Wireless Network
Segregation Utilising Modulo in Industrial Environments

By
Athanasios Paraskelidis

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth

School of Computing
University of Portsmouth
Lion Terrace, Portsmouth, Hampshire
PO1 3HE, United Kingdom

Date: February 2010
Abstract

With the success of wireless technologies in consumer electronics, standard wireless technologies are envisioned for the deployment in industrial environments as well. Industrial applications involving mobile subsystems or just the desire to save cabling make wireless technologies attractive. In industrial environments, timing and reliability are well catered by the current wired technologies. When wireless links are included, reliability and timing requirements are significantly more difficult to meet, due to the common problems that influence them such as interference, multipath and attenuation.

Since the introduction of the IEEE 802.11 standard, researchers have moved from the concept of deploying a single channel and proposed the utilisation of multiple channels within a wireless network. This new scheme posed a new problem, the ability to coordinate the various channels and the majority of the proposed works focus on mechanisms that would reduce the adjacent channel interference caused by the use of partially overlapping channels. These mechanisms are mainly algorithms that define rules to the allocation of the channels for the wireless nodes during each transmission. Many of the approached proposed during the last years have two very common disadvantages, they are hard to implement in real life and they do not take full advantage of the available spectrum, because they use only non-overlapping channels. The industries demand for solutions which would not move away from using proprietary hardware and software and any changes required to be made should not limit the availability of support for their networks. This would keep the cost low as it is the main factor that industries decide to replace their wires with radio links.

The proposed idea in this thesis borrows the concept of network segregation, firstly introduced for security purposes in wired networks, by dividing a wireless network into smaller independent subnetworks and in collaboration with a channel assignment, the Modulo. Modulo defines a set of rules that nodes should obey to when they transmit data. The utilization of multiple channels under the guidance of Modulo for each subnetwork, proves to improve the performance of an ad-hoc network even in noisy industrial environments with high levels of interference from external sources.
Acknowledgments

A number of people have contributed indirectly to this thesis in their support, discussions, ideas and friendship, many more than I could hope to list. They deserve a lot of respect and gratitude. It is really impossible to write all of their names here and I do apologize that I cannot acknowledge everyone by name.

First and foremost I would like to thank my family for their continuing support. Despite their apprehensions about my eternal life as a student, they have never wavered in their support. In everything I do they have supported me and it is without doubt I say that if it were not for this, I would not be where I am today.

Secondly, I would also like to express my deep appreciation towards my supervisor, Dr. Mo Adda, for his enthusiasm and guidance throughout my PhD. He has always been positive and supportive, even when things were not proceeding as planned.

I also wish to thank all my fellow university colleagues during these years, those who are still in the University of Portsmouth but also those who left. To start with I would like Mrs Amanda Peart for her never faltering willingness to help me understand the intricacies of university procedures, teaching and for her support during my research. A big thank to Penny Hart, for giving me the opportunity to work in the tutor centre and meet so many other great people. Also I would like to thank my ex-fellow PhD students Gareth, Mohammad, Antoniya, Vikas and Houda for the great times and support inside and outside of the university.

Least but not last, I would like to thank all my friends for their support and encouragement they provided and the enjoyment they brought to my life during all these years. Christos, Konstantinos, Panagiotis, Tania, Afroditi, Effie, Ria, Bill and all those whom I have missed out, thank you for every single second of your time.
Declaration

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

SIGNED: ______________________________
# Table of Contents

1 **Introduction** ........................................................................................................... 1

1.1 Background ............................................................................................................. 1

1.2 The 802.11 standard (WiFi) ................................................................................... 1

1.3 Types of 802.11 networks ....................................................................................... 3

1.3.1 Ad-hoc/independent networks ........................................................................... 4

1.3.2 Wireless Mesh Networks ................................................................................... 5

1.4 Motivation ............................................................................................................... 6

1.5 Contributions ......................................................................................................... 9

1.6 Thesis outline ....................................................................................................... 11

2 **Wireless Technology in Industry: An Overview** .............................................. 14

2.1 Introduction .......................................................................................................... 14

2.1.1 Wired versus wireless for industrial environment ............................................. 15

2.1.2 Characteristics of industrial environments ....................................................... 17

2.2 Challenges/problems in industrial environments ............................................... 19

2.2.1 Channel and Frequency ................................................................................... 19

2.2.2 Throughput and Capacity ................................................................................. 23

2.2.3 Scalability and availability ................................................................................ 23

2.2.4 Security ............................................................................................................. 24

2.3 Wireless technologies for industrial deployment ................................................. 25

2.3.1 Bluetooth Technology – IEEE 802.15.1 .......................................................... 25

2.3.2 IEEE 802.15.4 ................................................................................................. 27

2.3.3 IEEE 802.11 Standards ..................................................................................... 29

2.4 Wireless technologies comparison/discussion ..................................................... 30

2.5 Current and future approaches ............................................................................. 32

2.5.1 Current wired solutions .................................................................................... 32

2.6 Hybrid wired/wireless approaches ...................................................................... 34

2.6.1 Wireless Sensor Networks ............................................................................... 36

2.6.2 Fieldbus discussion ........................................................................................ 38

2.7 Conclusion ............................................................................................................ 39

3 **Multi-radio Network Routing & Channel Assignment Schemes** ............... 41

3.1 Background .......................................................................................................... 41
3.2 Wired routing protocol ........................................................................................................43
3.3 Wireless routing protocols .................................................................................................45
  3.3.1 Reactive routing protocols .........................................................................................46
  3.3.2 Proactive routing protocols .......................................................................................49
  3.3.3 Hybrid routing protocols ............................................................................................52
3.4 Multipath routing and mesh networks ..............................................................................54
  3.4.1 Split multipath routing – SMR ...................................................................................55
  3.4.2 Ad-hoc on demand multipath distance vector – AOMDV ........................................56
  3.4.3 Multipath source routing – MSR ..............................................................................57
  3.4.4 Comparison of multipath routing protocols .................................................................58
3.5 Channel assignment design strategies .............................................................................58
  3.5.1 Background of channel assignment problem ................................................................59
  3.5.2 Radio interference .....................................................................................................60
3.6 Taxonomy of existing channel assignments ........................................................................63
  3.6.1 Fixed channel assignment schemes ..........................................................................64
  3.6.2 Dynamic channel assignment schemes .....................................................................68
  3.6.3 Hybrid channel assignment schemes .........................................................................71
  3.6.4 Comparison of channel assignment schemes ..............................................................73
3.7 Conclusion .........................................................................................................................74

4 Reducing CCI Using Segregate Networks ......................................................................76
  4.1 Introduction ....................................................................................................................76
  4.2 Constraints of network segregation ...............................................................................77
    4.2.1 The problem of co-channel interference ..................................................................78
    4.2.2 Effectiveness of RTS/CTS in single channel networks ..............................................79
    4.2.3 Adjacent channel interference ................................................................................79
  4.3 Network segregation and its benefits ............................................................................86
    4.3.1 Mission and physical characteristics of the segregated network .........................86
    4.3.2 Operational characteristics of the segregated network ............................................87
    4.3.3 Features of network segregation .............................................................................89
  4.4 Implementation of segregate networks scenarios ..........................................................90
    4.4.1 Selection of the routing algorithm ..........................................................................91
    4.4.2 Network delay over network segregation .................................................................93
    4.4.3 GRID technology against network segregation .......................................................96
4.4.4 Network segregation in noisy environments................................. 103
4.5 Conclusion........................................................................................................ 109

5 Modulo Channel Assignment Algorithm ............................................. 111
  5.1 Introduction.................................................................................................. 111
  5.2 Modulo in multi-hop networks ................................................................. 113
    5.2.1 Operational characteristics of modulo .............................................. 113
    5.2.2 Modulo in chain topology ................................................................. 115
    5.2.3 Theoretical analysis of modulo ......................................................... 122
    5.2.4 Modulo and network segregation .................................................... 127
  5.3 Modulo in non-noisy segregate networks ................................................ 129
    5.3.1 Routing and channel assignment....................................................... 129
    5.3.2 End-to-end delay and modulo .......................................................... 133
  5.4 Modulo in noisy segregate networks ......................................................... 140
    5.4.1 Delay of segregated network over noise using modulo ...................... 141
    5.4.2 Network collisions in a noisy and heavy loaded network ..................... 144
    5.4.3 Nodes retransmissions for a noisy environment .................................. 147
    5.4.4 End-end-delay in a noisy and heavy loaded network .......................... 150
  5.5 Conclusion.................................................................................................... 152

6 Conclusions and Further Work .......................................................... 155
  6.1 Conclusions............................................................................................... 155
  6.2 Future Work............................................................................................... 156

7 Appendices .............................................................................................. 171
  7.1 Terminology and notation ...................................................................... 171
  7.2 Simulation environment .......................................................................... 172
    7.2.1 Introduction....................................................................................... 172
    7.2.2 Simulator ......................................................................................... 172
    7.2.3 Simulation parameters ...................................................................... 173
    7.2.4 Presentation of results...................................................................... 174
    7.2.5 GloMoSim 2.03 installation in Windows XP ....................................... 174
  7.3 Gateway nodes.......................................................................................... 175
  7.4 Graph theory ............................................................................................ 176
List of Figures

Figure 1.1. A simple ad-hoc wireless network ................................................................. 5
Figure 1.2. A Wireless Mesh Network (Ember 2002) ...................................................... 6
Figure 2.1. Co-channel interference between two nodes (Cisco, 2009) ......................... 21
Figure 2.2. The ISM spectrum for the IEEE802.11 standard (wndw, 2007) .................. 22
Figure 2.3. A scatternet containing 3 piconets ............................................................... 26
Figure 2.4. An IEEE 802.15.4 cluster tree (Blanco, 2007) ........................................... 28
Figure 2.5. The architecture of a Wireless Sensor Network. (Akyyildiz and
Sankarasubramaniam, 2002) ......................................................................................... 37
Figure 3.1. The four basic routing schemes ................................................................. 42
Figure 3.2. Route record creation for DSR ................................................................. 48
Figure 3.3. Example of ZRP routing with p = 2 .......................................................... 53
Figure 3.4. The representation of channel reuse in cellular networks ......................... 60
Figure 3.5. Representation of communication and interference ranges ....................... 61
Figure 3.6. Representation of channel dependency ..................................................... 63
Figure 3.7. Connectivity graph of CLICA (Marina and Das, 2005) ............................. 65
Figure 3.8. The two phases of MICA using Tabu search ............................................. 66
Figure 3.9. LLP in operation (Kyasamur and Vaidya, 2005a) ........................................ 72
Figure 4.1. Non overlapping channels of 802.11a (IEEE 802.11a, 2003) ..................... 82
Figure 4.2. Overlapping channels (IEEE 082.11b, 1999) ............................................. 83
Figure 4.3. A three segregated network utilising 3 channels ........................................ 88
Figure 4.4. Evaluation of various routing algorithms .................................................. 92
Figure 4.5. Average delay for various numbers of subnetworks .................................... 94
Figure 4.6. Assignment of channels in GRID. Number of channels n=9. In each grid the
top number is the channel number and the ones in the bottom are the grid coordinates. (Tseng et al., 2006) ................................................................. 97
Figure 4.7. The average end-to-end delay over number of nodes ................................. 98
Figure 4.8. The average delay of the networks for a variable number of nodes ............ 99
Figure 4.9. The average throughput of the networks for variable number of nodes .... 100
Figure 4.10. The average throughput of 4 the segregated network ............................... 101
Figure 4.11. Average Throughput of the GRID networks .......................................... 101
Figure 4.12. The delivery ratio of the networks for variable number of nodes .......... 102
Figure 5.19. The average delay in milliseconds of a 2 part segregated network utilizing two or more channels ................................................................. 138
Figure 5.20. The average delay in seconds of a 3 channel segregated network over noise increase ........................................................................... 141
Figure 5.21. The average delay in seconds of a 4 channel segregated network over noise increase ........................................................................... 142
Figure 5.22. The average delay in seconds of a 5 channel segregated network over noise increase ........................................................................... 143
Figure 5.23. Increase of collisions over noise for 3 channels per subnetwork .......... 144
Figure 5.24. Increase of collisions over noise for 4 channels per subnetwork .......... 145
Figure 5.25. Increase of collisions over noise for 5 channels per subnetwork .......... 146
Figure 5.26. Number of retransmissions using 3 channels per segregate network..... 148
Figure 5.27. Number of retransmissions using 4 channels per segregate network..... 149
Figure 5.28. Number of retransmissions using 5 channels per segregate network..... 149
Figure 5.29. The average delay in seconds of a 3 channel segregated network over noise increase ........................................................................... 150
Figure 5.30. The average delay in seconds of a 4 channel segregated network over noise increase ........................................................................... 151
Figure 5.31. The average delay in seconds of a 4 channel segregated network over noise increase ........................................................................... 152
Figure 7.1. Graph coloring of a multi-radio wireless network ............................... 177
Figure 7.2. Representations of different MR-WMNs .......................................... 179
List of Tables

Table 1.1. Comparison of 802.11 standards ................................................................. 3
Table 2.1. Comparison of the three main technologies ........................................... 30
Table 3.1. Comparison of four reactive protocols ..................................................... 49
Table 3.2. Comparison of four proactive protocols .................................................... 52
Table 3.3. Comparison of three hybrid protocols ....................................................... 54
Table 3.4. Comparison of three multipath protocols .................................................. 58
Table 3.5. Comparison of various channel assignment algorithms ......................... 74
Table 5.1. The parameters of the simulations ............................................................. 133
Table 5.2. The parameters of the simulations ............................................................. 140
<table>
<thead>
<tr>
<th><strong>Glossary of Terms</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACI</strong></td>
</tr>
<tr>
<td><strong>AODV</strong></td>
</tr>
<tr>
<td><strong>CAA</strong></td>
</tr>
<tr>
<td><strong>CCI</strong></td>
</tr>
<tr>
<td><strong>Delay</strong></td>
</tr>
<tr>
<td><strong>DSR</strong></td>
</tr>
<tr>
<td><strong>IEEE</strong></td>
</tr>
<tr>
<td><strong>Multi-hop</strong></td>
</tr>
<tr>
<td><strong>Multi-radio</strong></td>
</tr>
<tr>
<td><strong>Neighbour</strong></td>
</tr>
<tr>
<td><strong>Network Layer</strong></td>
</tr>
<tr>
<td><strong>Node</strong></td>
</tr>
<tr>
<td><strong>Routing</strong></td>
</tr>
<tr>
<td><strong>Segregate</strong></td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background

The communications, computer and consumer electronic industries are coming together rapidly, creating products and services that allow people to establish links and exchange data without using wires. No single device defines the field of wireless data communication and no single application solves the variety of problems inherent in connecting desktop, laptop and hand-held computers. Rather a class of solutions is evolving into what can only be called wireless data technologies.

Wireless communications is not new. The existence of electromagnetic waves that travel at the speed of light was predicted by James Clerk Maxwell in 1864. On the other hand, Heinrich Hertz proved Maxwell’s theory with the experiments in the middle of the 19th century, but the first person to send radio signals through the air is Guglielmo Marconi in 1895 with the use of a telegraphic device that coded information into series of marks and spaces (Muller, 1995). The first wireless communications were between ships and the shore and then there is the appearance of radio broadcast which ended up being the dominant means of publishing news and entertainment. During those years, radio technologies advanced rapidly and included many other applications in the areas of national defence and public safety, as well as business and industry.

