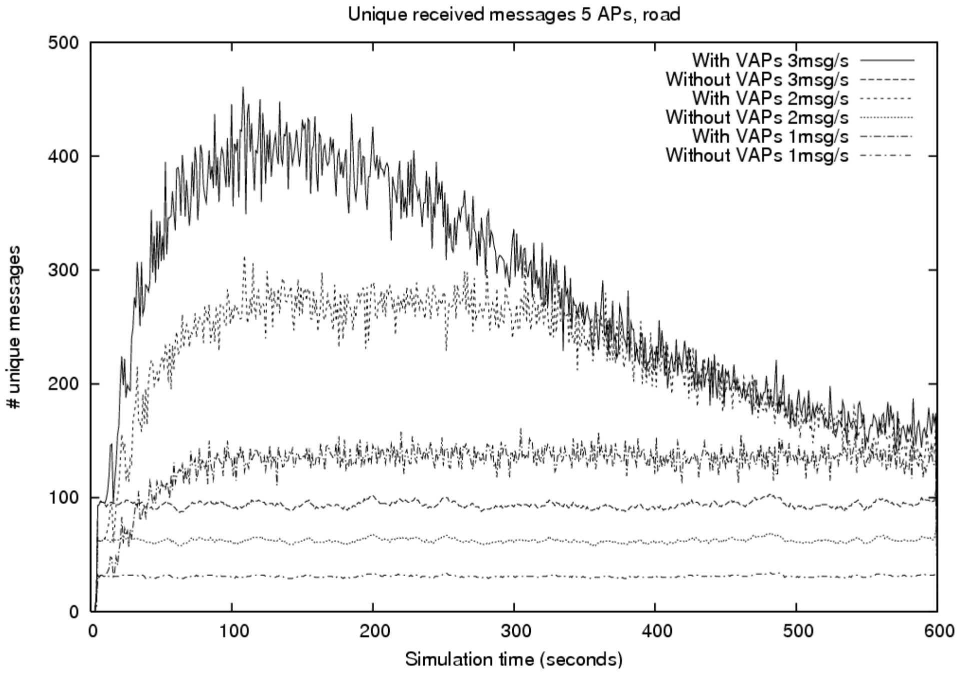


Figure 9.7: Messages uniques reçus pendant les 10 minutes de la simulation pour l'environnement routier avec des taux de circulation différentes

bre de messages uniques reçus au total. Toutefois, comme prévu, le nombre de messages uniques pour les scénarios où les VAPs ne sont pas présents est presque constant, car il ne dépend que des noeuds passant près du PA. Lorsque les VAPs sont activés, le nombre de messages unique reçus augmente significativement, car les 2 antennes ne sont pas assez pour diffuser l'information à travers l'ensemble du réseau. Les VAPs en profitent pour repropager des messages qui ont été perdus par les noeuds.

Le gain que la technique VAP présente est proportionnel au manque de couverture. Cela devient évident quand on regarde le graphique de la figure 9.10. Le graphe montre, pour les mêmes expériences, les premiers messages reçus par les AP et les VAPS. Quand le nombre de points d'accès augmente dans l'environnement routier, le nombre des premiers messages reçus par le biais des VAPs diminueVAPS. Le comportement est similaire pour l'environnement urbain.

L'utilisation des VAPS entraîne une augmentation entre 61,7% et 134,57% du trafic total du réseau. Toutefois, comme cette augmentation ne se produit

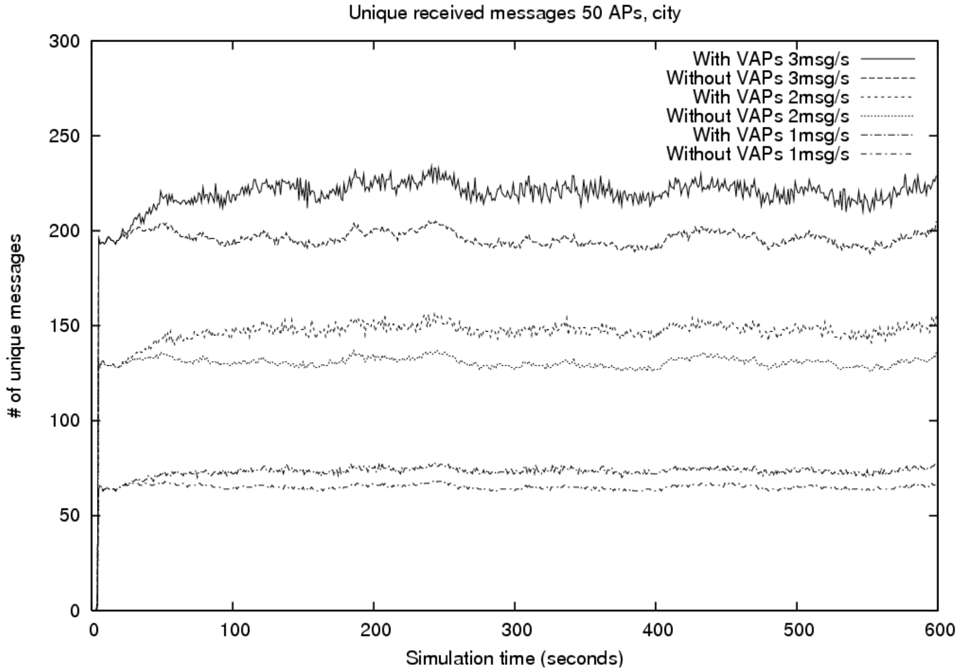


Figure 9.8: Messages uniques reçus durant les 10 minutes de la simulation pour lŠenvironnement urbain

que dans les zones non-couvertes, elle ne crée aucune interférence ni retard pour les points dŠaccès du système. Néanmoins, lévaluation de nombre de messages répétés est intéressant. Sur la figure 9.11, le nombre de messages répétés pour les réseaux qui utilisant les VAPs et ceux qui ne l'utilisent pas suit la même forme.