There are now two primary types of wireless communications, the wireless wide area networks called WANs and wireless local-area networks called WLANs both having a parallel role in the world of networks. This thesis focuses solely on the WLAN technology, stating the problems that arise during their operation, and at the same time presents possible solutions to overcome them.

1.2 The 802.11 standard (WiFi)

The wireless LAN can be characterized as being privately owned. As such, there are no costs associated with the usage. The geographic usage is small, measured in hundreds
of feet. It has been in widespread deployment for several years and the first IEEE 802.11 standard was introduced in 1997 (IEEE 802.11, 1997). The main reason for developing this standard was to provide interoperability in two dimensions (Kwok and Lau, 2007):

- **Interoperability between wireless LANs and existing wired LANs such as IEEE 802.3 Ethernet.**
- **Interoperability between wireless devices from different hardware manufacturers.**

Before the implementation of the IEEE 802.11 standard different hardware manufacturers developed their own wireless LAN products based on their ideas, and this lead to a serious problem of interoperability and incompatibility between wireless devices from different manufacturers. In order to facilitate the interoperability and normal deployment of wireless networks using devices from various manufacturers, the IEEE 802.11 working group has been set up to provide generally acceptable standards and specifications on Medium Access Control (MAC) mechanisms and Physical (PHY) links for wireless devices in order to share the wireless medium in a fair manner.

In view of the demand for different performance requirements from the wireless LANs, different groups have been developed such as A, B, G and E. The standard provided by Group A is 802.11a, which can provide theoretical capacity up to 54Mbps with 24 orthogonal channels and operates in the frequency of 5GHz unlicensed band – Unlicensed National Information Infrastructure (UNII) (IEEE 802.11a, 1999). This is a tempting capacity compared to wired networks.

On the other hand the 802.11 and 802.11b (IEEE802.11b, 1999) standards were designed to operate in the 2.4GHz, Industrial Scientific Medical (ISM) band. The 802.11 standard specifies operation with raw data rates of 1 or 2Mbps. The 802.11b standard (a modification to the original 802.11 Physical layer specifications) raises the bar to include 5.5 and 11 Mbps/Sec.
Table 1.1. Comparison of 802.11 standards.

<table>
<thead>
<tr>
<th></th>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio frequency</td>
<td>5GHz</td>
<td>2.4GHz</td>
<td>2.4GHz</td>
</tr>
<tr>
<td>Channels</td>
<td>8 overlapping</td>
<td>3 non-overlapping</td>
<td>3 non-overlapping</td>
</tr>
<tr>
<td>Maximum data rate</td>
<td>54Mbps</td>
<td>11Mbps</td>
<td>54Mbps (108Mbps)</td>
</tr>
<tr>
<td>Indoor range</td>
<td>Fair</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Wall penetration</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Radio interference</td>
<td>Not Likely</td>
<td>Probable</td>
<td>Probable</td>
</tr>
<tr>
<td>Compatible with</td>
<td>802.11g</td>
<td>802.11g</td>
<td>802.11b</td>
</tr>
</tbody>
</table>

Mobility is considered to be one of the most important gains for wireless communications. Using the wireless medium in order to connect to a network provides the users with great convenience as users can easily move with their wireless devices without the consideration of the limitation and location of the corresponding wired access point.

While replacing the wires is certainly an attractive feature of wireless LAN technologies, they pose legitimate security concerns. Since the signals travel through the air, they can be intercepted more easily by network intruders and unauthorized users. Security related concerns can be alleviated up to a certain point by the appropriate selection of wireless technology and to a greater extend by adding encryption. Encryption offers virtually infallible security and it can be implemented at each node or at the central control unit which is available from almost every wireless LAN vendor. Depending on the vendor, more than one encryption algorithm can be supported at the same time.

### 1.3 Types of 802.11 networks

The basic building block of an 802.11 network is the basic service set (BSS), which is simply a group of stations that communicate with each other. Communications take place within a fuzzy area, called the basic service area, defined by the propagation characteristics of the wireless medium. When a station is in the basic service area, it can communicate with the other members of the BSS. BSSs come in two forms.
Defining their basic components, the stations are coming first. These are devices that implement the standard IEEE 802.11 Media Access Control (MAC) and Physical (PHY) functionalities. On the other hand, there are the access points (AP), devices that provide an interface for other associated wireless stations to access a BSS. The last component is the Distribution System which connects multiple Basic Service Sets and/or integrates with other networking technologies. There are two types of networks based on the 802.11 standard, the infrastructure and the independent or ad-hoc networks. Since infrastructure wireless networks are not part of the research of this thesis, there will be a description only on ad-hoc networks.

1.3.1 Ad-hoc/independent networks

The type of a wireless network this thesis is focusing on is the independent basic service set (IBSS) showing in Figure 1.1. Stations in an IBSS communicate directly with each other and thus must be within direct communication range. The smallest possible 802.11 network is an IBSS with just two nodes. Usually IBSSs are composed of a small number of nodes set up for a specific purpose and for a short period of time. In order to set up an IBSS the nodes have to be configured into a ad-hoc mode and thus instead of IBSS these type of networks are called ad-hoc wireless networks. Ad-hoc mode allows users to spontaneously form a wireless LAN. For example, a group of people with 802.11-equipped laptops may gather for a business meeting at their corporate headquarters. In order to share documents such as presentation charts and spreadsheets, they could easily switch their laptops to ad hoc mode to form a small wireless LAN within their meeting room. The ad hoc form of communications is especially useful in public-safety and search-and-rescue applications. Medical teams require fast, effective communications when they rush to a disaster to treat victims.
In Figure 1.1, node A wants to communicate with node B. The problem is that node A is out of the range of node B so the direct communication between them is impossible but also there is no access point to relay transmissions. When these nodes are configured to operate in ad-hoc mode, data will travel through other nodes until it reaches the destination, being node B. The process to follow is that node A will start asking how it can reach node B and which path the data has to follow. The role of this procedure falls on the routing protocol that will set up a route and inform node A which is the next hop to receive the data. Then node A starts relaying data through its neighbours and consecutively they will relay the data to another node as the protocol specifies it. As long as nodes are fixed and relatively small in numbers, it is an easy and straightforward operation. When the number of devices grows performance suffers in relation to network throughput, delay and reliability. Especially when within the network there are a many mobile nodes, it has been identified (Schindelhauer, 2006) that the network’s management and performance become a difficult task. With the introduction of ad-hoc technology into wireless networks, numerous and time consuming researches from many scientists in the world (Thoppian and Prakash, 2006), attempted to overcome the problems that appeared in a multi-hopping environment.

1.3.2 Wireless Mesh Networks

As mentioned before the nodes inside an ad-hoc network can either be mobile or static and the differences between these two categories are greatly related to complexity and
performance. In the case of static nodes operating in ad-hoc mode there is a new type of network called the wireless mesh network (WMN). A WMN, as shown in Figure 1.2, is a communication network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh routers themselves may be static or have limited mobility. Wireless mesh networks are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity.

![Figure 1.2. A Wireless Mesh Network (Ember 2002)](image)

WMNs are undergoing rapid commercialization in many other application scenarios such as broadband home networking, community networking, building automation, high-speed metropolitan area networks, and enterprise networking. The basic initiative behind these is that WMN can offer cheap and high speed interconnections (Akyildiz et al., 2004) between various points of interest over large distances combining many existing wireless technologies such as Wi-Fi, the Internet, cellular and sensor networks.

### 1.4 Motivation

Nowadays wireless LANs are mainly used in environments like home and office/small businesses networks. During the last three years (BT, 2008) there is a wide spread of wireless LANs from users who are not computer oriented and this happens because the offered hardware from different vendors have been standardized and there is not
different configuration procedures for each vendor. Apart from that there are new security algorithms appearing and are embedded into any new hardware products coming from the production line. These make the user to feel more confident when deploying a wireless LAN within a house or a business environment. Also, the majority of the ISPs (Virgin Media, 2009) now offer wireless solutions such as wireless routers/modems and wireless broadband enabling the consumers to enjoy the benefits of wireless communications.

Whereas in a home or office deployment the bandwidth requirements are not very high and can be assured by current available technologies, the same does not happen for large enterprise developments. In such cases the bandwidth, the reliability and the cost parameters often restricts the use of wireless communications. There is a competition going on between wired and wireless networks within industrial environments. Many companies (Ember 2005) are setting as target the replacement of their wired network with a wireless one in an effort to reduce mainly costs but maintaining the reliability and good performance of a wired link.

In an industrial or factory floor setting, the benefits of using wireless technologies are manifold. First of all, the cost and time needed for the installation and maintenance of the large number of cables normally required in such an environment can be substantially reduced, thus making plant setup and reconfiguration easier. This is especially important in harsh environments where chemicals, vibrations, or moving parts exist that could potentially damage any sort of cabling. In terms of plant flexibility, stationary systems can be wirelessly coupled to any mobile subsystems or mobile robots that may exist in order to achieve a connectivity that would otherwise be impossible.

At the beginning of this research, an organization expressed its interest on the idea of enabling enterprises to replace their current wired infrastructure with a wireless multi-hop network. The interest was from a research centre in Culham, Oxford called JET, the Joint European Torus (EFDA, 2009), which performs experiments on nuclear fusion. The centre maintains a fully equipped environment with machinery and sensors able to perform tests on fusion, for the production of electricity. The experiments do not follow a
standard pattern so from time to time they test various equipments and techniques depending on the nature of the experiment. This requires the installation of extra hardware and sensors in order to monitor every activity that takes place during their testing. Currently the monitoring and the data collection is performed with the help of a wired network extending from the main testing area, the core, up to the data centre where the data is stored for further analysis.

The area where the experiments are performed holds these characteristics of an industrial environment with metal constructions, thick walls able to protect the external area and the employees from radiation and high magnetic fields. Any network installation that takes place within this area is considered industrial and the cost for these is quite high according to the company. As mentioned in the previous paragraph, very often, new sensors and equipment are installed for data collection and consequently new wires are fitted connecting them to the current network. Once the experiments are finished, the newly installed hardware might be considered useless and is usually removed. The same doesn’t always happen with the wires. Any attempt to remove the cabling would increase further the cost and thus it is left as it is.

The implementation of a wireless network would solve the cabling problem but would also increase the flexibility during the experiment’s design phase by requiring less time. The question that appears in that case is if a wireless network can actually operate in harsh environment. The metal constructions, the existence of electrical equipment transmitting electrical and electromagnetic noise, vibration and also the periodic appearance of radiation, in the form of charged atomic nuclei entering a plasma state, could set the use of wireless networks prohibitive.

Considering the above scenario only as a starting point, the main motivation of this work is to investigate the possibility that a wireless network will be able to survive inside a noisy industrial environments and be able to compete against a wired network offering a fast, reliable and cheap solution to any interested company. Since we are interested in a wireless mesh network deployed in a harsh environment there are numerous challenges appearing but this work will focus on achieving fast and reliable data transfers within the industrial area by using an efficient routing protocol embedded with
a channel allocation algorithm able to ensure reduction of interference from adjacent nodes and other sources.

1.5 Contributions

This research makes a number of contributions to the use of wireless communications inside harsh industrial environments setting a comparison frame for these industries trying to replace their wired infrastructures with wireless ones. We examine the performance of wireless networks using a single channel compared to multichannel and multihop WMN. Although multichannel solutions are a way to overcome interference from neighbouring nodes and other sources may pose other problems making their deployment a big issue.

The main contribution of this thesis is that it tries to reduce the complexity that current solutions include to their design and implementation stages. The famous Italian artist Bruno Munari quoted, “Progress means simplifying, not complicating” and this is the axiom that describes our proposed approach. During the next chapters, a number of proposed solutions are presented and although they seem promising, when it comes to real life, they are difficult to be implemented for commercial use. Apart from the proposed research ideas, there are many already implemented solutions that enable the adaptation of wireless networks in harsh industrial environments. All these solutions are based on proprietary hardware developed for particular purposes and needs. Deployment of these solutions can be made only by a limited number of companies who happen to be their designers and developers. Following the steps of the IEEE 802.11 which came to establish a standard to the use of wireless, this research tries to avoid complexity, using common commercial hardware, easy to be installed and deployed by people with some knowledge on wireless technologies. Generally companies try to avoid proprietary hardware in order to reduce maintenance costs and in cases of malfunction it can easily be encountered from the company’s existing technical support staff.

Another contribution of this work is that it tries to prove its advantages over existing single channel wireless networks, by proposing a multichannel approach that enables
each node inside a network to utilize more than one channel. Although many of these benefits of multichannel deployments have already been proved, as discussed in the following chapters, it is the first step to ensure the advantage of our approach against single channel operations. In our work, the benefits of a multichannel architecture are proved through simulations of various scenarios considering variable environmental conditions and network sizes. Examining the results from the simulations when each node operates with at least two or more channels, the gains regarding network's average delay and reliability should not be underestimated.

The next contribution is the examination of wireless network segregation for fixed wireless nodes. Network segregation is the division of the network into smaller subnetworks isolating the operation of each one from the rest. This is a first step in order to reduce the interference from adjacent nodes. Inside a single channel network all the nodes operate using a common channel. Consequently, the power each node emits affects all its neighbours which are within its transmission range. In our case instead of utilizing a single channel, the network is segregated into smaller networks and each one is using a different frequency than the rest resulting in fewer nodes using the same frequency and thus reducing adjacent interference. Instead for instance of having a uniform network with 90 nodes using a single common channel, the network is divided into two and up to five subnetworks with 18 or more nodes placed within. Since smaller number of nodes operates in the same frequency their transmission power can be increased to achieve better connectivity with each other and thus achieving better coverage of the area.

Examining all the available routing protocols available for use inside an ad-hoc wireless network a single protocol proves its reliability and suitability for the proposed approach. Focus is given on the routing protocol as it facilitates the multichannel functionality and the channel allocation algorithm designed to take the channel assignment decisions as data is relayed from node to another. Ad-hoc On Demand Vector routing, AODV (Perkins and Royer, 1999), is adapted for the proposed network architecture taking advantage of all the benefits this architecture provides. AODV is now able to transmit through multiple routes adapting to the segregate network concept.
Another contribution of this work is the channel allocation algorithm designed and implemented for multichannel and multi-hop networks called modulo. Modulo is a distributed algorithm which defines the decisions that each node has to take once a path is being established and data is transmitted through this path. Modulo is able to minimize adjacent interference from neighbouring nodes that operate on the same channel frequency. It is also able to eliminate the hidden terminal and exposed terminal problems as even nodes using the same range of frequency channels can transmit simultaneously. At the same time it increases the throughput and minimize the average delay within the network. Reliability is also improved as there are fewer collisions taking place inside the network.

Chapter 2, focuses is on wireless systems used for data acquisition from sensors, monitoring and machinery control. These sensors and controllers are wireless nodes that exchange data and commands between them and a control room. The traffic produced from such operations is relatively small when compared to scenarios examined in our approach. There is limited research on wireless networks able to achieve low delay, high throughput and increased reliability inside a noisy environment by overtaking the role of a wired backbone and this research mainly focuses on the physical and link layers. Our work tries to enhance this research area by examining and identifying the problems that appear during the deployment of such networks on the network layer.

To enable an analysis of such an algorithm several simulations were developed in order to provide a critical investigation by comparing other approaches in terms of their complexity and functionality. Finally a general framework, network architecture and a channel assignment algorithm are proposed to the use of the 802.11 standard inside a noisy and harsh industrial environment.

1.6 Thesis outline

Chapter 2 investigates the role of wireless in industrial environments, the problems that appear during their deployment and also the current wireless technologies and implementations. More specifically the problems of interference appearing in such
areas and the effects they have on wireless signals are discussed and analyzed. The three main wireless technologies presently used are introduced and evaluated by pointing out their main advantages and disadvantages.

Chapter 3 discusses two main characteristics of wireless networks. Firstly, there is an approach to routing protocols implemented for usage inside an ad-hoc environment. The challenges, the problems and the limitations that routing faces for ad-hoc networks are discussed and at the same time a comparison is performed between the most common algorithms. Since the number of available routing protocols and proposals is quite large, they are categorized following certain criteria trying to focus on issues regarding route set up, failure recovery and performance. The second part of Chapter 3 includes an introduction to the issues related to channel allocation algorithms within multichannel ad-hoc networks related to wireless routing. The transition from single channel networks to multichannel ad-hoc networks has solved many problems such as the hidden terminal problem, but new challenges and problems have appeared. Many researchers have proposed a variety of schemes trying to encounter them and these are critically evaluated and categorized based on their approach techniques and the complexity they add to the 802.11 standard.

Chapter 4 presents the methodology that was followed by our approach. This starts by an introduction to the network segregation technique by investigating the benefits and the drawbacks it can have on a wireless network performance. Network segregation is considered as a technique that makes network management and deployment easier. Apart from that it hides problems such as loss of communication between the wireless nodes and they appear during the network’s operation, so we define the parameters that have to be followed when dividing a WLAN into subnetworks. Although having a single channel network might look easier and more flexible, network segregation is the first step to reduce interference from neighbouring nodes. Our approach indicates that moving to a multichannel environment might partially solve the co-channel interference problems the channel allocation decisions for the network’s nodes becomes the main drawback.
Chapter 5 focuses on the channel assignment algorithm proposed in this work. Initially the deployment of modulo technology into a chain topology is examined, showing the benefits that this approach offers on network capacity and delay. Setting this as the starting point for further development, the next step relates to a combination of modulo with a segregate network, while is compared to uniform multichannel networks but also to location aware channel allocation algorithms. Modulo technology demonstrates its advantages and limitations dependent on the number of channels that are utilized inside the network. While in the previous chapter, it was shown how network segregation reduces the impact of co-channel interference, in this chapter modulo is introduced against adjacent node interference and noise produced by other sources. The results show the gains achieved according to the network performance, delay and throughput, network reliability such as collisions and retransmissions by simulating a wide range of scenarios.

Finally Chapter 6 provides a summary of the key findings of the research work carried out its limitations and how these could be overcome through further investigation including future that could be performed on the proposed idea.
2 Wireless Technology in Industry: An Overview

2.1 Introduction

Wireless networking applications continue to flourish at an incredible pace as wireless features, functions, security, and throughput improve. 802.11 is the standard on which wireless networking operates today, and products that employ the technology support a broad range of uses for enterprises and home users. The benefits of Ethernet as a high speed, low cost, open, common transport medium have led to increasing rates of adoption for industrial applications. The use of wireless technologies and especially the Ethernet physical medium, increases industrial Ethernet connectivity and flexibility, often with substantial upfront and lifetime cost savings. Wireless Ethernet technologies have advanced in a similar manner to their cable and fiber tethered counterparts, and wireless is now a practical option in the factory.

Before moving any further the question which has to be asked first is whether wireless can be used inside an industrial facility. Looking through the Internet and performing a simple search engine with the keywords wireless, industrial, Ethernet and networks will come up with numerous results, almost 400.000, of web pages which have to do with the use of wireless networks in industrial environments. So the answer to the question is yes, it has been tested and it works thus there is a vast number of vendors who design and implement their hardware specifically for industrial facilities.

The next answer that comes up is which of the many wireless technologies is suitable for industrial Ethernet. The answer depends to a great deal on the application environment, throughput and latency requirements, distance between nodes, and the local wireless regulatory situation. Proper wireless industrial Ethernet network planning and installation is the key to satisfactory performance. All these technologies are discussed later in this chapter. There will be a relatively brief review of them pointing out the main characteristics, the advantages and disadvantages of each one, how they
satisfy the criteria of a harsh environment and also why they cannot be directly compared to the work of this thesis.

2.1.1 Wired versus wireless for industrial environment

The operation of nearly every factory and industrial setting depends on vital data flow between machinery, control, and monitoring devices. Throughout the range of applications, from periodic status updates to continuous process control, the most important aspect of any communication system is timely delivery without failure. The Ethernet networking standard has understandably gained popularity in industry; Ethernet delivers high performance at reasonable cost, accommodates a wide range of uses, and is almost universally supported.

But for all of its advantages, wired Ethernet shares the shortcomings of all cabled connections: necessary tethering equipment and limiting placement options. Distance between nodes is also an obstacle, as cable length limits are quickly exceeded in many industrial settings. And, new cable runs, moves, or upgrades easily disrupt plant operation. To avoid cabling shortcomings, industrial end users and systems integrators are turning to wireless Ethernet technologies. The key to a successful transition lies in selecting a wireless implementation that retains the benefits of Ethernet without adding new headaches.

In a harsh industrial environment, most cable runs have to be in conduit, and redundant runs were required in critical operations. On top of that, all wiring had to be installed by a licensed plant electrician. Knowing that the average cost of industrial wiring is about $200/foot (Frenzel, 2004), someone has to wonder how many industrial networking projects or systems are delayed or never implemented because of the significant cost of laying the cables (think backhoe or conduit) coupled with the related complexity. Another serious problem for wire installation in industrial environments comes actually after the fitting of the cable. In many cases, especially for companies who conduct many experiments require the frequent installation of new sensors, depending on the type of experiment, for just a limited period of time. After that time this cable is often considered useless for a number of reasons such as length, quality or location. During
the installation in order to make sure there will be no malfunction to the cable, it is being installed in a permanent way. This way the cable is not possible to be removed even if considered not useful as it would require extra time and cost similar to its installation.

On the other hand wireless technology the main advantages of wireless networks are:

- **Lowers the cost of wiring**: Wireless networks negate the cost of the wire previously needed to connect devices and controllers. Wireless solutions allow networks to be established over distances or in applications where the price of cable might have been prohibitive. Since the medium for wireless transmissions is the air, there is no limit to the space that can be covered for transmission but also none will charge you for using the air for data transmissions as long as one of the Industrial Scientific and Medical ISM bands is used (ITU, 2007). The (ISM) radio bands are reserved internationally for the use of RF electromagnetic fields for industrial, scientific and medical purposes other than communications (ITU – 2004).

- **Lower cost components**: Extensive and growing use of wireless Ethernet or Wi-Fi in high-volume commercial and consumer markets is leading to inexpensive components compared to those of other wireless networks. To connect, for example, wirelessly three devices we will just need 3 wireless NICs enabled in ad hoc mode, whereas a wired interconnection would need 3 NICs, couple meters of cables and a hub/switch/router. In the case where multiple sensors are scattered around a very large area for monitoring and command control and they were connected by wire, the use of hubs and/or switches would be necessary. On the other hand if the sensors featured wireless connectivity, then data would be relayed from one wireless ad-hoc node to the other eliminating the need for extra hardware and saving couple hundreds or even thousands of pounds.

- **Fast installation, maintenance and expansion**: Another benefit of wireless is the speed of deployment. Wired systems can take days or weeks to be properly installed, isolated and commissioned. Wireless networks require only the end
points to be installed, saving hours or days for each instrument installed. Other instruments can be added as required without the need for expensive, disruptive cabling and labour. A further benefit is the ease of reconfiguration and expansion. If there is need for a plant expansion, or relocation of sensors, there is no expensive conduit to be moved or added.

- **More flexibility through mobility:** During the recent years wireless networks are improving in an aspect which is considered one of the most important and attracts many new users and this is mobility. The users are able to move from one area to another and at the same time to keep their wireless connection alive.

Until recently wired networks were considered irreplaceable in the industrial areas because of the problems that appeared in the wireless operations. The progress achieved in wireless networks since their first appearance made the use of wireless networks possible within harsh industrial environments

### 2.1.2 Characteristics of industrial environments

Industrial environments are uniquely different from office and home environments. High temperatures, excessive airborne particulates, multiple obstacles and long distances separating equipment and systems, are special challenges that make it difficult to place and reach sensors, transmitters, and other data communication devices. The physical size of an industrial area requiring coverage is often large enough like hundreds or even thousands of square feet, and within those buildings are even more physical challenges. The large volume of metal typically found in the construction of the building as well as within the environment, such as large vessels, piping and machinery can cause problems to the RF signals — as can equipment that emits electromagnetic noise, such as large motors. The presence of multiple fixtures and equipment can create RF ‘blind spots. Industry regulations can also add significantly to the installation cost, since, for example, some wiring may need to be run through metal conduit and finally, hazardous and/or explosive materials found in many industrial environments add yet another level of complexity (Motorola – 2007).
The list can go on and on in order to be able to illustrate in depth all the available features of industrial areas and how they possibly affect the performance of wireless links. As this would require too much time effort, this work is making a reference to these problems presenting a list of all possible characteristics that could be present inside a harsh environment. It should be noted that the harshness of an environment depends on many factors and is considered a variable state. It is difficult but not impossible to find all the factors present at the same time in the same area. Nowadays there is a large diversity in the industrial areas where wireless networks are deployed and operated and these are factories, process control plants, warehouses, oil and gas pipelines, building controls, hospitals, trucks and automobiles, public utilities, and city facilities like lighting and traffic control (Frenzel, 2004).

To sum up the harshness factors are presented below although the list cannot and should not be limited only to these (Taylor, 2004).

- Dust and other airborne contaminants;
- Exposure to chemicals, grease, oil, etc.;
- Exposure to corrosive materials;
- Exposure to explosive atmospheres;
- Exposure to ultraviolet radiation;
- High humidity levels;
- High levels of EMI/RFI interference;
- High levels of shock/impact;
- High levels of vibration;
- Immersion in liquids;
- Power source voltage surges, and other transients;
- Splashing by liquids;
- Wide temperature ranges; and
- Wide voltage deviations of power sources.
Running wireless applications inside a harsh environment can be significantly challenging as there are some certain requirements and problems that have to overcome. These are presented and analyzed in the following paragraphs of this Chapter.

2.2 Challenges/problems in industrial environments

Achieving success in the challenging industrial environment is dependent upon understanding the unique requirements, and how these requirements translate into criteria for the selection of the most crucial aspect of any mobility solution — the wireless infrastructure. The selection of the right infrastructure will ensure the performance and the functionality needed in today’s industrial applications, will also make sure that the network can grow adapting to the changing and growing needs of the industry. At the same time it reduces the risk of failures and which can lead to terrible results and loss of important data which is collected either from experimental equipment or from sensors that ensure the safe and reliable operations of the industry. The general cost to design and deploy a wireless network within such an environment is costly.

2.2.1 Channel and Frequency

Since in wireless networks the medium for transmissions is the air and data is sent from one node to the other in the form of electromagnetic waves, frequency and channels are mainly affected. The problems that appear are numerous and influence the network’s performance in many ways as studied by researchers (Willig et al., 2002) and (Downey, 2007) below are presented the most common setbacks found in a wireless environment.

- **Path Loss**: The signal strength of a radio signal decreases with the distance between a transmitter and a receiver. This decrease is known as path loss. The magnitude of the path loss depends on several parameters, including the antenna technology, the frequencies used, and the environmental conditions that are present. An often-used approximation (Rappaport, 2002) of path loss is the log-distance model.
\[ P_r(d) \sim P_t \cdot \left( \frac{d_0}{d} \right)^\gamma \]  

(1)

In this model, the received signal strength \( P_r \) for distances \( d \) larger than a reference distance \( d_0 \) and a radiated signal strength \( P_t \) behaves as shown in equation 1 and also \( d_0 \) depends on the antenna technology. The reference distance depends on the antenna technology. The so-called \textit{path-loss exponent} \( \gamma \) typically assumes values between two (free-space path loss) and six depending on the environment. In factory environments, path loss exponents between two and three have been observed (Rappaport, 1989-a) but sometimes values smaller than two can occur (Rappaport, 1989-b) as well.

- **Half-duplex operation of transceivers**: Wireless transceivers are not able to transmit and receive simultaneously on the same channel because their own signals would drown all signals from any other stations. Because of this fact, most wireless transceivers are half-duplex. They inhibit simultaneous transmit and receive operations while allowing the same circuitry to be shared, thus reducing the transceiver complexity. The primary disadvantage of this approach is the time losses experienced from explicit receive-transmit turnovers.

- **Multipath**: Typical open radio frequencies (900 MHz and 2.4 GHz) used within today’s wireless data communication applications have a reasonable penetration rate through office cubicles, drywall, wood and other materials found in a home or office, but tend to bounce off larger objects, metals, and concrete. This bounce can redirect the data signal and return it to the original transmitter, causing an echo also called multi-path. First generation wireless systems easily became confused with this type of interference and would cancel transmission all together. The result was a state referred to as “radio null” and prevented data communication.

- **Co-channel Interference**: Ad-hoc wireless networks can operate into two different configurations depending on the use of frequency channels. The first configuration is where all the nodes that are transmitting and receiving radio
signals operate on the same/identical channel. In this case neighboring nodes which are in the transmission range of a particular node will create problems to its transmissions with the form of interference and more specifically co-channel interference (CCI) or otherwise crosstalk. As shown in Figure 2.1, the volume of the interference depends on the distance between the pair of the nodes exchanging data and the other co-channel nodes that happen to be within their transmission range. CCI is mainly met in WLANs operating in infrastructure mode. The level of the interference is significantly related to the number of nodes that operate in the same frequency and specifically more the nodes higher the volume of the CCI is in the area and this phenomenon is not limited only to WLANs but has been proved to exist any type of wireless communications such as in satellite communications (Singh et al., 2005) and cellular networks (Chhabra et al., 2005) as shown by experimental results. The most common and easier measure to reduce CCI is by decreasing the power of the transmitters $P_t$ or the use of more frequencies by dividing the area into cells as performed in cellular networks (Scourias, 1997).

![Figure 2.1. Co-channel interference between two nodes (Cisco, 2009)](image)

- **Adjacent channel interference**: As mentioned in CCI, a wireless network might operate under a different configuration where the wireless nodes operate in different frequency spaces. It means that the whole frequency spectrum is
divided into smaller spaces and each of these spaces is utilized from various nodes. For example in the 802.11b/g (IEEE802.11, 2007) standards, the ISM band of 2.4GHz frequency with range from 2.401GHz up to 2.495GHz, is divided into 13 spaces for use in Europe and 11 for use in American Continent. These spaces are called channels with 22MHz bandwidth whereas the center frequency separation is set to 5MHz. This results in having only 3 non-overlapping channels for use in Europe, channels 1, 6, 12. The phenomenon of overlapping channels creates the problem of adjacent channel interference (ACI), from neighbouring channels because of their increased width as seen in Figure 2.2. Generally ACI is the result of inadequate filtering from the lack of a “brick wall” filter that keeps the spectrum in any channel limited to that channel. The energy in the overlapping regions between the channels and which corresponds to adjacent channels will cause interference. When for example a node operates in channel 3, sources of ACI are considered nodes that operate in channels 1, 2, 4, 5. Usually in most cases it is sufficient to take under consideration only the interference coming from the two channels on either side of the used channel. ACI is one of several components that make up the total noise and interference observed by a receiver. ACI may degrade the received signal quality of a modulated signal (Potman et al., 2006), which may then adversely impact performance. Various techniques may be used to mitigate the deleterious effects of ACI. These techniques may improve performance when ACI is present but may actually degrade performance when ACI is not present (Renk et al., 2006).