La Figure 9.11 présente les résultats pour différents débits, ainsi que pour différents taux de transmission. Chaque noeud VAP peut transmettre à la même vitesse du flux généré ou à 4 fois ce taux. Par exemple, si le flux est généré au taux de 1 message/seconde (m/s), les VAPs peuvent transmettre des messages à $1m/s$ ou à $4m/s$. Le nombre de messages répétés augmente en augmentant le nombre de VAPs. De cette façon, le nombre de messages répétés diminue également, comme il y a moins de VAPs actifs. Dix est presque le meilleur nombre de points d'accès pour ce scénario. Avec moins de 10 noeuds, nous avons beaucoup de zones blanches et avec plus de 10, le réseau est si couvert que les points d'accès commencent à interférer et le nombre de messages répétés augmente à nouveau, non pas en raison des

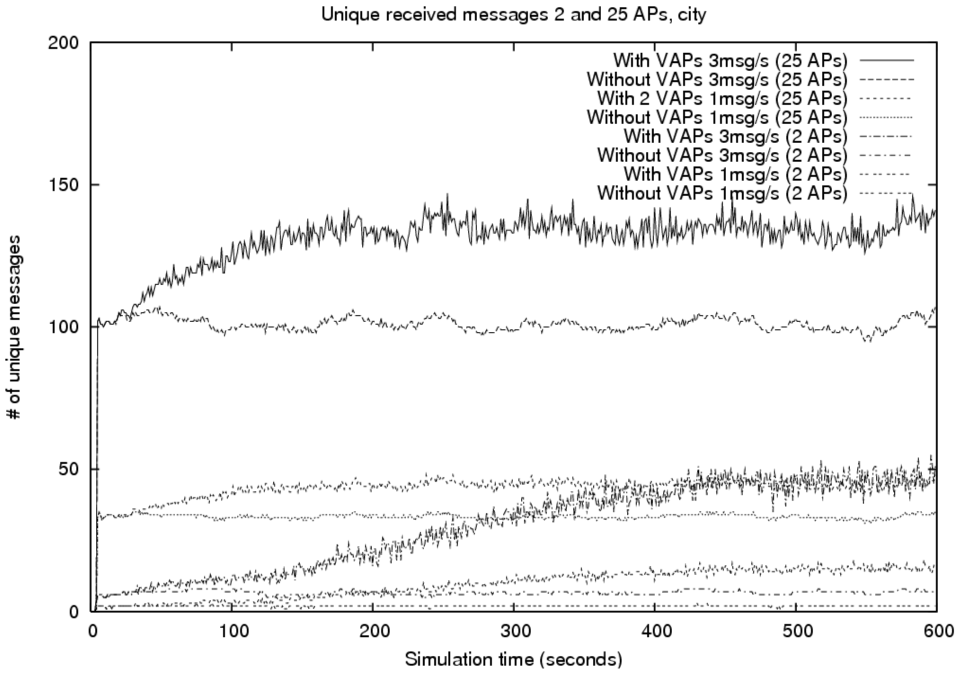


Figure 9.9: Messages uniques reçus durant les 10 minutes de simulation dans l'environnement routier avec un nombre différent de points d'accès et de taux de trafic

VAPS, mais parce qu'un noeud mobile commence à recevoir des messages de plus d'un AP.

Gestion de la Topologie

La gestion de la topologie, ou contrôle de la topologie, est lťutilisation dť algorithmes pour réduire la topologie initiale du réseau afin dť économiser de l'énergie, augmenter la durée de vie du réseau et améliorer sa stabilité. L'objectif principal est de maintenir une topologie stable, normalement visant à réduire le nombre de noeuds actifs, et/ou des liens, pour économiser les ressources et organiser le réseau.

Pour Wightman-et-Labrador [109], le contrôle de la topologie se compose de deux sous-problèmes: la construction et l'entretien topologie topologie. La construction de la topologie est la phase initiale où les noeuds sont d'abord déployés et organisés. Au début, il n'y a aucun contrôle sur la position

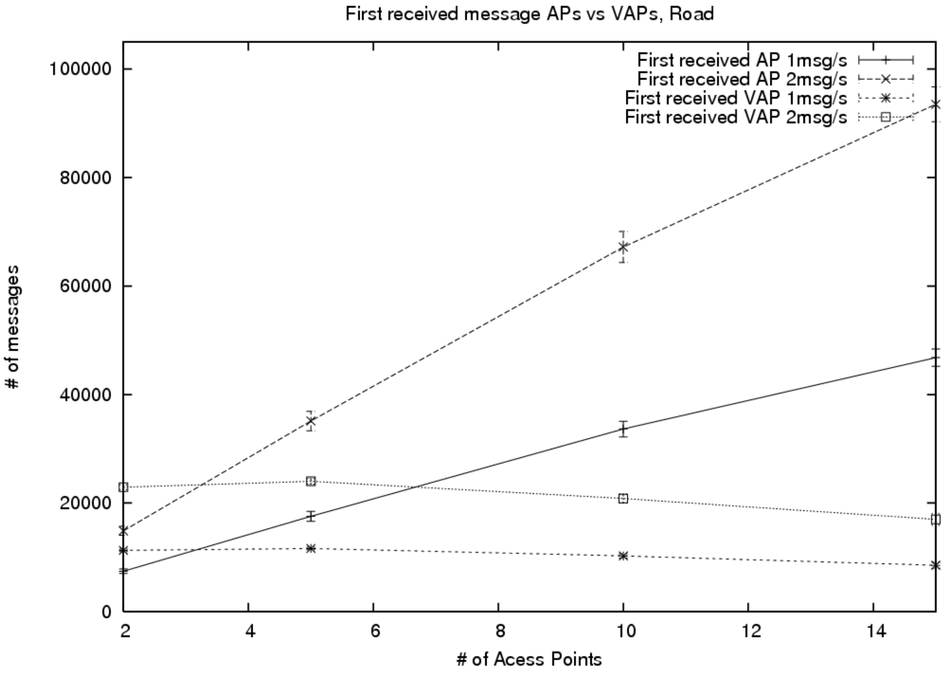


Figure 9.10: Nombre de premiers messages reçus d'un AP et VAP

des noeuds et de leurs interconnexions. Certaines zones peuvent être plus peuplées ou avoir un trop grand nombre de noeuds, et d'autres peuvent être mal couvertes et connectées. L'objectif de la phase de construction de la topologie est de minimiser ces divergences.

Le déploiement et la gestion des noeuds dans les réseaux ad hoc sans fil est un problème difficile et il devient encore plus intéressant quand on le considère dans le contexte des réseaux de sécurité publique. Non seulement ce type de réseau, par nature, est vie-critique, mais il a également des exigences strictes. En outre, ces exigences pourraient varier considérablement pour les sites de catastrophes différents [85]. Une structure de réseau stable est essentielle pour permettre la création d'algorithmes efficaces pour les couches supérieures [91]. Les RSPs doivent être fiables même quand ils sont déployés dans des environnements difficiles.