![Figure 2.2. The ISM spectrum for the IEEE802.11 standard (wndw, 2007)](image)

- **Third party noise**: The electromagnetic emissions created by large motors, heavy equipment, high power generation and usage, and other typical industrial
machinery could create extremely high levels of “noise” that interfered with early wireless equipment. In these “noisy” environments, transmitters and remote nodes may be unable to “hear” each other, resulting in frequent data loss.

2.2.2 Throughput and Capacity

Throughput, the amount of data transferred per unit time, and latency, the time between transmission and reception, are generally counterparts. Throughput is highly dependable on the quality of the wireless links during the transmissions. It has been proved (Gummadi et al, 2007) that interference can severely influence the reliability of a wireless link and consequently degrade the network’s performance. In addition, adjustable throughput and latency settings are also important to allow system fine-tuning to specific requirements. On the other hand in ad-hoc wireless networks where multi-hopping capabilities are activated using a single channel, it has been investigated (Kumar and Gupta, 2000) that while data is relaying from node to node there is a scale down to the capacity and at the same time there is a noticeable increase of the delay throughout the network. The same has been proven (Li et al, 2003) also for multichannel networks but in this case the degradation is smaller compare to the single channel counterparts. Higher throughput (in longer packets) may mean decreased overhead, but it comes at the cost of higher latency and overall network delays. For best industrial results overall, data throughput needs to match application requirements closely, as overestimating or "over providing" speed has trade offs, most notably, decreased effective range.

2.2.3 Scalability and availability

Network configurations seldom remain static for long — in fact, they only grow. In the case of WLANs, growth occurs for reasons of both coverage (providing basic radio service in a given area) and capacity (providing the performance users really need to be productive). It’s also worth mentioning here that the ongoing evolution of the 802.11 standard may dictate growth as well — capacity can be added via radios compatible not only with 802.11b, but also the faster 802.11a and 802.11g. This means that a successful WLAN architecture must allow users to plan for growth and change without
knowing exactly what growth and change will be required. Scalability also means flexibility. It’s critical for an enterprise-class implementation to place as few limitations on users and network managers. Deployments, both primary and successive, must be accomplished with minimal disruption to the existing infrastructure, WLAN devices can be easily interconnected over an existing Ethernet infrastructure, minimizing the cost to install and deploy and making the best use of the current physical plant. Finally, scalability must allow investment protection and lower total cost of ownership. Growth must be smooth and non-disruptive and additional coverage and capacity must be straightforwardly integrated to current network’s capabilities.

At any given time the network should also be able to ensure the availability of resources in case new nodes/clients enter the network but also in case of failures. Wireless networks are prone to failures and these should be encountered immediately and without the least disruption in their operation. Industrial WLAN architectures must be self-discovering, self-configuring and self-healing according to policies set by the network administrator. Should a node fail, nearby nodes should automatically be re-configured to pick up the load regardless their location. It should be noted that in such cases, infrastructure architectures are difficult to provide the required flexibility and availability as once an access point goes offline. Every node that is out of the range of the rest access points will not be able to join again the network. Such a behavior is not permitted inside an industrial environment. The data that is flowing through the nodes are very important for the company’s operation and any possible loss of data would have disastrous results to the network and the general safety.

2.2.4 Security

Early adoption of the IEEE 802.11 standards created a large number of security issues and continues to require a high level of counter-measures to ensure the safety of data and business systems. Security plays a big part in ensuring reliability. The network must be protected from unauthorized users who could initiate attacks that can lead to downtime, the introduction of erroneous information or the theft of company data. To achieve a level of security on the wireless system equal to that of the wired LAN, the wireless system should offer a comprehensive portfolio of security features that can be
layered as needed to achieve the right level of security for different applications. The basic parameters that can ensure the security of a wireless LAN are the access control, the data protection and monitoring. Access control can be achieved through authentication techniques that guarantee only certified users to access the network. There should be tiers of access and each employee would be categorized according to his position in the company and by logging in the network would allow him/her to have access only to particular resources.

Wireless LANs are considered prone to data theft and other malicious acts as data is being sent through the air from node to node and the only option is to encrypt it during transmission. There are numerous technologies and protocols that enable data encryption and each one has its advantages and disadvantages (Beck and Tews, 2008).

**2.3 Wireless technologies for industrial deployment.**

For the various reasons listed at the beginning of the introduction, wireless technologies might be of advantage in industrial environments. Due to the general tendency towards standardization and the fact that cheap, commercial wireless technologies are available, it seems only logical to investigate these for their suitability in industrial deployment. Of particular interest for industrial environments are technologies that do not require any sort of frequency licensing. These technologies include the wireless personal area network (WPAN) technologies such as IEEE 802.15.1/Bluetooth and IEEE 802.15.4/ZigBee as well as the wireless local area network (WLAN) technologies from the IEEE 802.11 family.

**2.3.1 Bluetooth Technology – IEEE 802.15.1**

Bluetooth (BT) was originally designed as a cable replacement technology (Sturman and Bray, 2000) aimed at providing unproblematic wireless connectivity (Haartsen, 1998) for consumer devices in an ad-hoc mode (Bisdikian, 2001). In order to allow for deployment almost worldwide, the BT Special Interest Group (SIG) placed the
technology in the unlicensed ISM-band at 2.4 GHz. By designing a comparably straightforward system, the designers of BT intended for it to have widespread use.

As shown in figure 2.3, Bluetooth networks are organized into piconets in which a master node coordinates the traffic to and from up to seven active slave nodes. The master node originates the request for a connection setup. Within a single piconet, the various slaves can only communicate with each other via the master. Every bluetooth unit can be a member of up to four different piconets simultaneously but being master in only one of them. (Miklos, 2000).

Piconet traffic is strictly organized into a time division multiple access/duplex schemes (Gummalla and Limb, 2000). In this scheme, the master is only allowed to start transmitting in odd numbered time slots, each slot being 625 μs long, while slaves can only respond in even numbered slots after having been polled by a master packet. To minimize this collision effect as well as to cope with the fact that frequencies used by other devices on the radio channel can vary significantly over the bandwidth of the 2.4 GHz ISM band. Every piconet performs a rather fast frequency hopping (FH) scheme over 79 carries of 1 MHz bandwidth each and the maximum hopping frequency of this scheme is set at 1.6 kHz.

![Figure 2.3. A scatternet containing 3 piconets](image)

Because of the short range of BT and the small number of slaves that are active at any given time, several independent BT piconets will most likely co-exist on a factory floor. The co-existence of Bluetooth in the same area was investigated (Zurbes, 2000) by
performing radio network simulations (Matheus et al, 2003). The results show that in the interference scenarios the provided Forward Error Control Correction (FEC) methods are unsuitable to handle the almost binary character of the transmission channel. In order to obtain a good throughput and have low interference, it is disadvantageous to use short packet types. But using small packets inside an industrial environment cannot be guaranteed as the traffic bursts during the network operation might be very often and the network load can fluctuate accordingly (BSIG, 2004).

2.3.2 IEEE 802.15.4

The IEEE 802.15.4 standard (IEEE 802.15.4, 2003) was finalized in October 2003 and specifies the characteristics of the physical layer and the MAC layer of a radio networking stack. The goal of this standard was to create a very low cost, very low power, two-way wireless communication solution that meets the unique requirements of sensors and control devices (Callaway, 2002). In contrast to Bluetooth and IEEE 802.11, IEEE 802.15.4 has been specifically developed for use with applications in which a static network exists that has many infrequently used devices that transmit only small data packets.

In order to encourage widespread deployment, IEEE 802.15.4 has been placed in unlicensed frequency bands. When using the 2.4 GHz ISM band, IEEE 802.15.4 systems can get the same sort of global deployment as Bluetooth and IEEE 802.11b/g systems. The IEEE 802.15.4 standard has also been specified for use in the 868 MHz ISM-band in Europe and in the 915 MHz ISM-Band in North America. Within these bands, direct sequence spread spectrum (DSSS) is used in order to comply with the respective sharing rules of each band as well as to allow for simple analogue circuitry to be used. The maximum data rate of the DSSS is 250 Kbit/s in a single channel within the 2.4 GHz band. In total, the 2.4 GHz band accommodates 16 such channels. In the 868 MHz ISM band one channel with a data rate of 20 Kbit/s is available, whereas in the 915 MHz band ten channels of 40 Kbit/s each can be used. Because of various system parameters, especially the MAC protocol that is in use, the maximum user data rate will most likely be about half of its supposed value, or less (Howitt and Gutierrez, 2003).
The IEEE 802.15.4 standard differentiates between two different kinds of devices. A full-function device (FFD) can become a network coordinator and can work with other FFDs in a peer-to-peer fashion. Reduced-function devices (RFD), on the other hand, are always associated with one of these FFDs and are limited to exchanging data with this device alone (Benkic et al., 2007).

The IEEE 802.15.4 supports two different modes of operation, the unbeaconed and the beaconed. The differences of the two modes, their advantages and disadvantages have been researched (Howitt and Gutierrez, 2003) and evaluated repeatedly (Krishnamachari and Raghavendra, 2004).

There is sometimes confusion between IEEE 802.15.4 and ZigBee. The ZigBee alliance (Zigbee, 2008) is a consortium driven by industry and research institutions.
2.3.3 IEEE 802.11 Standards

There has been already a mention on the IEEE 802.11 standards in Chapter 1 and in this Chapter. Since Bluetooth and 802.15.4 have been presented with their key points the same will be done for the 802.11, as only the most common variations and extensions of IEEE 802.11 systems will be discussed here. Compared to the other two technologies, this thesis focuses mainly on the 802.11 and is explained thoroughly in the following chapters.

First of all the IEEE 802.11a (IEEE 802.11a, 1999) is placed in 5 GHz bands that are license exempt in Europe (5.15-5.35 GHz and 5.47-5.725 GHz) and unlicensed in the US (UNII bands, 5.15-5.35 GHz and 5.725-5.825 GHz). Over the whole spectrum, this allows for 21 systems to be running in parallel in Europe and eight in the US (IEEE 802.11a, 2003). The IEEE 802.11a physical layer (PHY) is based on the multi-carrier system Orthogonal Frequency Division Multiplexing (OFDM). The maximum user-visible rates depend on the packet sizes transmitted. In the 54 Mbit/s mode, the transmission of Ethernet packets that are 1500 bytes long results in a maximum user rate of about 30 Mbit/s, while sending packets with user payloads of just 60 bytes results in a throughput of 2.6 Mbit/s (Mattheus, 2004).

Second comes the IEEE 802.11b (IEEE 802.11b, 1999) which is a high rate extension to the original IEEE 802.11 DSSS mode and thus uses the 2.4 GHz ISM band. Although in principle either 11 or 13 different center frequencies can be used for the DSSS (depending on whether you are in the US or in Europe), only three systems can actually operate in parallel. In addition to supporting the 1 and 2 Mbit/s modulation rates of the basic IEEE 802.11 system, the payload of the IEEE 802.11b PHY allows for modulation with 5.5 and 11 Mbit/s Complementary Code Keying (CCK) (Biasi, 2008).

The faster version of 802.11b came on the 2003 and is called IEEE 802.11g (IEEE802.11g, 2003). It is actually an extension to the IEEE 802.11b specification and is consequently also placed in the 2.4 GHz band. It supports four different physical layers of which two are mandatory: the PHY that is identical to IEEE 802.11b and an OFDM PHY that uses the same modulation and coding combinations as IEEE 802.11a. Because of the different frequency band, the maximum user transmit rates are about 26
Mbit/s for Ethernet packets and about 2 Mbit/s for packets with user payloads of 60 bytes when using the 54 Mbit/s modulation scheme.

It can be seen that when transmitting packets that contain small payloads throughput values are significantly reduced. This reduction is due to the comparably large overhead of IEEE 802.11 packets and the different parameters present in the CSMA protocol (Matheus, 2004). IEEE 802.11 has been specifically optimized to transmit large data files, therefore showing a suboptimal performance when the majority of data is made up of short control packets. Measurements for the throughput of TCP/IP traffic in Ethernet packets for the IEEE 802.11b specification, for example, has returned results of a 5 Mbit/s maximum throughput (Mobilian, 2001).

### 2.4 Wireless technologies comparison/discussion

In the last few sections we examined three different systems. All three systems have been designed for use in different scenarios, thus offering various advantages and disadvantages over one another depending on their use. The 802.11 systems are suitable for transmitting large amounts of data. IEEE 802.15.4 is suitable when communication is occasional, small packet sizes are used, and power consumption is a problem. Bluetooth fills the gap between these two by being able to transmit at medium data rates with lower power consumption than IEEE 802.11. In Table 2.1 are presented the various characteristics of each technology, making easy the comparison between them.

<table>
<thead>
<tr>
<th></th>
<th>IEEE 802.11a/b/g</th>
<th>IEEE 802.15.4</th>
<th>Bluetooth/802.15.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>50-100 meters</td>
<td>10 meters</td>
<td>10 meters</td>
</tr>
<tr>
<td>Max. Data Rate</td>
<td>54 Mbits/sec</td>
<td>Up to 250Kbit/sec</td>
<td>3 Mbits/sec</td>
</tr>
<tr>
<td>Power consumption</td>
<td>low</td>
<td>Very low</td>
<td>medium</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Forward Error Correction</td>
<td>no</td>
<td>no</td>
<td>available</td>
</tr>
<tr>
<td>Transmission Scheme</td>
<td>DSSS/OFDM</td>
<td>DSSS</td>
<td>FHSS</td>
</tr>
<tr>
<td>Uses</td>
<td>Cable Replacement/Large transfer networking</td>
<td>Monitoring and controlling</td>
<td>Short Distance cable replacement</td>
</tr>
<tr>
<td>Power source</td>
<td>wired</td>
<td>Battery/wired</td>
<td>Battery/wired</td>
</tr>
<tr>
<td>Battery life duration</td>
<td>-</td>
<td>long</td>
<td>medium</td>
</tr>
</tbody>
</table>

Table 2.1. Comparison of the three main technologies
From Table 2.1 the results that can be deduced about the most appropriate technology for use within an industrial environment depend solely on the purpose of the network. Nowadays the WLANs that are deployed in the industry have been designed to replace the cable but only to a limited extent. This extent is mainly for monitoring and remote controlling of various sensors whose task is to coordinate the functions of data acquisition. This explains the low data rates supported by the IEEE 802.15.4 and the Bluetooth.

The purpose of this thesis differentiate from monitoring and controlling as its main objective is to provide a wireless network architecture that is able to achieve high rates of data transmission from the sensors to a storage facility inside the company where this data will be analyzed and presented in a readable format. During the experiments, the data produced from the sensors, depending on the type and number of sensors, usually reach the wireless network to its limits as it can arrive at 30 Gigabytes within an hour. Taking into consideration of Bluetooth and IEEE 802.15.4 it is obvious that these technologies cannot cope with the data produced. It is similar in the case of a Wireless Sensor Network (WSN). Whereas Bluetooth and IEEE 802.15.4 could satisfy the role of the sensors interconnection, our approach focused on the other main component of a WSN, the sink. The sink is responsible for transferring the collected data arriving to it from the sensors to the end user. The sensors are physically placed into a harsh environment but also the sink usually has to face almost the same harshness. Deploying an IEEE 802.11 wireless network in a harsh environment automatically defines the problems especially related to the reliability of the wireless links and explained in previous sections inside this chapter.

For the rest of this thesis, the main focus will be given on the IEEE 802.11 technology, examining possible techniques that could enable a corresponding WLAN to operate inside a harsh environment and minimizing the effects of interference, CCI and ACI. The network proposed is using wireless links to interconnect a variable number of nodes, working in an ad-hoc mode relaying data through multiple simultaneous routes over a number of hops until the data reaches its destination. There is no control or monitoring required and it should be considered as a direct cable replacement network with high speed rates, minimum delay and collisions.
2.5 Current and future approaches

The vast majority of current approaches/technologies used for wireless communications in an industrial environment focus mainly on factory and automation applications. With the simplification of accessing machinery, many industrial applications exist that could benefit from the use of wireless technologies. The localization and tracking of unfinished parts (Rybksi et al., 2002), the coordination of autonomous transport vehicles (Kongezos and Allen, 2002) and mobile robots as well as applications involving distributed control are all areas in which wireless technologies could be used in an industrial environment (Janet et al., 1999).

2.5.1 Current wired solutions

Networks in the area of factory automation have been developed with the specific requirement of tight real-time capabilities. These networks are typically used in industrial environment and they are called fieldbuses. Generally, fieldbuses can be categorized as local area networks. However, many different types of fieldbuses coexist, ranging from very small and primitive networks that are usually installed in cars such as the Controller-area Network called CAN (Kunert and Zitterbart, 1997, ISO-a, 1993, Cena and Valenzano, 2005), to more sophisticated networks used for factory communication such as PROFIBUS (UTE-a, 1996, Jecht et al., 2005) and WorldFIP (UTE-b, 1996, Thomesse, 2005). This large range of fieldbus systems categories is caused because of the wide diversity of industrial applications served by them. The one common characteristic between them is that they share the same tight timing conditions.

The extension of fieldbus systems is generally limited and it usually varies from a few tens to a few hundreds of meters. They are, therefore, not capable of covering the vast areas typical of modern industrial plants. The number of devices in an area of a plant may be so large as to require more than one fieldbus to interconnect them (Cavalieri and Panno, 1998). One way to overcome these restrictions was by implementing fieldbus islands (Kunert and Zitterbart, 1998). In the coming paragraphs there is a brief introduction to the PROFIBUS and WorldFIP in order to identify their structure and operational characteristics.
2.5.1.1 PROFIBUS

The PROFIBUS protocol is one of the most popular fieldbuses classified by international standards such as IEC61158 and EN50170. The history of PROFIBUS goes back to a publicly promoted plan for an association started in Germany in 1987. The goal was to implement and spread the use of a bit-serial fieldbus based on the basic requirements of the field device interfaces. PROFIBUS offers functionally graduated communication profiles which are the DP (Decentralize Periphery) and FMS (Fieldbus Message Specification). DP is the most frequently used profile (PROFIBUS Spec, 2000) and it permits mono-master or multi-master systems. This way it provides a high degree of flexibility during system configuration. On the other hand FMS is designed for communication of programmable controllers (Ozcelik and Ekiz, 2004).

PROFIBUS allows a maximum extension of 200 meters at 500 Kbps data rate. This aspect implies the existence of field bus islands, especially in larger installations. PROFIBUS frame format includes 0-246 bytes of variable data and 3-9-bytes of protocol control information (PROFIBUS Tech, 2002).

2.5.1.2 WorldFIP

Another broadly used fieldbus protocol is the WORLDFIP which was introduced in 1986, as a requirement of companies asking for a fieldbus that would employ a single protocol for every possible task that would be required to be undertaken, while some other fieldbuses might require two or even three more protocols to cover the same range of tasks (UTE-b, 1996).

WorldFIP implements the producer-(distributor)-consumer model, in which communication is based on unacknowledged broadcasts of data identifiers (by the distributor), to which the station possessing the identified data item (the producer) responds by broadcasting its current value (Thomesse, 2005). All nodes interested in this data (the consumers) copy the received value into an internal link-layer buffer for later delivery to the higher layers. This can be regarded as an instance of a publish/subscribe interaction pattern (Eugster et al, 2003).
The data rate that can be achieved in such a system lies between the 1Mbps and 2.5Mbps depending on the traffic and task requirements. Compared to the PROFIBUS speed is increased significantly, although this speed advantage sometimes is not utilised depending on the task requirements of the network (Thomesse, 2005).

2.6 Hybrid wired/wireless approaches

As described in the previous section, traditional wired fieldbus systems face network performance degradation for large numbers of segments because of their reliance on cabling. The scalability problems they encounter when there is the need to extend the fieldbus forced the companies to have a look on the alternative option such as the wireless technology. With the advancements of wireless technology, a wireless network can be integrated to an existing fieldbus system (Willig et al. – 2005) and consequently there is the creation of the wireless fieldbus or also called hybrid wired/wireless system.

The wireless Fieldbus has strengths based on mobility, ease of installation and maintenance due to the lack of cabling. In general, the industrial environment is error prone and the reliability of wireless technology is lower than a wired counterpart. In addition to reliability issues of wireless links, it was preferable not to change the protocols of the existing wired nodes (Decotignie, 2005). The coupling devices transferring packets between the wired and the wireless components of the network introduced additional forwarding delay (Koulamas et al., 2004). Therefore, it is difficult to support a real-time transmission and multiple input/output nodes in the industrial environment. For these reasons, it is necessary to design a wireless Fieldbus which can support multiple nodes and guarantee real-time transmission of mixed traffic in an industrial environment. Almost all the available commercial technologies described earlier in this chapter, have been used to implement a hybrid fieldbus system and each one comes with its advantages and disadvantages compared to the rest regarding the network needs and limitations.

There were some studies on the hybrid methodology using the IEEE 802.11 protocol based on the PROFIBUS technology (Willig, 2003, Lee et al., 2002) and the gains were on the data rate of the extended wireless system with simultaneous improvements on
the behaviour of the wireless links in order to overcome the harshness of the industrial environments. On the other hand, another approach based on IEEE 802.11 relates to the implementation of R-Fieldbus (Rauchhaupt, 2002). The R-Fieldbus architecture provided a complete solution where multiple segments and multiple wireless cells are interconnected via the physical layer intermediate systems called repeaters. This solution was compatible with standard PROFIBUS, but the main drawback was the fact that all messages were broadcasted throughout the network, leading to no error containment between different domains and low sensitivity to failures (Sousa et al., 2007).

Bluetooth was another wireless technology used and proposed for a wireless fieldbus and in this case, both of the approached were based on two different concepts. In the first one (Miorrandi and Vitturi, 2004), Bluetooth was used as an extension of a PROFIBUS-DP system and on the second approach (Dzung et al., 2005) it was implemented on each node of the network in an attempt to replace the wires of the system. The main initiatives of using the Bluetooth technology were the low cost of the Bluetooth devices and the fast transmission rate. However they both were composed of few nodes and had a small coverage area, hence, it was difficult to apply them in large factory areas where multiple nodes are required.

IEEE 802.15.4 was also proposed for implementing a hybrid fieldbus system. The first proposal (Baker, 2005) was a low rate wireless personal area network (LR-WPAN) used for data gathering and control with the use of sensors. The coordinator node of the LR-WPAN could manage multiple nodes and support a large range of tasks. Each node of this technology was not expensive and the coordinator could handle many input and output nodes at the same time. The drawback in this approach was it could not handle efficiently mixed real-time traffic, a requirement for industrial applications. The second approach (Dong-Hyuk and Dong-Sung, 2008), introduced a wireless fieldbus that was able to manage up to 255 multiple nodes and it’s response times could be guaranteed within 100 ms. By the use of a superframe based on IEEE 802.15.4 MAC protocol, it managed to achieve proper bandwidth allocation, traffic control and low power consumption. The main disadvantages of the system were the low data rate available because of the specification of the protocol but also the limited number of nodes that it
could serve. This approach would be inappropriate for large scale industrial environments, as if the network exceeded the proposed volume, then it would start underperforming.

One last wireless technology used for implementing a wireless fieldbus was the WiMAX or 802.16 MAC protocol. The authors in this attempt (Iskefiyeli and Ozcelik, 2007) attempted to improve the scalability of a PROFIBUS system by interconnecting their various segments through WiMAX links. The initiative behind this proposal was to address the limits to the data rates that are imposed as the distance between the various segments increases from 200 meters to 1200 meters and has been discussed earlier in this chapter. In order to overcome this limits, the authors (Iskefiyeli and Ozcelik, 2007) used wireless 802.16 links as backbones achieving high speed data communications over large distances. Although this system provides a complete solution for interconnecting large numbers of PROFIBUS segments, it introduces extra mechanisms such packet encapsulation for communication between the fieldbus and WiMAX segments. Such mechanisms add extra delay to packet transmissions cannot meet the real-time requirements.

2.6.1 Wireless Sensor Networks

A wireless sensor network (WSN) (Karl and Willig, 2005, Akyyildiz and Sankarasubramaniam, 2002), is a complete different form of technology for data gathering and task performance from the ones mentioned in the previous paragraphs. Sensor networks offer a complete wireless communication between the various nodes of the network without requiring any wiring between them.

They consist of a large number of small, energy- and resource-constrained sensor nodes. An individual sensor node is composed of sensor circuitry (for example temperature or humidity), a microcontroller, small amounts of RAM and program memory, a wireless transceiver and an energy supply, most often a battery. Some nodes might also be attached to actuators and in this case sensor networks are sometimes referred to as wireless sensor- and actuator networks. While each individual sensor node has limited computational capabilities, the nodes can communicate
wirelessly and perform collaborative signal processing tasks. With wireless sensor networks it is possible to collect much more real-time data than was possible before, from places which are hazardous or otherwise inaccessible for wired technologies.

Wireless sensor networks can be used in many ways in industrial and factory automation (Kahn et al., 2005). An important class of applications is monitoring of equipment and machinery health, using for example vibration, heat or thermal sensors but there are scenarios where sensors are typically not part of any control loop and therefore the timeliness requirements are not extremely hard, but reliability is an important issue (Singhvi et al., 2005).

The architecture of a WSN, is similar to that of ad hoc networks, but there are also some important differences. In sensor networks all nodes cooperate to fulfill a common task. A sensor network is designed as a whole to run a single or very few related applications, which involves sensing the physical environment and collaborative processing of sampled data. Sensor networks have more structure than ad hoc networks. There are typically a few sink nodes present, to which the sensor nodes report their data. The sink nodes can configure to control the operation of the sensor nodes, they provide the interface to human users and they can serve as gateways to other networks.

![Figure 2.5. The architecture of a Wireless Sensor Network. (Akyyildiz and Sankarasubramaniam, 2002)](image-url)
The two main challenges of sensor networks are energy efficiency and scalability. Energy- and power-efficiency has a significant influence on protocol design. For many node designs the wireless transceiver requires the largest share of the overall power budget. Depending on the actual combination of microcontroller and transceiver, the microcontroller can execute several hundreds or even thousands of instructions with the same energy as needed for transmitting one bit on the wireless channel (Krishnamachari et al., 2002, Madden et al., 2002) On the other hand, the need for redundancy increases the number of nodes in a sensor network. When large areas have to be observed, the number of required nodes can be in the range of thousands or even tens of thousands. Scalability is therefore a second critical concern, and one of the immediate results is that individual sensor nodes and the overall sensor network should be self-organizing (Santi, 2005).

2.6.2 Fieldbus discussion

In the previous paragraphs there has been an overview of both wired and wireless fieldbus systems. Wired fieldbuses were the first to be introduced about twenty years ago and as has been described in this chapter, they provided and solved many problems but also they found many new applications inside the industrial environment for data gathering and command control. As technology progressed and new technologies appeared for industrial applications the needs for faster and more reliable fieldbus systems appeared. There were some solutions proposed for increasing the network speed but it’s scalability seemed to be the main problem. Factory areas kept expanding and at the same time fieldbuses struggled to follow because of the limitations of their technology to grow in number of nodes and covered distances.

With the advance of wireless technology, many researchers thought that they could overcome the scalability problems by deploying wireless links between the fieldbus nodes or segments. Wireless capabilities were added to the nodes but having to maintain the protocol compatibility of the existing wired systems, the improvements to the network speed were minimized although more nodes could be connected to the fieldbus and the number of segments increased significantly.
The use of wireless technologies in fieldbus systems has resulted in many attempts with some of them being very interesting and useful for the deployment of wireless local area networks. Nevertheless, fieldbus systems are not the main target of this thesis and the research described. Although it examines the existence of wireless nodes inside industrial environments and identifies the problems and the challenges, it avoids focusing on the fieldbus or the wireless sensor networks technologies. The main target is to investigate the behavior of a WLAN not at the physical and link layer but merely on an efficient routing algorithm with the use of a channel assignment algorithm able to provide a high capacity and reliable wireless network based on the 802.11 protocol.

2.7 Conclusion

The replacement of wired networks with wireless ones is a fact in an enterprise area. The reasons behind this trend are based on the advantages that wireless networks compared to the wired counterparts. On the other hand there are numerous problems which have been discussed by explaining the reasons of their existence in an industrial environment and how they affect a wireless network’s performance. The main problem of such environment is the interference produced from neighbouring nodes that happen to be within the transmission range of other nodes. There are other problems such as throughput and delay of wireless links which are also dependant on the existence of interference in the area. At the end there was a comparison of various wireless technologies by pointing out their advantages and disadvantages and the role that each one can undertake.

Next step was to introduce the forms of networks for industrial deployment. The initial implementations of such networks were solely based on wired solutions, called fieldbuses. It soon was made clear that wires posed problems for certain scenarios and technologies and the best was to overcome them was by implementing wireless nodes and transmitting data over air. These solutions gave the advantage of interconnecting large segments of fieldbuses together and avoid the use of cables over large distances.

The next chapter of this thesis will focus on the routing protocols available for multi-hopping and multi-channel ad-hoc networks, taking into consideration the
characteristics of industrial network problems but also on the techniques to avoid CCI and ACI and increase the average throughput of the network. There will be review of the main routing methods for both mesh and ad-hoc architectures, evaluating them and selecting the one that will best fit into the requirements of this thesis. In addition to routing, the next chapter will also critically evaluate the variety of possible Channel Allocation Algorithms, designed and proposed by different researchers trying to overcome the effects of interference.
3 Multi-radio Network Routing & Channel Assignment Schemes

3.1 Background

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network, electronic data networks (such as the Internet), and transportation networks. In wired networks such as the Internet, in general, routing will be performed by using IP (Internet Protocol) addresses. There are specific IP address ranges assigned for each country and within this country there will be further subsets assigned for each region, similar to a telephone system with its country and area codes. On the other hand in IP networks, the geographical separation is not as distinct as there could be several IP ranges of one area depending on who is the Internet Service Provider (ISP). This way the network can be organized in a tree-like configuration, with the individual computers at the bottom and increasingly large address ranges as you move up the tree, with the whole address space being the head. In order for routers to be able to automatically discover the address of its neighbour routers, broadcasts a HELLO packet periodically giving information for the network it is member of. This information is saved in the receiver nodes for further use. Although it might sound simple and straightforward when talking about a wired network, in the case of a wireless network the process becomes more complicated because of their nature, architecture and requirements.

As explained in Chapter 1, there are currently two variations of wireless networks. The first is known as the *infrastructure network* (i.e., a network with fixed and wired gateways). The interconnecting devices for this type of networks are called the base stations. When the a wireless node, such as a laptop, enters a wireless network, will start searching for a base station which accommodates it and provides it with all the required procedures and services in order to access the internet or to communicate with other wireless nodes within the same area.
The second variation of wireless network is the independent mobile network, commonly known as an ad-hoc network. Independent networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in a random manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network.