Notre approche consiste à créer un environnement du marché libre où les noeuds peuvent changer librement les points de connexions. Nous considérons que la qualité du service offerte par deux fournisseurs distincts est la même. Chaque noeud est libre de fixer ses prix, et elles varient selon la

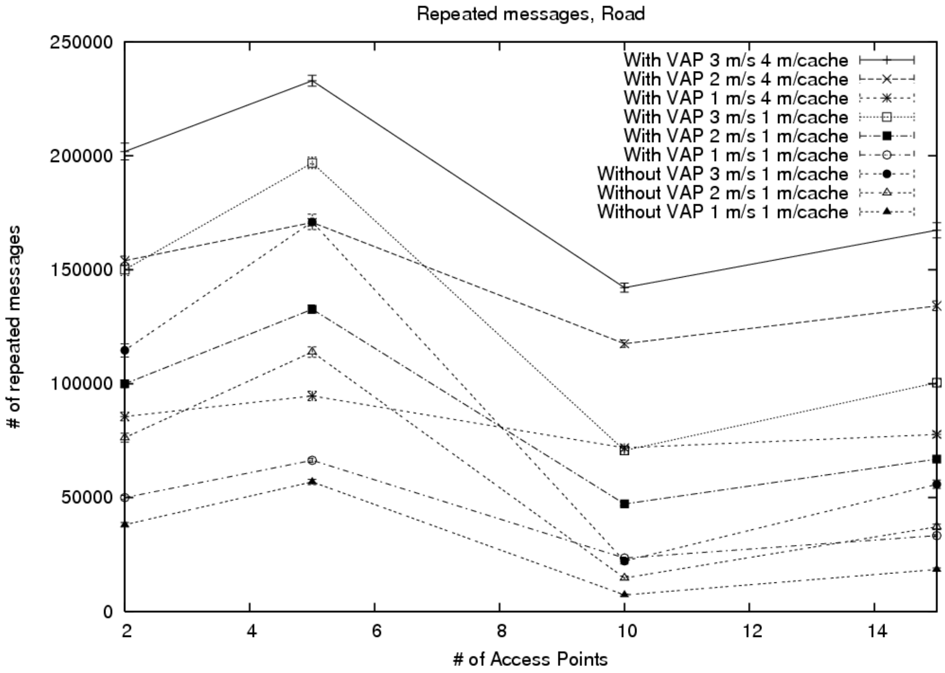


Figure 9.11: Messages répétés de l'environnement routier

charge et le type de noeud, mais entre les noeuds de la même catégorie le prix de base est la même. Les noeuds sont libres de choisir leur fournisseur et de changer de fournisseur, si ils ont un certain gain derrière cela. Dans notre configuration définitive, aucun noeud ne veut ou ne peut changer de fournisseur sans avoir à payer plus et aucun fournisseur ne peut augmenter ses prix sans perdre de clients. Ainsi, cette stratégie fondée sur le marché (MBS) atteint un équilibre qui est Pareto optimal.

Pour atteindre l'objectif principal de cette partie de la thèse, qui est la création de topologies stables, l'algorithme proposé ici a trois objectifs principaux.

1. Comme l'application cible sont RSPs, la topologie et les mécanismes visant à garantir la connectivité doivent être stable, fiable et rapidement déployables.

2. Les clusters doivent non seulement avoir à peu près la même taille, mais il est également important d'être en mesure de contrôler et d'affiner la forme du réseau et les tailles de cluster

3. Diminuer le numéro des clusters le plus possible.

La gestion de la topologie basée sur le marché

La gestion basée sur le marché (MBS) décrite ici a l'intention de créer et de maintenir des architectures de réseau bien définies d'une manière souple et dynamique. La technique a en effet le pouvoir de changer tout le comportement du réseau en ajustant un petit ensemble de paramètres, sans avoir besoin d'équipements spéciaux ou de protocoles complexes.

Nous basons notre solution sur les lois d'offre et de la demande. La première loi d'offre et de la demande nous dis que lorsque la demande est supérieure à l'offre, les prix montent et lorsque l'offre est supérieure à la demande, les prix baissent. La puissance de ces forces, montante et descendante, dépend de la différence entre l'offre et la demande. La seconde loi de l'offre et de la demande, dit que plus grand est la différence entre l'offre et la demande, plus grande est la force exercée sur les prix. La troisième loi stipule que les prix ont tendance à atteindre un point d'équilibre, où l'offre est égale à la demande [57].

Si nous alignons nos principaux objectifs avec les lois de l'offre et la demande, nous verrons que ces trois lois s'accordent parfaitement aux exigences principales d'un algorithme de gestion de la topologie

Évaluations

Les évaluations ont été faites en utilisant le simulateur Sinalgo [96] dans une zone de $2km^2$. Nous varions le nombre de noeuds et la portée de communication des noeuds. Toutes les expériences ont été réalisées en utilisant une machine Intel Xeon 1,86 GHz avec 16 Go de RAM et Linux Fedora Core version 6. Tous les graphes sont présentées avec un intervalle de confiance de 99% et chaque point est le résultat de la moyenne de 34 simulations avec différentes configurations de réseau. Les noeuds arrivent de façon aléatoire et sont placés de façon uniforme sur la zone observée. La mise en oeuvre centralisée fonctionne comme un oracle: ses résultats sont les meilleurs possibles et sont impossibles à obtenir avec des algorithmes distribués qui ont seulement une vue partielle du réseau. Toutefois, cette mise en oeuvre hors ligne nous montre à quel point l'algorithme proposé est loin de la solution théorique minimale CH optimale.

Toutes les expériences ont été réalisées pour des communication différentes de 50, 100, 150, 200, 250 et 300 mètres. Toutefois, comme les résultats définitifs de ces variations ne présentent pas de différence significative, nous ne présenterons que les valeurs obtenues pour les expériences portée de 200 mètres de communication. Pour évaluer la capacité d'adaptation de la solution proposée, nous avons défini différentes configurations de réseau et des coûts associés aux différents noeud. Nous avons créé six scénarios différents avec différents coûts de base pour chaque type de noeud. Les configurations des coûts de base utilisés dans les expériences sont:

- Configuration 1: favorise la création de clusters, autant que possible. Les valeurs de base des coûts de connexion sont CH = 20, MR = 5, RN = 1.
- Configurations 2 à 5: présentent des différences par rapport à la configuration régulière. L'objectif de ces configurations est de déterminer si de petites variations de coûts ont une influence sur le comportement des algorithmes. β Les valeurs sont:
  - Configuration 2 CH = 0, MR = 2, RN = 1
  - Configuration 3 CH = 0, MR = 5, RN = 3
  - Configuration 4 CH = 0, MR = 7, RN = 5
  - Configuration 5 CH = 0, MR = 20, RN = 5
- Configuration 6: Tente de former le réseau le plus près possible du minimum. Pour ce cas, les valeurs sont: CH = 0, MR = 50, RN = 45.