In both variants of the wireless network, there are four different delivery semantics such as unicast, broadcast, multicast and anycast as presented in Figure 3.1. In unicast a message is delivered to a single specified node, whereas in broadcast the message is sent to all the nodes into the network. On the other hand in multicast a message is delivered only to a group of nodes that expressed interest in receiving it. Finally for the anycast semantic, a message is delivered only to one node from a group for example, it happens to be closest to the source.

<table>
<thead>
<tr>
<th>The unicast scheme</th>
<th>The broadcast scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Unicast Diagram" /></td>
<td><img src="image2" alt="Broadcast Diagram" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The multicast scheme</th>
<th>The anycast scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3" alt="Multicast Diagram" /></td>
<td><img src="image4" alt="Anycast Diagram" /></td>
</tr>
</tbody>
</table>

**Figure 3.1. The four basic routing schemes**

This chapter introduces briefly the traditional routing algorithms firstly deployed in wired networks and then will present the three categories of routing protocols for use in an ad-
hoc network: the reactive, the proactive and the hybrid by evaluating some examples for each category. A comparison between these three schemes is performed and the results will present the advantages and disadvantages of each approach. Also this chapter will present the limitations and problems that ad-hoc wireless networks face within a mesh network and their evolution in order to achieve a better and more reliable performance taking advantage of the benefits of a mesh topology.

Within a wireless mesh network, routing is not the only major concern. Channel assignment for multi-radio mesh networks is an area of research which has been greatly investigated, and there numerous proposals on how to manage multiple radios and channels sometimes in co-ordination with new or existing routing techniques. Nowadays, because of the deployment of more bandwidth hungry applications, traditional single channel networks have reached their limitations. Considering also the interference produced since all the nodes operate in the same frequency channel, researchers started to find ways in order to deploy multiple channels on each node either by using a single radio or multiple. Just like the routing proposals which are presented in the following sections of the chapter, a large number of proposals for channel assignment algorithms is related to the network variations such as topology and size, traffic pattern and levels of interference (Mirchandani et al., 2007b).

### 3.2 Wired routing protocol

Routing is a fundamental issue for networks. A lot of routing algorithms have been proposed for wired networks and some of them have been widely used. Dynamic routing approaches are prevalent in wired networks. Distance Vector routing (Hedrick, 1988) and Link State routing (McQuillan et al., 1978) are the two most famous routing algorithms being used in wired networks.

Distance Vector routing protocols are based on the Bellman-Ford (Tanenbaum, 1996) routing algorithm. In Distance Vector routing, every router maintains a routing table in which it stores the cost information to all reachable destinations. A router exchanges cost information with its neighbours from time to time to update its routing table. The cost can be calculated based on metrics such hop number, queue length or delay. If
multiple paths exist, the shortest one will be selected. The main weakness of Distance Vector routing algorithm is the slow convergence. The most common protocol of this category is the Routing Information Protocol (RIP) (Malkin, 1993)

In Link State routing algorithm, each node periodically notifies its current status of links to all routers in the network. Whenever a link state change occurs, the respective notifications will be flooded throughout the whole network. After the collection of the notifications, all routers get to know at least a small part of the total network. In Link State the metrics usually used are the number of hops, link speed and traffic congestion. A common protocol of Link State algorithm is the Open Shortest Path First (OSPF) (Moy, 1998).

In wired networks, the two algorithms above perform well because of the predictable network properties, such as static link quality and network topology. However the dynamic feature of an ad-hoc network weakens their effectiveness. In such networks, frequent topology changes will greatly increase the control overhead and as consequence this will require more bandwidth. Furthermore, Distance Vector and Link State routing algorithms will cause routing information inconsistency and route loops when used for dynamic networks.

Although numerous routing protocols have been proposed for ad-hoc networks, there does not exist a universal scheme that works well in scenarios with different network sizes, traffic overloads, and node mobility patterns. Moreover, these protocols are based on different design philosophies and proposed to meet specific requirements from different application. Thus, the performance of an ad-hoc routing protocol may vary dramatically with the variations of network status and traffic overhead. The performance deviations of mobile ad-hoc network routing protocols make it a very difficult task to give a comprehensive performance comparison between a large number of routing protocols.

Generally a routing protocol needs to address three key issues to provide a service in a communications networks:
• Route Discovery - This process involves the discovery of the path through the network to the destination. The routing protocol has to establish which nodes packets need to be routed through to reach the destination and this path will usually fit certain criteria.

• Packet Relay - Once a path has been discovered between the source and the destination, the routing protocol is responsible for passing the packets along it. This includes handling the dropped packets and sensing link failures so that route maintenance may be initiated. In addition, this part of the protocol is also responsible for initiating route discovery when a new packet without a route is received or created.

• Route Maintenance – A route can become invalid at any point due to node failures or changes in network topology; however, in an ad-hoc network, node mobility is the most common cause of a route becoming invalid due to the change in topology. Therefore, a routing protocol is expected to handle this scenario and rediscovery or alter the route as quickly as possible to maintain the communication path.

3.3 Wireless routing protocols

To compare and evaluate ad-hoc network routing protocols, appropriate categorization methods are important. Classification methods help researchers and designers to understand individual characteristics of routing protocols and find their relationship with others. These characteristics mainly are related to the information which is exploited for routing, when this information is acquired, and the roles which nodes may take in the routing process. Taking into consideration the above, currently the routing protocols deployed in a ad-hoc network are divided into three main categories, the proactive, the reactive protocols.

Reactive routing protocols for ad-hoc networks are also called "on-demand" routing protocols. In a reactive routing protocol, routing paths are searched only when needed. A route discovery operation calls up a route-determination procedure. The discovery procedure terminates either when a route has been found or no route available after examination of all route combinations. In a wireless network, active routes may stop
being valid because of node mobility or weak radio links between the wireless nodes, therefore route maintenance is an important operation for reactive routing protocols.

A proactive routing protocol is also called "table driven" routing protocol. Using a proactive routing protocol, nodes in an ad-hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one. All nodes need to be continuously aware of the network topology and when a network topology change occurs, respective updates must be publicizes throughout the network to notify the change.

The third category is called hybrid routing protocols and it is an attempt to combine the good aspects of proactive and reactive routing protocols and overcome their weaknesses. The protocols that fall within this category exploit hierarchical network architectures. Proper proactive and reactive routing approaches are exploited in different hierarchical levels, respectively.

Choosing a protocol depends very much on the application to which it is being deployed. Reactive protocols cause a connection initiation delay due to the discovery process taking place at that time; however, the route discovered is more likely to be up to date. Proactive protocols often respond slowly to changes in topology as the information converges slowly by nodes sharing information. In addition, proactive protocols incur an overhead regardless of whether any communication is taking place in that part of the network or not.

### 3.3.1 Reactive routing protocols

On-demand routing protocols were designed to reduce the overheads in proactive protocols by maintaining information for active routes only. This means that routes are determined and maintained for nodes that require sending data to a particular destination. A large number of different reactive routing protocols have been proposed to increase the performance of reactive routing but only some very common examples are presented below.
3.3.1.1 Dynamic source routing – DSR

The Dynamic Source Routing (DSR) (Johnson and Maltz, 1996) is a reactive unicast routing protocol that utilizes source routing algorithm. In source routing algorithm, each data packet contains complete routing information to reach its destination. Additionally, in DSR each node uses caching techniques to maintain route information that it has acquired. When a source node wants to send a packet of data to a destination DSR has two main stages which are going through before it starts the data transmission, the route discovery stage and the route maintenance stage. If a route is available, the source node incorporates the routing information within the data packet otherwise it will initialize a route discovery procedure by broadcasting route request packets.

During route request the sender node sends the request and the next node which receives it checks its own routing cache. In case it doesn’t have routing information for the requested destination, it attaches its own address to the route record field and forwards it its neighbours. When the request packet reaches the destination or any other in-between node that has information to the destination, it produces a route reply packet. The reply packet includes address of all the nodes that the request packet has travelled through.

Once the route has been created either a route reply packet is routed back to the source and in three ways. In the first case the node already has a route back to the source. In the second case the network has bi-directional links and the reply packet is sent using collected routing information in the route record field in reverse order. The third option takes place when there are one-directional links and a new route discovery process initiates in order to reach the source node. Finally in this case, when the data link layer detects a link failure, a route error packet is generated and sent backwards to the source and initialises another route discovery operation.
3.3.1.2 Ad-hoc on-demand distance vector – AODV

The second example of the reactive routing protocol family is the Ad Hoc On-demand Distance Vector Routing (AODV) protocol (Perkins and Royer, 1999). As a reactive routing protocol, AODV only needs to maintain the routing information about the active paths. In AODV, routing information is maintained in routing tables at nodes. Every mobile node keeps a next-hop routing table, which contains the destinations to which it currently has a route.

When a node wants to send data packets to another node, but doesn’t have a route available to the destination, will initiate the route discovery process. During this process, the source will broadcast route request (RREQ) packets. These packets include address of the source and the destination nodes, a broadcast ID that is used as identifier, the last seen sequence number of the destination and also the source’s sequence number.

Every node maintains a cache to keep track of RREQs it has collected. The cache also stores the path back to each RREQ sender. When a node receives a RREQ it checks the destination sequence numbers it currently holds and in order to maintain fresh routing information a route reply (RREP) packet is created and sent back to the source.
The use of HELLO packets is essential when a node wants to notify its existence to its neighbours and this way the link status of the next-hop is successfully monitored. In case of a link failure discovered by a node, a route error (RERR) packet is broadcasted.

This chapter tries to cover a very limited number of reactive routing protocols and present the main procedures taking place for route discovery and maintenance. There are of course vast number of protocols available and although they operate under the same concept, they take into consideration different metrics in order to set up their routing information.

### 3.3.1.3 Comparison of reactive routing protocols

The number of reactive routing protocols is vast and very often there are new proposals or some are based on current solutions by offering improvements on their functionality. For this reason Table 3.1 gives a general picture of the similarities and differences between the route discovery and maintenance between AODV, DSR, TORA and SSR. The Temporally Ordering Routing Algorithm (TORA) is a routing algorithm based on the concept of link reversal. TORA improves the partial link reversal method by detecting partitions and stopping non-productive link reversals and can be used for highly dynamic mobile ad-hoc networks (Park and Corson, 1997). The final competitor is the Signal Stability Routing algorithm (SSR) (Dube et al., 1997), whose metrics are signal strength and location stability.

<table>
<thead>
<tr>
<th></th>
<th>Update Destination</th>
<th>Update Period</th>
<th>Structure</th>
<th>Multicast Capability</th>
<th>Hello message</th>
<th>Route Metric</th>
<th>Multiple Routes</th>
<th>Unidirectional Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>AODV</td>
<td>Source</td>
<td>Event</td>
<td>Flat</td>
<td>Yes</td>
<td>Yes</td>
<td>Fastest &amp; shortest</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>DSR</td>
<td>Source</td>
<td>Event</td>
<td>Flat</td>
<td>No</td>
<td>No</td>
<td>Shortest</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TORA</td>
<td>Neighbors</td>
<td>Event</td>
<td>Flat</td>
<td>No</td>
<td>No</td>
<td>Shortest</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSR</td>
<td>Neighbors</td>
<td>Periodically / Event</td>
<td>Flat</td>
<td>No</td>
<td>Yes</td>
<td>Signal Stability</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

***Table 3.1. Comparison of four reactive protocols***

### 3.3.2 Proactive routing protocols

In proactive routing protocols, each node maintains routing information to every other in the network. The routing information is usually kept in a number of different tables.
These tables are periodically updated in the case of the network topology changes. The differences between these protocols exist in the way the routing information is updated and detected and the type of information kept at each routing table. Furthermore, each routing protocol may maintain different number of tables. This section describes two proactive protocols such as WRP and DSDV.

### 3.3.2.1 Wireless Routing Protocol – WRP

The Wireless Routing Protocol (WRP) (Garcia and Murthy, 1996) is a proactive unicast routing protocol for ad-hoc networks. To adapt to the dynamic features of mobile ad hoc networks, some mechanisms are introduced to ensure the reliable exchange of update messages and reduces route loops.

In WRP, every node maintains a number of tables that include information such as distance, routes, cost of network links and a Message Retransmission List (MRL). Each entry in the routing table contains the distance between a destination node, the predecessor and the successor. Storing the predecessor and the successor in the routing table helps to avoid counting to infinity problems as this is the main problem of the initial distance vector routing algorithm. Every node creates an entry for each neighbouring node in its link-cost table. This entry usually encloses the cost of the link to the neighbour and the number of the timeouts since a message free of errors was received from that neighbour.

On the other hand the MRL contains the nodes that didn’t acknowledge an update message and if needed this message will be resent. In the case that no changes happen to the routing table since the last update, the node is obliged to send a HELLO packet to maintain connectivity. Due to the large number of tables every node has to maintain, the memory requirements are quite demanding but also being a proactive protocol it has limited scalability and is not suitable for large networks.
3.3.2.2 Destination sequence distance Vector – DSDV

Another proactive routing algorithm is the Destination Sequence Distance Vector also called DSDV (Perkins and Bhagwat, 1994). DSDV as the WRP is also based on the Bellman-Ford algorithm but they use different methods to improve routing performance in ad-hoc networks.

When a new entry is saved in the routing table of DSDV, it includes the next hop towards a destination, the cost metric for the routing path to the destination and finally a destination sequence number. This number is used in DSDV to distinguish old routes from new ones and avoid the creation of route loops.

Route updates can either be performed at certain time intervals or in the case of an event. Every node periodically transmits updates including its routing information to its close neighbours. Also DSDV has two ways of sending routing table updates, the first being “full dump” update type and the full routing table is included inside the update. The second way is through an incremental update which contains only those entries that have been changes since the last performed update. Finally the “full dump” may be performed by sending many packets whereas the incremental may need just only one.

3.3.2.3 Comparison of proactive routing protocols

Just like in the case of reactive, proactive protocols also have been developed and improved significantly during the recent years either by proposing new ones or by improving current developments. In the case of existing protocols many researchers have implemented and added extra features like these that can be found in Table 3.2. For clarification purposes FSR is the Fisheye State Protocol (Gerla, 2002) a descendent of the Global State Routing protocol (GSR) (Chen and Gerla, 1998). FSR updates the network information for nearby nodes at a higher frequency than for the remote nodes, which lie outside the fisheye scope. Finally, the last member to the comparison is the Cluster-head Gateway Switch Routing algorithm (CGSR). CGSR is a hierarchical routing protocol where the nodes are grouped into cluster and there is no need to maintain a cluster hierarchy. Instead, each cluster is maintained with a cluster-
head, which is a mobile node elected to manage all the other nodes within the cluster (Chaing, 1997).