Les configurations 1 et 6 sont diamétralement opposées en dans le sens que la première vise à stimuler la création de CHs et que la seconde vise à maintenir le nombre de clusters aussi petit que possible. Les différences entre les configurations de réseau et la forme finale désirée sont exprimées par les histogrammes de la figure 9.12. Ces histogrammes ont été créés à partir de scénarios typiques de simulation. Nous pouvons observer que la technique arrive vraiment à contrôler la topologie du réseau allant du cas extrême d'un nombre à peu près au minimum de CHs.

Figure 9.13 montre un exemple du comportement attendu de l'algorithme de cluster simple qui a été simulé. Figure 9.14 montre la machine d'état pour l'algorithme de cluster générique.

Le graphe de la figure 9.15 nous montre le nombre de CH crée pour l'algorithme de cluster simple. Nous pouvons également observer que le nombre de CHs sont créées dans tel que prévu. Les petits changements dans le coût des valeurs montrent également que l'utilisation de la technique nous permet de faire un contrôle à grain fin du réseau. En ce qui concerne la

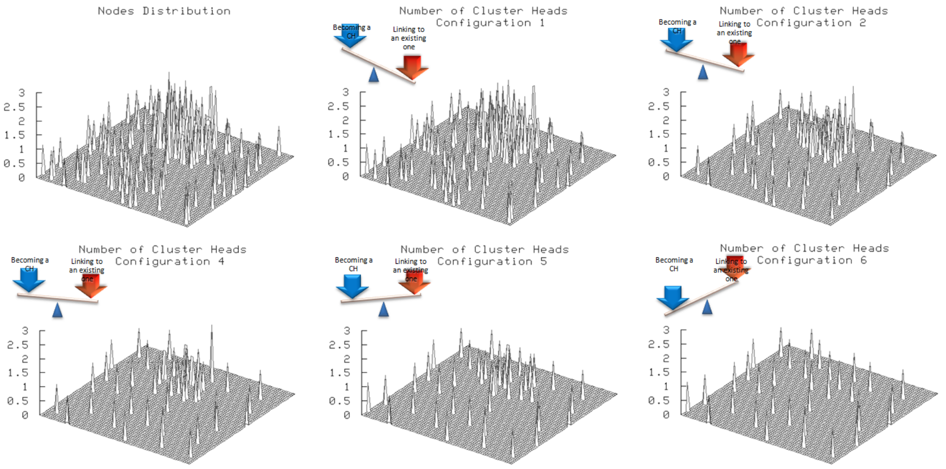


Figure 9.12: Nombre de clusters réparties à travers le réseau en fonction de différentes configurations évaluées.

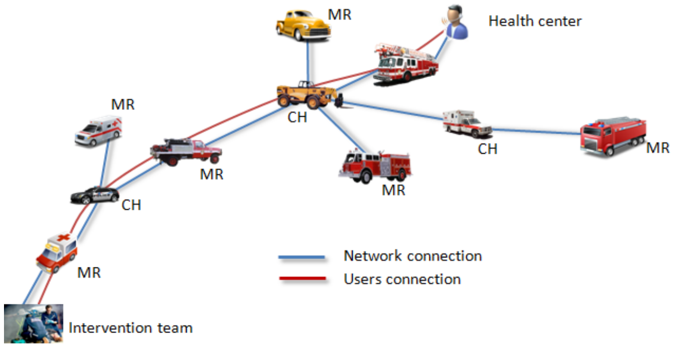


Figure 9.13: architecture cluster simple, montrant une communication de bout en bout aux utilisateurs

configuration minimale, les valeurs de configuration accessibles en 6 sont très proches de celles trouvées par l'algorithme minimum WCIDS, normalement à l'intérieur de l'intervalle de confiance de 99%.

La figure 9.16 présente le taille moyenne des groupes. Nous définissons la taille de cluster comme: $RSE = (RMN + RRN)/nCH$, où RSE est le rapport entre la taille des clusters, RMN RRN et NCH qui sont respectivement le nombre de routeurs mobiles, noeuds de relais et les cluster-heads de l'ensemble du réseau. La moyenne indiquée est la moyenne calculée sur tous les scénarios évalués. A partir de ces graphes, nous pouvons percevoir que

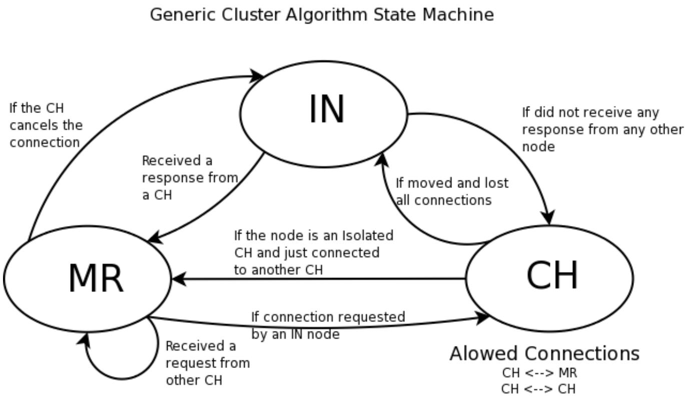

Generic Cluster Algorithm State Machine
IN
MR
CH
If the CH cancels the connection
Received a response from a CH
If did not receive any response from any other node
If moved and lost all connections
If the node is an Isolated CH and just connected to another CH
If connection requested by an IN node
Received a request from other CH
Alowed Connections
CH <--> MR
CH <--> CH

Figure 9.14: machine de l'Etat pour l'algorithme de cluster générique

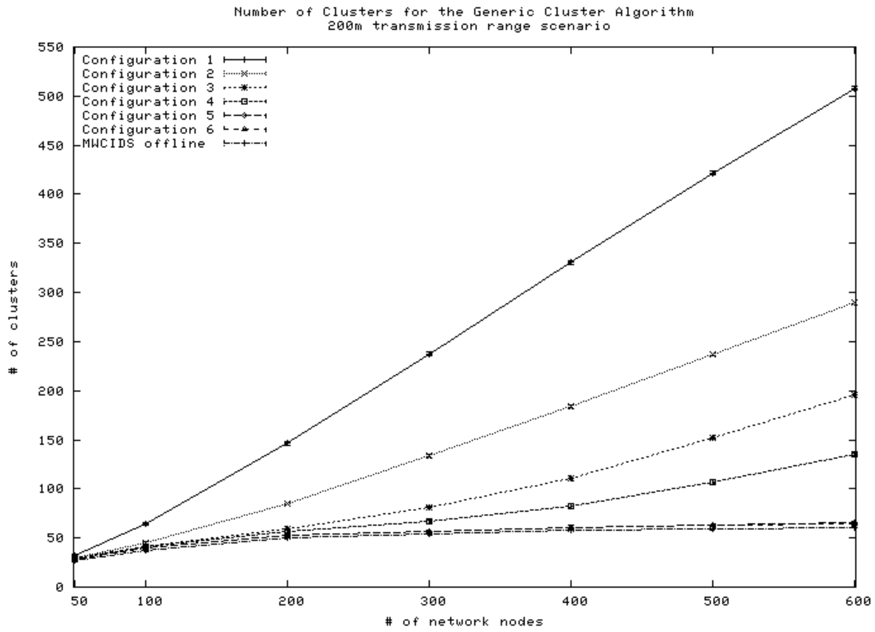


Figure 9.15: Nombre de noeuds tête de groupe pour la topologie de regroupement génériques

par un ajustement précis des coûts, nous pouvons modéliser le comportement des groupes. Nous pouvons percevoir que les graphes démontrent que les différentes configurations permettent d'atteindre un point stable, sauf la configuration où nous avons l'intention d'augmenter le nombre de clusters, autant que possible. La taille moyenne des clusters atteint un point de saturation et reste stable indépendamment du nombre de noeuds dans le réseau.

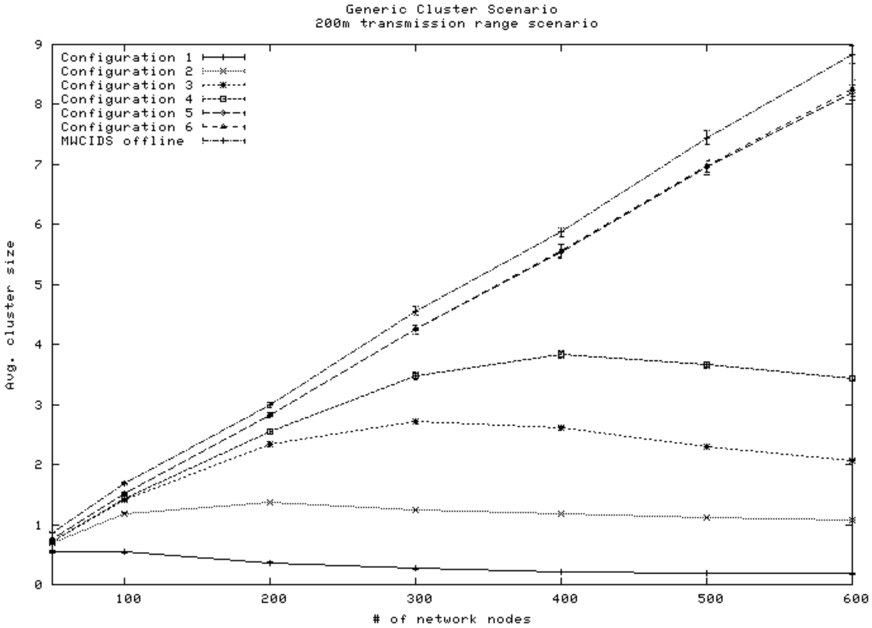


Figure 9.16: Nombre de noeuds par cluster pour la topologie de regroupement génériques

Bibliography

[1] IEEE Standard 802.16-2004, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std 802.16e, February 2006

[2] IEEE Standard 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Oct. 2004

[3] IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz, IEEE Std. 802.16a, Apr. 2003

[4] 9/11 Commission, National Commission on Terrorist Attacks Upon the United States. 2004. The 9/11 Commission Report: final Report of the National Commission on Terrorist Attacks Upon the United States, Retrieved October 13, 2009, from http://www.9-11commission.gov

[5] M. H. Ahmed, Call admission control in wireless networks: a comprehensive survey, Com-munications Surveys & Tutorials, IEEE, First Qtr. 2005, 7(1): 49-68

[6] I. F. Akyildiz, X. Wang, and W. Wang, Wireless mesh networks: a survey. Computer Networks; 47(4): 445-487, 2005

[7] Anthony M. Townsend, and Mitchell L. Moss, Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications, Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service, New York University, May 6, 2005

[8] N. Aschenbruck, E. Gerhards-Padilla, M. Gerharz, Frank, and M. Martini, Modelling mobility in disaster area scenarios, In Proceedings of the ACM MSWiM '07, Chania, Crete Island, Greece, October, 2007

[9] N. Aschenbruck, C. de Waal, and P. Martini Distribution of Nodes in Disaster Area Scenarios and its Impact on Topology Control Strategies, 2nd MCN, in conjunction with the IEEE Infocom, Phoenix, AZ, USA, April 18, 2008

[10] K. Balachandran, K. C. Budka, T. P. Chu, T. L. Doumi, and J. H. Kang, Mobile Responder Communication Networks for Public Safety, IEEE Communications Magazine, January, 2006

[11] L. Bao, and J.J. Garcia-Luna-Aceves, Topology management in ad hoc networks, In Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03), Annapolis, MD, USA, 2003

[12] J. Q. Bao and W. C. Lee, Rapid deployment of wireless ad hoc backbone networks for public safety incident management, in Proc. IEEE Globecom, Washington D.C., USA, November, 2007

[13] P. Basu, N. Khan, and T. D. C. Little, A mobility based metric for clustering in mobile ad hoc networks. In Proceedings of the International Workshop on Wireless Networks and Mobile Computing (WNMC'01), Scottsdale, AZ, USA, 2001

[14] E. M. Belding-Royer, Multi-Level Hierarchies for Scalable Ad hoc Routing , Kluwer, Wireless Networks 9, 461-2013478, 2003

[15] C. Bettstetter, H. Hartenstein and X. Perez-Costa, Stochastic properties of the random waypoint mobility model: epoch length, direction distribution, and cell change rate. In Proceedings of ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, 2002