<table>
<thead>
<tr>
<th></th>
<th>Update Destination</th>
<th>Update Period</th>
<th>Structure</th>
<th>Multicast Capability</th>
<th>Hello Message</th>
<th>Route Metric</th>
<th>Unidirectional Link</th>
<th>Multiple Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRP</td>
<td>Neighbours</td>
<td>Event/ Periodically</td>
<td>Flat</td>
<td>No</td>
<td>Yes</td>
<td>Shortest</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DSDV</td>
<td>Neighbours</td>
<td>Event/ Periodically</td>
<td>Flat</td>
<td>No</td>
<td>No</td>
<td>Shortest</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FSR</td>
<td>Neighbours</td>
<td>Periodically</td>
<td>Flat</td>
<td>No</td>
<td>No</td>
<td>Shortest</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CGSR</td>
<td>Neighbours &amp; Clusterheads</td>
<td>Periodically</td>
<td>Hierarchical</td>
<td>No</td>
<td>No</td>
<td>Shortest</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 3.2. Comparison of four proactive protocols

3.3.3 Hybrid routing protocols

Hybrid routing protocols are a new generation of protocol, which are both proactive and reactive in nature. These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads. This is mostly achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes using a route discovery strategy. Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of zones by each node. Apart from the zone-based protocols, there have been proposals that grouped the network nodes into trees and clusters. Since the majority of the proposed hybrid routing protocols until now were zone-based (Sarkar et al, 2008), this section describes only a representative of this category and specifically the ZRP.

3.3.3.1 Zone Routing Protocol – ZRP

The ZRP (Haas, 1997, Haas and Pearlman, 1998) combines the advantages of the proactive and reactive approaches by maintaining an up-to-date topological map of a zone centred on each node. Within the zone, routes are immediately available. For destinations outside the zone, ZRP employs a route discovery procedure, which can benefit from the local routing information of the zones.
Proactive routing uses extra bandwidth to maintain routing information, while reactive routing imposes long route request delays. Reactive routing also inefficiently floods the entire network for route determination. ZRP aims to address the problems by combining the best properties of both approaches. ZRP reduces the proactive scope to a zone centred on each node. In a limited zone, the maintenance of routing information is easier.

In ZRP, the network is divided into routing zones according to distances between mobile nodes. Given a hop distance \( p \), also called radius, and a node \( N \), all nodes within radius at most \( p \) from \( N \) belong to the routing zone of \( N \). Peripheral nodes of \( N \) are \( N \)'s neighbouring nodes in its routing zone which are exactly \( p \) hops away from \( N \).

![Figure 3.3. Example of ZRP routing with \( p = 2 \)](image)

For example in Figure 3.3, the routing zone of \( S \) with \( p \) equals to 2, nodes from A to F are interior nodes, nodes G up to J are peripheral and node K is out of the routing zone. According to this all the nodes inside the routing zone imply to internal routing rules while communication between \( S \) and \( K \) nodes would require global based routing decisions as explained below.

### 3.3.3.2 Comparison of hybrid routing protocols

The hybrid family includes a large number of proposals that have been developed in the last decade. While others tried to improve their initial suggestions some attempted to
combine the advantages of both approaches and present new proposals which would overcome any possible drawbacks. In this section ZRP is compared with two more such as the ZHLS, Zone-based Hierarchical Link State (Joa-Ng and Lu, 1999) and the Distributed Spanning Trees (DST) based routing algorithms (Radakrishnan et al., 1999). ZHLS employs hierarchical structure and divides the network into non-overlapping zones, and each node has a node ID and a zone ID, which is calculated using a GPS. On the other hand, DST, the nodes in the network are grouped into a number of trees. Each tree has two types of nodes; route node, and internal node. The root controls the structure of the tree and whether the tree can merge with another tree, and the rest of the nodes within each tree are the regular nodes. Table 3.3 gives an approach on the main differences of the three schemes.

<table>
<thead>
<tr>
<th></th>
<th>Update Destination</th>
<th>Update Period</th>
<th>Structure</th>
<th>Multicast Capability</th>
<th>Hello Message</th>
<th>Route Metric</th>
<th>Unidirectional Link</th>
<th>Multiple Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZRP</td>
<td>Neighbours</td>
<td>Periodically/Event</td>
<td>Flat</td>
<td>No</td>
<td>Yes</td>
<td>Shortest</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ZHLS</td>
<td>Source</td>
<td>Event</td>
<td>Hierarchical</td>
<td>No</td>
<td>No</td>
<td>Shortest</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DST</td>
<td>Neighbours</td>
<td>Periodically</td>
<td>Hierarchical</td>
<td>No</td>
<td>No</td>
<td>Stable</td>
<td>Routing</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 3.3. Comparison of three hybrid protocols

3.4 Multipath routing and mesh networks

All the proposals presented until now in this chapter regarding various routing algorithms could be classified according to their ability to set up a single path and unicast, when needed and route all the transmitted data through this path. In the case of a failure the routing algorithm starts its discovery mechanism to find a new route and continue any transmissions between the same pair of source and destination. These types of algorithms deploy the unicast routing, as presented in the beginning of this chapter, thus they are called unicast routing algorithms. On the other hand, these unicast algorithms can also send the information using not a single path but instead to send a number of packets simultaneously through alternative routes. These algorithms are called multipath routing algorithms and they adopt the benefits of a wireless mesh network (WMN) such as multiple paths, load balancing, better scalability and self organizing.
Wireless mesh networks (WMNs) are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. WMNs are originally comprised of two types of nodes: mesh routers and mesh clients. A mesh router contains additional routing functions to support mesh networking and through multi-hop communications, the same coverage can be achieved by a mesh router with much lower transmission power.

Over the years, there were proposed schemes that included to their functionality the multipath routing. Multipath routing is a technique that takes advantage of the original physical network resources by utilizing multiple source-destination paths. It is used for a number of purposes, including bandwidth aggregation, minimizing end-to-end delay, increasing fault-tolerance, enhancing reliability, load balancing, and so on. Although a WMN is similar to ad hoc networks in some respects, such as both being multi-hop wireless networks, there are a few important differences that warrant different routing strategies. First of all, mesh routers are usually static and consequently mobility is not an issue. This means network topology change is less frequent than in ad hoc networks. Secondly, mesh routing protocols do not have energy consumption restrictions, since mesh routers are not battery powered. Thirdly, the traffic distribution in a WMN is generally skewed. This is because traffic is usually directed towards/from particular points.

Numerous multipath routing protocols have been proposed for use in wireless ad hoc networks. Many of them are based either on AODV or DSR, both being described in previous sections of this chapter.

### 3.4.1 Split multipath routing – SMR

SMR (Lee and Gerla, 2001) is a multipath protocol based originally on DSR. Unlike many prior multipath routing protocols, which keep multiple paths as backups routes, SMR is designed to utilize multipath concurrently by splitting traffic onto two maximally disjoint routes. Two routes said to be maximally disjoint if the number of common links is minimum (Taft-Plotkin et al., 1999).
Within SMR the intermediate nodes do not reply to RREQs even if they have saved routes for the required destination. Another task of the intermediate nodes is to forward RREQ packets that were received from different links to the node that the initial RREQ was received from. This further increase the number of routes received by the destination, although this comes at a cost of increased overhead. The shortest delay route, identified by the first RREQ to arrive at the destination, is used. The destination then selects the second route as the one that is maximally-disjoint to the first route.

In the event of a route failure, every entry, regardless of destination, in the source’s routing table that shares common intermediate nodes with the fail route is removed. After this if the other route remains valid, either a new route discovery is initiated, or the protocol waits until the second route fails also. This way SMR is more efficient than its predecessor the DSR, as the delay of the network decreases because with a single route failure the protocol doesn’t initiate a route discovery, but only when both fail. Another improvement of this arrangement is the generation of smaller overhead always compared to DSR.

### 3.4.2 Ad-hoc on demand multipath distance vector – AOMDV

It is pretty clear that AOMDV is based on the original AODV but with changes made to the route discovery and maintenance procedures in order to support multipath routing (Marina and Das, 2003). AOMDV ensures that alternate paths at every node are disjoint, therefore achieves path disjointness without using source routing.

Compared to AODV, AOMDV includes two additional fields in the route entry, the hop-count and the last-hop. These two help to solve the problems of loop freedom, and path disjointness. When AOMDV performs multipath route discovery, the hop-count field contains the length of the longest path for a particular destination sequence number, and is only initialized once. Therefore the hop count remains unchanged until a path for a higher destination sequence number is received. This way the loop freedom is guaranteed as long as a node never advertises a route shorter than one already advertised, and never accepts a longer one.
For the path disjointness problem the algorithm deploys the following procedure. A node discards a path advertisement that has either a common next-hop or a common last-hop as one already in the route table. As long as each node sticks to this rule, all paths for the same destination sequence number are guaranteed to be link-disjoint. Finally, the route maintenance is analogous to that of AODV and in case of a link error a RERR for a destination is created when the last path to the destination fails.

### 3.4.3 Multipath source routing – MSR

The Multiple Source Routing (MSR) (Wang et al., 2001) is purely based on the reactive DSR protocol and is considered to be an extension of the initial implementation. MSR consists of a scheme to distribute data traffic amongst multiple routes within a wireless network (Wang et al., 2002). It uses the same route discovery process as DSR with the exception that multiple paths can be discovered and returned compared to the single path in DSR.

To begin with, when a source node asks for a route to a destination, but if there isn’t one available in the cache, MSR will commence a route discovery process by flooding the network with RREQ packets. Each intermediate node contributes to the route discovery by appending its own address to the route record. When the RREQ packet reaches the destination, a RREP will be issued and it is send back

Since source routing is used in MSR, intermediate nodes do nothing but forward the packet according to the route in the packet-header. A multiple-path table is used for the information of each different route to a destination. This table contains for each route to the destination three basic essentials. Firstly the index of the path in the route cache, secondly the destination ID and finally the delay and the calculated load weight. When data is transmitted from a source node to a destination, the traffic is distributed among multiple routes.
3.4.4 Comparison of multipath routing protocols

A selection was made of these algorithms that could cover the three basic requirements for a route selection in a multipath environment. As seen in Table 3.4, the first one is SMR, a routing algorithm that is based on DSR. SMR chooses the shortest path with the minimum delay and which is maximally disjointed. All the decisions are made from the source node, it establishes two paths for each transmission and new routes are discovered in the case these two paths fail and no more data is possible to be sent through. The next algorithm is AOMDV, a successor of AODV, enabled to send data over to the same destination utilizing multiple paths. AOMDV during the route discovery period searches for routes that either have node or links disjoints so it will not rely on source routing. Decisions are made locally by the intermediate nodes through the route. In case of a failure, a back up route is activated and at the same time a route discovery is initiated. The final contestant is MSR, again a DSR based algorithm that follows a more detailed approach on the route selection. During the route discovery phase, routes are selected only if they satisfy some link reliability requirements. If these QoS requirements are satisfied for a number of routes, then these are selected and data is distributed among them. In case, the reliability level drops below the defined threshold, the route is dropped and a replacement is sought. Loop free routes are ensured from all three algorithms.

<table>
<thead>
<tr>
<th>Base Protocol</th>
<th>Route Discovery</th>
<th>Update Destination</th>
<th>Route choice</th>
<th>Traffic Distribution</th>
<th>Route Maintenance</th>
<th>Hello Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMR</td>
<td>DSR</td>
<td>Shortest delay/disjoint</td>
<td>Source</td>
<td>Source</td>
<td>Two paths</td>
<td>Both paths fail</td>
</tr>
<tr>
<td>AOMDV</td>
<td>AODV</td>
<td>Link/node disjoint path</td>
<td>Neighbor</td>
<td>Intermediate</td>
<td>Single path</td>
<td>Path fail</td>
</tr>
<tr>
<td>MSR</td>
<td>DSR</td>
<td>QoS requirement</td>
<td>Source</td>
<td>Source</td>
<td>Multiple</td>
<td>Limited QoS / Path fail</td>
</tr>
</tbody>
</table>

Table 3.4. Comparison of three multipath protocols

3.5 Channel assignment design strategies

At first we should define the main problem for using multiple radios and channels within a wireless network. For two 802.11 based interfaces to communicate with each other, they need to be assigned to a common channel. Within a multi-radio environment,
where more than one radios are used, there is the problem on how these radios will be coordinated in order to work effectively. However, the number of available channels is limited and as more interfaces within the same interference range are assigned to the same radio channel or a partially overlapping channels, the effective bandwidth available to each interface decreases (Mirchandani et al., 2007a). Therefore, a good channel assignment algorithm needs to effectively balance between the goals of maintaining connectivity and increasing aggregate bandwidth. The problem definition will increase in complexity when we combine the constraints associated with routing and topology control along with the channel selection problem.

### 3.5.1 Background of channel assignment problem

The channel assignment problem has been extensively studied in the context of wireless cellular networks (Katzea and Naghshineh, 1996). The basic concept used was to divide the radio spectrum into a set of non-interfering disjoint radio channels. These channels could then be used simultaneously whilst maintaining an acceptable adjacent channel separation. Various techniques are used to divide the radio spectrum, such as frequency division (FD), time division (TD) and code division (CD).

The minimum distance at which co-channels can be reused with acceptable interference is called the co-channel reuse distance. The co-channel interference (explained in chapter 2) caused by frequency reuse is the most restrictive factor on the cellular system capacity. On the other hand, the channel assignment in wireless 802.11 networks is different. First of all the topology of a wireless multi-hop network is different from that of cellular networks as seen in figure 3.4.
Figure 3.4. The representation of channel reuse in cellular networks

Secondly, channel assignment in wireless multi-hop networks is mainly aiming at minimizing the interference between all the nodes that compose the network within the same spectrum. In cellular networks, channel assignment focuses on the interference between the base stations and the user's mobile device and vice versa. Cellular networks use a technique called frequency hopping (FH) and which rapidly changes frequencies transmissions during radio transmissions with the base station. The main advantage of FH is that it manages to reduce the effect of noise and interference quite successfully (Katzela and Naghshineh, 1996). This technique could be used in ad-hoc networks, however with the current 802.11 standard, the switching time latency is still extremely high (Raniwala and Chiueh, 2004).

3.5.2 Radio interference

The term radio spectrum is broadly used to describe the collection of electromagnetic waves frequencies within the range of approximately 3 Hz to 30 GHz. A radio channel represents the radio spectrum within a limited range, such as a range of 2.47-2.55 GHz.

Various governmental regulatory bodies are created establish policies to control who is using a particular range, when is it used and its purpose. Each country has its own body
and the policies often differ according to the needs and the implication in each country. There are many different bands, and within bands there are different classes of applications such as radio, analogue and digital TV. The regulators determine factors such as transmit power levels, exact frequency range occupied by a particular band. Spectrum regulations are a very complex topic. There are many sources of information available to anyone that would like to find out more about this topic (Nuechterleain and Weiser, 2005).

### 3.5.2.1 Channel interference

Interference is an important factor that influences the ability of two linked nodes to reliably communicate and achieve the desired transmission rate. In the area of 802.11 networks, there are two types of interference that affect the various channel selection algorithms, as presented later in this chapter.

Related to the term interference, there are two terms which should be defined and distinguished, communication range and interference range. The former defines the range in which a reliable transmission between two wireless nodes can take place. The latter is the range in which the transmission between two nodes might be affected by other nodes transmissions which happen to use the same or an overlapping channel. As seen from Figure 3.5, interference range is always larger than the communication range.

![Figure 3.5. Representation of communication and interference ranges.](image)

61
3.5.2.2 Constraints and challenges in channel assignment

Given the interference model and the connectivity graph theory, the main challenge for a channel assignment algorithm (CAA) is, first of all, to assign a frequency channel to each radio in such a way to minimize interference and maximize connectivity among the nodes. Although, apart from it there is a number of challenges (Raniwala et al., 2004) that a CAA should try to satisfy and these are:

- The total number of channels is fixed.
- The number of distinct channels that can be assigned to a wireless node is limited by the number of its radios.
- Two nodes that share a virtual link expected to carry certain amount of traffic should be bound to a common channel.
- The sum of the expected traffic loads on the links that share the same channel and that interference with each other should not exceed the channel’s raw capacity.