[16] D. Beyer, N. van Waes, and C. Eklund, Tutorial: 802.16 AC Layer Mesh Extensions Over-views, IEEE 802.16 (document S802.16a-02/30), St. Louis, March 11, 2002

[17] R. Bruno, M. Conti and E. Gregori, Mesh networks: commodity multihop ad hoc networks. IEEE Communications Magazine 2005; 43(3): 123-134

[18] J. Burgess, B. Gallagher, D. Jensen, D. and B. Levine, MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks, Proc. IEEE Infocom, Barcelona, Spain, April, 2006

[19] D. Câmara, A. A. F. Loureiro, and F. Filali, Methodology for Formal Verification of Routing Protocols for Ad Hoc Wireless Networks, IEEE GLOBECOM 2007, Washington, DC, November, 2007

[20] D. Câmara and C. Bonnet, Topology Management for Public Safety Networks, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany, June, 2009.

[21] J. Camp, and E. Knightly, The IEEE 802.11s Extended Service Set Mesh Networking Standard, IEEE Communications Magazine, 46(8):120-126, August 2008

[22] C. A. V. Campos, D. C. Otero and de Moraes, Realistic individual mobility Markovian models for mobile ad hoc networks, Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE , vol.4, no., pp. 1980-1985 Vol.4, 21-25, March, 2004

[23] M. Cao, W. Ma, Q. Zhang, X. Wang, and W. Zhu, Modelling and performance analysis of the distributed scheduler in IEEE 802.16 mesh mode, MobiHoc '05. ACM Press, Urbana-Champaign, IL, USA, May 25 - 27, 2005

[24] Min Cao, Wenchao Ma, Qian Zhang, Xiaodong Wang, Analysis of IEEE 802.16 Mesh Mode Scheduler Performance, IEEE Transactions on Wireless Communications, vol. 6, no. 4, April 2007

[25] Min Cao, Vivek Raghunathan, and P. R. Kumar, A Tractable Algorithm for Fair and Efficient Uplink Scheduling of Multi-hop WiMax Mesh Networks, Proceedings Second IEEE Workshop on Wireless Mesh Networks, pp. 101-108, Reston, VA, Sep. 25, 2006

[26] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall and H. Weiss, Delay Tolerant Network Architecture, April, 2007, Retrieved October 18, 2009, from http://www.ietf.org/rfc/rfc4838.txt

[27] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. Pocket Switched Networks: Real-world mobility and its consequences for Opportunistic Forwarding. Technical Report UCAM-CL-TR-617, University of Cambridge, 2005

[28] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass and, J. Scott, Impact of Human Mobility on Opportunistic Forwarding Algorithms, IEEE Transactions on Mobile Computing 6, 6, Jun, 2007

[29] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris. Span: An energy-eficient coordination algorithm for topology maintenance in ad hoc wireless networks, In Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom'01), Rome, Italy, 2001

[30] S. Cheng, P. Lin, D. Huang, and S. Yang, A study on distributed/centralized scheduling for wireless mesh network, In Proceeding of the 2006 International Conference on Communications and Mobile Computing, ACM Press, Vancouver, British Columbia, Canada, July, 2006

[31] H. T. Cheng, H. Jiang, and W. Zhuang, Distributed medium access control for wireless mesh networks, Wireless Communications and Mobile Computing, V.6, I.6, Sep. 2006

[32] C. Chiang, Wireless Networks Multicasting. PhD thesis, Department of Computer Science, University of California, Los Angeles, USA, 1998

[33] CHORIST, Integrating Communications for enHanced envirOnmental RISk management and citizens safeTy Information Society Technologies - FP6 programme, Retrieved December 01, 2009, from http://www.chorist.eu

[34] V. Chvatal, A greedy heuristic for the set-covering problem, Math of Operation Research, vol. 4, no. 3, 1979

[35] Larry Collins, Technical Rescue Operations: Common Emergencies, Published by PennWell Books, 2005

[36] Congressional Budget Office, H.R. 6658 Disaster Response, Recovery, and Mitigation Enhancement Act of 2008, Congressional Budget Office Cost Estimate, October, 2008

[37] S. Das, A. Nandan, G. Pau, M. Y. Sanadidi and M. Gerla, SPAWN: Swarming Protocols for Vehicular Ad Hoc Wireless Networks, Proceedings of the First ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2004), Berkeley, 2004

[38] R. B. Dilmaghani, and R. R. Rao, On Designing Communication Networks for Emergency Situations, In Proc. IEEE International Symposium on Technology and Society (ISTAS 2006), June, 2006

[39] P. Djukic, and S. Valaee, 802.16 mesh networking, in Handbook of WiMAX (S. Ahson and M. Ilyas, eds.), CRC Press, 2007

[40] DTNRG Delay Tolerant Networking Research Group, 2009, Retrieved October 18, 2009, from http://www.dtnrg.org/wiki

[41] ETSI TR102_638, Draft ETSI TR 102 638 V1.0.7, Technical Report, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, June, 2009

[42] K. Fall, A Delay-Tolerant Network Architecture for Challenged Internets, In ACM SIGCOMM, Karlsruhe, Germany, August, 2003

[43] FEMA, Integrated Public Alert and Warning System (IPAWS), FEMA website, Retrieved October 13, 2009, from http://www.fema.gov/emergency/ipaws/

[44] G. G. Finn, Routing and addressing problems in large metropolitan scale internetworks, Technical Report RR-87-180, ISI Research Report, 1987

[45] M. Fiore, J. Haerri, C. Bonnet, F. Filali, Vehicular mobility simulation for VANETs, ANSS-40 2007, 40th IEEE Annual Simulation Symposium, Norfolk, USA, March, 2007

[46] N. Frangiadakis, D. Câmara, F. Filali, A. A. F. Loureiro and N. Roussopoulos, Virtual access points for vehicular networks, Mobilware 2008, 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, ACM, Innsbruck, Austria, February, 2008

[47] R. Gandhi and S. Parthasarathy, Distributed algorithms for connected domination in wireless networks, J. Parallel Distrib. Comput., Jul. 2007

[48] M. Garey, and D. Johnson, Computers and Intractability: A Guide to the Theory of NP-Complet., Freeman, New York, 1979

[49] S. Guha, and S. Khuller, Approximation Algorithms for Connected Dominating Sets, Algorithmica, volume 20, 1998

[50] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and Patil, L. (2008, August). Proxy Mobile IPv6, IETF RFC 5213

[51] J. Haerri, C. Bonnet, F. Filali, Kinetic graphs: a framework for capturing the dynamics of mobile structures in MANET, EURECOM, Rapport de recherche RR-07-195, May, 2007

[52] K. Harras and K. Almeroth, Transport Layer Issues in Delay Tolerant Mobile Networks, IFIP Networking, Coimbra, Portugal, May, 2006

[53] J. Harri, M. Fiore, F. Fethi, and C. Bonnet, VanetMobiSim: generating realistic mobility patterns for VANETs, in Proc. of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET'06), Los Angeles, USA, September 29, 2006

[54] T. W. Haynes, S. T. Hedetniemi, and Peter J. Slater, Fundamentals of Domination in Graphs, CRC; 1 ed., Jan, 1998

[55] T. C. Hou, and V. O. K. Li, Transmission range control in multihop packet radio terminals, IEEE Transactions on Communications, 34(1):38-44, 1986

[56] Y. Huang, W. He, K. Nahrstedt and W. C. Lee, Incident Scene Mobility Analysis, IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability, May, 2008

[57] Hubert D. Henderson, Supply And Demand, Kessinger Publishing Company, July 2004

[58] P. Hui and J. Crowcroft, How small labels create big improvements, Fifth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom Workshops'07, pp. 65-70, White Plains, New York, USA, 19-23 March, 2007

[59] G. Iapichino, C. Bonnet, O. Del Rio Herrero, C. Baudoin and I. Buret, Combining Mobility and Heterogeneous Networking for Emergency Management : a PMIPv6 and HIP-based Approach, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany, June, 2009

[60] IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE), U.S. Department of Transportation, January 9, 2006

[61] Intelligent Car, Intelligent Car | Europa - Information Society, Retrieved October 18, 2009, from http://ec.europa.eu/information_society/activities/intelligentcar/index_en.htm

[62] IPNRG, InterPlanetary Internet Special Interest Group, Retrieved October 18, 2009, from http://www.ipnsig.org/home.htm

[63] IRTF, IRTF-Internet Research Task Force, Retrieved October 18, 2009, from http://www.irtf.org/

[64] S. Jain, K. Fall, R. and Patra, Routing in a Delay Tolerant Network, ACM, SIGCOMM'04, Portland, Oregon, USA, August, 2004

[65] L. Jia, R. Rajaraman, and T. Suel. An eficient distributed algorithm for constructing small dominating sets. In Proceedings of the ACM Symposium on on Principles of Distributed Computing (PODS'01), Newport, RI, USA, 2001

[66] D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6, IETF RFC 3775, June, 2004

[67] E. P. C. Jones, Practical Routing in Delay-Tolerant Networks, Master thesis, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, 2006

[68] H. Kaneda, K. Kobayashi, H. Tajima and H. Tosaki, Japan's Missile Defense: Diplomatic and Security Policies in a Changing Strategic Environment, Japan Institute of International Affairs, March, 2007

[69] Mehmet S. Kuran, and Tuna Tugcu, A survey on emerging broadband wireless access technolo-gies, The International Journal of Computer and Telecommunications Networking, Volume 51 , Issue 11 August 2007

[70] Miguel A. Labrador, Pedro M. Wightman, Topology Control in Wireless Sensor Networks with a companion simulation tool for teaching and research, Springer Science + Business Media B.V., 2009

[71] C. Liu and J. Wu, Scalable Routing in Delay Tolerant Networks, ACM MobiHoc'07, Montreal, Quebec, Canada, September, 2007

[72] H. Lorin, H. Unger, P. Kulling and L. Ytterborn, The great Hanshin-Awaji (Kobe) earthquake January 17, 1995, KAMEDO Report No 66, SoS Report 1996: 12

[73] G. Mainland, L. Kang, Sébastien Lahaie, D. C. Parkes, and M. Welsh, Using virtual markets to program global behavior in sensor networks, ACM SIGOPS European Workshop, Leuven, Belgium, Sept., 2004

[74] McKinsey and Co., Increasing FDNY's Preparedness, City of New York: New York City Fire Department web site, 2002, Retrieved October 13, 2009,from http://www.nyc.gov/html/fdny/html/mck_report/toc.html

[75] T. Melodia, D. Pompili, and I.F. Akyildiz, On the interdependence of topology control and geographical routing in ad hoc and sensor networks, IEEE Journal on Selected Areas in Communications, 23(3):520-532, 2005

[76] MESA, Project MESA - Mobile Broadband for Public Safety, Retrieved October 13, 2009, from http://www.projectmesa.org/

[77] S. F. Midkiff and C. W. Bostia, Rapidly-deployable broadband wireless networks for disaster and emergency response. In Proc. First IEEE Workshop on Disaster Recover Networks, June 2002

[78] R. Moskowitz, P. Nikander, P. Jokela and T. Henderson, Host Identity Protocol, IETF RFC 5201, April, 2008

[79] P. Mundur and M. Seligman, Delay Tolerant Network Routing: Beyond Epidemic Routing, Proc. of ISWPC, Santorini, Greece, May, 2008

[80] A. Nandan, S. Das, G. Pau, M. Y. Sanadidi and M. Gerla, Cooperative Downloading in Vehicular Ad Hoc Wireless Networks, Proceedings of IEEE/IFIP International Conference on Wireless On demand Network Systems and Services, St. Moritz, Switzerland, January, 2005

[81] R. Nelson, and L. Kleinrock, The spatial capacity of a slotted aloha multihop packet radio network with capture. IEEE Transactions on Communications, 32(6):684-694, 1984

[82] P. Nikander, T. Henderson, C. Vogt and J. Arkko, End-Host Mobility and Multihoming with the Host Identity Protocol, IETF RFC 5206, April, 2008

[83] D. Niyato, P. Wang and C. M. Teo, Performance analysis of the vehicular delay tolerant network, Proc. IEEE WCNC'09, Budapest, Hungary, April, 2009

[84] Open Air Interface, Retrieved December 19, 2009, from http://www.openairinterface.org/

[85] Rajmohan Rajaraman, Topology control and routing in ad hoc networks: a survey, ACM SIGACT News, v.33 n.2, June 2002

[86] R. Ramanathan, and R. Hain, Topology control of multihop wireless ntworks using transmit power adjustment. In IEEE INFOCOM, pages 404-413, Telaviv, Israel, March 2000

[87] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain and R. Krishnan, Prioritized epidemic routing for opportunistic networks. In Proceedings of the 1st international Mobisys Workshop on Mobile Opportunistic Networking, San Juan, Puerto Rico, June, 2007

[88] RATCOM, the Risk prevention, RATCOM website, Retrieved October 13, 2009, from http://ratcom.org/default.aspx

[89] Simone Redana, Matthias Lott, Performance Analysis of IEEE 802.16a in Mesh Operation Mode, in Proc. of IST SUMMIT 2004, Lyon, France, June 2004

[90] H. C. Sanchez, L. Franck and A. Beylot, Routing metrics in Delay Tolerant Networks, Rapport de recherche, IRIT/RR–2007-22–FR, Institut National Polytechnique de Toulouse, Novembre, 2007, Retrieved October 18, 2009, from http://www.enseeiht.fr/b̃eylot/IRITBeylot6.pdf

[91] P. Santi, Topology Control in Wireless Ad Hoc and Sensor Networks, WILEY, July 2005

[92] P. Santi, Topology control in wireless ad hoc and sensor networks, ACM Comput. Surv. 37, 2, 164-194, Jun. 2005

[93] A. Sarrafi, M. H. Firooz, and H. Barjini, A Cluster Based Topology Control Algorithm for Wireless Ad-Hoc Networks, International Conference on Systems and Networks Communication, October, 2006

[94] R. Shah, S. Roy, S. Jain and W. Brunette, Data mules: Modeling a three tier architecture for sparse sensor networks, IEEE Sensor Network Protocols and Applications, 2003

[95] J. Shen, S. Moh and I. Chung, Routing Protocols in Delay Tolerant Networks: A Comparative Survey, The 23rd International Technical Conference on Circuits/Systems, Computers and Communications, Kaikyo Messe Shimonoseki, Shimonoseki City, Yamaguchi-Pref., Japan, 2008

[96] Distributed Computing Group at ETH Zurich, Sinalgo - Simulator for Network Algorithms, Retrieved December 19, 2009, from http://disco.ethz.ch/projects/sinalgo/

[97] R. Sivakumar, P. Sinha, and V. Bharghavan. Cedar: A core-extraction distributed ad hoc routing algorithm. IEEE Journal on Selected Areas in Communications, 17(8): 1454-14655, 1999

[98] T. Small and Z. J. Haas, The Shared Wireless Infostation Model- A New Ad Hoc Networking Paradigm (or Where there is aWhale, there is aWay), In Proceedings of ACMInternational Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), pp. 233–244, 2003

[99] T. Small and Z. J. Haas, Resource and Performance Tradeoffs in Delay-Tolerant Wireless Networks, ACM, SIGCOMM'05 workshop on Delay Tolerant Networking and Related Topics (WDTN), pp. 260-267, Philadelphia, PA, USA, August, 2005

[100] T. Spyropoulos, K. Psounis and C. S. Raghavendra, Performance analysis of mobility-assisted routing, ACM Mobihoc 2006, Florence, Italy, May, 2006

[101] Yong Sun, Dharma Basgeet, Khurram Rizvi, Zhong Fan, Paul Strauch, Dynamic Frame Structure for IEEE802.16j Relaying Transmission to Support Efficient Scheduling, IEEE 802.16, IEEE C80216j-06_224, November, 07, 2006

[102] H. Takagi, and L. Kleinrock, Optimal transmission ranges for randomly distributed packet radio terminals. IEEE Transactions on Communications, 32(3):246-257, 1984

[103] M. Tariq, M. Ammar and E. Zegura, Message Ferry Route Design for Sparse Ad hoc Networks with Mobile Nodes, ACM Mobihoc 2006, Florence, Italy, May, 2006

[104] A. M. Townsend and M. L. Moss, Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications, Center for Catastrophe Preparedness and Response and Robert F. Wagner Graduate School of Public Service, New York University, May, 2005

[105] A. Vahdat and D. Becker, Epidemic routing for partially connected ad hoc networks, Technical Report CS-2000-06, Duke University, 2000

[106] Y. Wang, H. Wu, DFT-MSN: The Delay Fault Tolerant Mobile Sensor Network for Pervasive Information Gathering. In Proceedings of Twenty-fifth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2006

[107] Y. Wang, H. Dang and H. Wu, A survey on analytic studies of Delay-Tolerant Mobile Sensor Networks, Wiley, Wirel. Commun. Mob. Comput. 2007; 7:1197-1208 Published online 16 May 2007

[108] WIDENS, Wireless Deployable Network System, 2006, Retrieved October 13, 2009, from http://www.comlab.hut.fi/projects/WIDENS/

[109] Pedro Wightman and Miguel A. Labrador, Topology Maintenance: Extending the Lifetime of Wireless Sensor Networks, IEEE LatinCom 2009, Medellin, Colombia, Sept. 8 - 11, 2009

[110] Y. Xu, S. Bien, Y. Mori, J. Heidemannn, and D. Estrin, Topology control protocols to conserve energy in wireless ad hoc networks, Technical Report Center for Embedded Networked Sensing Technical Report 6, UCLA, 2003

[111] Q. Xu, T. Mark, J. Ko and R. Sengupta, Vehicle-to-Vehicle Safety Messaging in DSRC, in Proc. of ACM VANET, 2004

[112] Xiaokai Yang, Economics: New Classical Versus Neoclassical Frameworks, Wiley-Blackwell, Jan 2001

[113] X. Yang, J. Liu, F. Zhao and N. Vaidya, A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning, in Proc. of ACM MOBIQUITOUS, 2004

[114] J. Zander, Radio Resource Management in Future Wireless Networks: Requirements and Limitations, IEEE Commun. Mag., vol. 35, no. 8, pp. 30-36, Aug. 1997

[115] Rui Zhao, Mesh Distributed Coordination Function for Efficient Wireless Mesh Networks Supporting QoS, Communication Networks, RWTH Aachen University, Master Thesis, April 2007

[116] Hua Zhu and Kejie Lu, Performance of IEEE 802.16 Mesh Coordinated Distributed Scheduling Under Realistic Non-Quasi-Interference Channel, in Proc. of the International Conference on Wireless Networks (ICWN'06), Las Vegas, USA, June 26-29, 2006

[117] M. Zonoozi and P. Dassanayake, User Mobility Modeling and Characterization of Mobility Patterns. IEEE Journal on Selected Areas in Communications 1997; 15(7): 1239–1252, 1997