Initially, channel assignment seems to be a straightforward problem of graph colouring (Raniwala et al., 2004). However, standard graph colouring cannot capture the above constraints and specifications of the problem (Jensen and Toft, 1995). On the other hand, an edge-colouring formulation fails to capture the second constraint, where no more than the number of radios per node colours can be incident to a node but also cannot entirely satisfy the fourth constraint (Jensen and Toft, 1995).

A key problem in the design of channel assignment for multi-radio ad-hoc and mesh networks is the channel dependency among the logical links that share a common channel. In Figure 3.6 for example, there are six non-overlapping channels available and the links \((a, e)\), \((e, d)\), \((d, i)\) and \((l, h)\) all share the same channel, channel 3. If any of these nodes decides to reassign the channel on these virtual links then the rest have to alter their assignment as well resulting in a ripple effect.
Finally, a CAA should take into consideration the amount of traffic load on the virtual links. It may be assumed that each virtual link in the network has the same traffic load. However this is not always true and particularly some links may hold more traffic than others, for example in Figure 3.6, nodes $a$ and $b$ could play the role of gateway nodes to a wired network (Raniwala et al., 2004).

### 3.6 Taxonomy of existing channel assignments

Channel assignment algorithms in a multi-radio ad-hoc environment consist of assigning channels to the radios in order to achieve efficient channel utilization and also to guarantee a satisfactory level of connectivity. The problem of optimally assigning channels in such a topology has been proven to be NP-hard based on its mapping to a graph colouring theory problem (Garey et al., 1974, Garey and Johnson, 1979). Channel assignment schemes can be generally partitioned into three main categories:

- **Fixed channel assignment** – Specific channels can only be used in designated cells, different groups of channels may be assigned in adjacent channels, and the same group can be assigned to the cells that are outside of the mutual interference range.
- **Dynamic channel assignment** – all channels assignments are temporary and the situation is re-assessed from time to time and the channels are assigned according to certain criteria.
• Hybrid channel assignment – All available channels are divided into two groups. One group is used for fixed channel allocation and the other is used for dynamic allocation.

A more detailed categorization could be based on the locality of the channel assignment process and the strategies deployed. The above general taxonomy is based on the dynamics of the assignment process aiming to provide a better understanding of the algorithms that have been proposed from various researchers Conti et al., 2007.

3.6.1 Fixed channel assignment schemes

Fixed assignment schemes assign channels to radios either permanently or for time intervals that are long enough to supersede radio switching time. Such schemes can be further subdivided into common and varying channel assignments.

3.6.1.1 Common channel assignment

The common channel assignment (CCA) (Draves et al., 1997) is the simplest form of a CAA. Draves et al. proposed an algorithm where the radios of each node are all assigned the same set of channels. The main benefit is that the connectivity of the network is the same as that of a single channel network, while the use of multiple channels increases network throughput. However, the gains may be limited in scenarios where the number of non-overlapping channels is much greater than the number of radios available in each node. This scheme fails to take into account the various factors affecting the performance of a CA resulting in inefficient utilization of the network resources.

3.6.1.2 Centralized channel assignment (C-HYA)

This algorithm is based on the Hyacinth (Raniwala and Chiueh, 2004), a multi-channel wireless mesh network architecture, and is using a centralized channel assignment algorithm (Raniwala et al., 2004). In the proposed algorithm traffic is mainly directed
toward gateway nodes as it travels to/from the Internet. It assigns channels in a way that ensures network connectivity and also satisfies the bandwidth limitations of each link as long as the offered load is known.

Although this scheme integrates connectivity and traffic patterns, the assignment of channels in links may cause a ripple effect as already assigned links have to be revisited. According to the authors’ results, by deploying only two radios per node, an improvement by a factor of 8 of the network goodput is possible, when compared to a single channel network.

### 3.6.1.3 Connected low interference channel assignment (CLICA)

CLICA (Marina and Das, 2005) is a traffic independent channel assignment scheme that computes the priority for each node and assigns channels based on both the connectivity and conflict graphs. The algorithm can override the priority of a node to account for the lack of flexibility in terms of channel assignment and to ensure network connectivity. It should be noted that although the algorithm manages to avoid link revisits, it doesn’t fit in the role of traffic patterns in channel assignment.

![Connectivity graph of CLICA (Marina and Das, 2005)](image)

**Figure 3.7. Connectivity graph of CLICA (Marina and Das, 2005)**

In Figure 3.7, shows the connectivity graph of a network utilizing the CLICA scheme. CLICA is naturally recursive and follows a chain of the least flexible nodes to maintain network connectivity and also once the decision is made upon channel assignment no
changes take place during the algorithm execution. The results show the effectiveness of CLICA through the reduction of interference in the network.

3.6.1.4 Minimum interference channel assignment (MICA)

MICA (Subramanian et al., 2005) is an extension of CLICA and utilizes two new heuristic based algorithms. The first one is based on a popular heuristic search technique called Tabu (Hertz and de Werra, 1997) that was designed for graph colouring problems. The second is a greedy heuristic inspired by the greedy approximation algorithm for Max K-cut (Frieze and Jerrum, 2006) problems in graphs. The Tabu search based method starts with a random assignment. At the same time, the method remembers the best solution seen so far and stops when the maximum number of iterations allowed is reached without a better solution being found. This solution is the best without taking into consideration the interface constraints such as, the total number of channels available at any network node is less than or equal to the number of radios on that node. As a result, the last step in the algorithm is to start from the node with the maximum violations of the interface constraint and combine any assignments of radios that share the same channel and share an edge between them in such way as to minimize the increase in conflicts.

Figure 3.8. The two phases of MICA using Tabu search
Figure 3.8 shows the merge operation and its output before and after the second phase. On the left figure, *i* stands for the node picked for the merge operation. The number of colours incident on *i* is reduced by picking two colours *C3* and *C2* that are incident of *i* and changing the colour of all *C3* coloured links to *C2*. In order to ensure that this change does not create interface constraints violations on other nodes, the change will iteratively propagate to all *C3* coloured links that are connected to the links whose colour has been changed from *C1* to *C2*. The above propagation of colour change ensures that for any node *j* either all or none of the *C3* coloured links incident on *j* are changed to colour *C2*. Once the second phase is completed, the merge should look like in Figure 3.8(b).

### 3.6.1.5 Traffic and interference aware channel assignment (MesTic)

The last examined CAA in the area of the fixed channel schemes is MesTic and stands for Mesh based Traffic and Interference aware Channel assignment (Skalli et al., 2007). It is a fixed, rank based polynomial time greedy algorithm for centralized channel assignment that visits nodes once in the decreasing order of their rank. The rank of each node *R* is computed on the basis of its link traffic characteristics, topological properties and number of radios on a node according to equation 2.

\[
R\left(\text{node}\right) = \frac{\text{Aggregate traffic (node)}}{\text{min hops from gateway (node) } \times \text{number of radios (node)}}
\]  

(2)

From equation 2 it can be seen that the aggregate traffic flowing through a mesh node has an impact on the channel assignment approach. The principle is that if a node relays more traffic, assigning it a channel of least interference will increase the network performance, such as the throughput, and also increases the rank of the node. The number of radios on a node gives flexibility in channel assignments and should inversely affect its priority, for example, less radios available, higher the priority in channel assignment.
Simulation results have shown that MesTiC performs better than other CAA for various topologies and traffic profiles (Skalli et al., 2006). There are some drawbacks though with this scheme related to the use of common channel. Such an operation can increase the interference between the nodes and also consumes valuable bandwidth and it increases the complexity of the scheme. At the same time might force the algorithm to assign the rest of the nodes with channels that are more susceptible to co-channel interference. Also, more nodes within the network might require the use of more channels and consequently more radios installed on the nodes.

### 3.6.2 Dynamic channel assignment schemes

In contrary to fixed, dynamic channel assignment strategies allow any radio to be assigned any channel but also radio can frequently switch from one channel to another. When nodes need to communicate with each other, a coordination mechanism is usually used in order to ensure that they are listening on the same channel. For example, such a mechanism might ask from all nodes to visit a predetermined channel periodically to negotiate channels for the next phase of transmissions (So and Vaidya, 2004). More focus is given in this category of CAA the idea described in this thesis is strongly related to the proposal of a dynamic channel assignment scheme.

#### 3.6.2.1 Slotted seeded channel hopping (SSCH)

In SSCH mechanism (Bahl et al., 2004), the algorithm uses a pseudo-random sequence where each node should switch channels synchronously in this random sequence so that all neighbours meet periodically in the same channel. In this approach the interfaces must be capable of fast synchronous channel switching. Specifically, time is divided into slots and the channels are switched at the beginning of each slot according to the following equation.

\[
\text{New Channel} = (\text{Old Channel} + \text{Seed}) \mod (\text{Number of Channels}) \quad (3)
\]

Although it is a simple approach which avoids complex mechanisms in channel allocation, it lacks into two aspects. First of all, all nodes should switch to a certain
channel in order to communicate with each other, arrange the channels for each node and then continue with their transmissions. Although the authors point out that the nodes should be able to fast switching, in 802.11, channel switching takes place in 80\mu sec (Wu et al., 2000). This process would increase the average delay of the network over time and for long lasting transmissions. The second aspect is that it doesn’t take into consideration the interference that might be present from external resources. In such case some nodes might delay during their switching process and as a result the switching in overall might not succeed leading to absences of transmissions.

3.6.2.2 Distributed channel assignment scheme (D-HYA)

A set of dynamic and distributed channel assignment algorithms was proposed in (Raniwala and Chiueh, 2004). These algorithms can react to traffic loads changes in order to improve the aggregate throughput and achieve load balancing. Based on the Hyacinth architecture (Raniwala et al., 2004), the algorithm builds on a spanning tree network topology. The algorithm works in such a way that each gateway node is the root of a spanning tree and every mesh node belongs to one of these trees. The channel assignment problem consists of two main steps, the neighbour-to-interface binding and interface-to-channel binding.

In neighbour-to-interface binding, the node selects the radio to communicate with every node, dependency among the nodes is eliminated to prevent ripple effects in the network (Raniwala et al., 2004). This is achieved by imposing a restriction to the set of the radios a node uses to communicate with its parent node. On the other hand, in interface-to-channel binding where the node selects the channel to assign to every radio, the goal is to balance the load among the nodes and relieve interference.

There are three main disadvantages to this approach. The first one is the tree topology constraint of the scheme, which poses a potential difficulty in controlling multi-path routing in mesh networks. The second disadvantage is the usage of a common channel on each node for the management of channel assignment. This approach wastes bandwidth and sets severe limitations on network capacity especially when nodes have only two interfaces (Prodan and Mirchandani, 2009). Finally the third constraint is that
the common channel can be considered as a strong source of interference on the frequency that is used for the co-ordination of channels, partially or completely affecting thus the throughput of the network.

In 2007, Raniwala and Chiueh presented an improved version of the above proposal (Raniwala and Chiueh, 2007) considering a combined solution for the channel assignment and routing issues discussed above by incorporating the usage of a virtual control network instead of a dedicated interface-channel on each router. Their work contains careful analysis of all aspects of resource allocation problems relevant to 802.11 based mesh networks, although they still do not manage to overcome the rest of the problems from their previous proposal (Raniwala and Chiueh, 2004).

3.6.2.3 Other dynamic channel assignment schemes

The work of Ko et al. (Ko et al., 2007) specifically deals with the channel assignment problem on wireless mesh networks. The authors have adopted their theoretical work in one of their previous approaches (Ko and Rubenstein, 2003) and created a self-stabilising distributed protocol and an algorithm for channel assignment. Their method assumes that the interference is symmetric and is based on an interference range of three hops and results in improvement of only 20% compared to random channel assignment (Ko et al., 2007). In reality most of the times interference will be asymmetric because neighbouring node interface might transmit on the same channel at different powers. In contrast a better proposal would not assume symmetric interference and would not require a dedicated channel for frequency co-ordination, which is a significant advantage. Also the interference cost function (Ko et al., 2005) has not been justified as it has not been based on an interference model. Another limitation of the proposal as in (Raniwala and Chiueh, 2004) is the usage of an extra common channel for channel assignment management.

In (Jain et al., 2003) authors state that the addition of new nodes can actually improve a per-node throughput because the richer connectivity provides increased opportunities for routing around interference hotspots in the network that offsets the increase in traffic load caused by the new nodes. No assumptions were made about the homogeneity of
nodes in relation to radio range or other characteristics as well as regularity in communication patterns.

The conclusion from this work (Jain et al., 2003) was that neither multi-path routing nor doubling the range of the radio increases cumulative throughput. On the other hand, by using two channels instead of one, the network may achieve the maximum possible throughput. In realistic conditions we cannot simply obtain information that has to be fed into the proposed model and the capacity predicted by the model.

In another approach (Leung and Kim, 2003), Leung and Kim have deployed heuristics that is based on interference measurements, although they do not define a threshold value range and a mechanism to keep a channel change under control. This could result in an infinite loop of channel changes that is caused by a slight disparity in noise or by cyclical interference.

The use of partially overlapping channels has been proposed (Subramanian et al., 2005) with the interference model to be theoretically based on a conflict graph and the interference data is acquired through the measurement of link pair interference.

3.6.3 Hybrid channel assignment schemes

Hybrid channel assignment strategies combine both statistic and dynamic assignment properties by applying a fixed assignment for some radios and a dynamic assignment for other radios. Regarding the fixed radios, they are classified based on whether the fixed radios use a common channel or a varying channel approach. The fixed radios can be assigned a dedicated control channel or a data and control channel, whereas the rest of the radios can be switched dynamically among channels (Conti et al., 2007). Generally hybrid assignments are quite attractive because, as with fixed assignment, they allow for simple coordination algorithm while still retaining the flexibility of dynamic channel assignment.
3.6.3.1 Link layer protocol for radio assignment (LLP)

An innovative link layer radio assignment algorithm was proposed (Kyasamur and Vaidya, 2005a) that categorises available radios into fixed (F) and switchable (S). Fixed radios are assigned for long term intervals specific fixed channels, which can be different for different nodes. On the other hand, switchable radios can be switched over short time ranges among the non-fixed channels based on the amount of data traffic. By distributing fixed radios of different nodes on different channels, all channels can be used while the switchable radios can be used to maintain connectivity as shown in Figure 3.9.

Two coordination protocols were proposed in order to decide which channels should be assigned to the fixed radio. The first one is a function that generates a hash based on the node identifier to select which channel to assign to the fixed radio. The second protocol is by exchanging Hello packets that contain information on the fixed channel used by a node. Based on the received Hello packets, nodes may choose to set their fixed channel to an unused or lightly loaded channel.

![Figure 3.9. LLP in operation (Kyasamur and Vaidya, 2005a)](image)

However, this work was extended (Kyasamur and Vaidya, 2006) by using the second protocol described above (Hello packets) and the authors implemented a hybrid channel assignment scheme. The main benefit of this CA scheme is that it is fairly insensitive to radio switching delay and selects routes that have low switching and diversity cost. On the other hand, the assignment of fixed channels has to be carefully balanced in order to achieve a good performance.
3.6.3.2 Interference –aware channel assignment (BFS-CA)

In this proposal, it was addressed the problem of channel assignment in WMNs in the presence of interference from collocated wireless networks (Ramachandran et al., 2006). The authors suggest a dynamic centralised interference-aware algorithm aimed at improving the capacity of the WMN backbone and at minimising interference. To compensate for the weaknesses of a dynamic network topology, the proposed solution assigns one radio on each node to operate on a default common channel throughout the network. This ensures a common connectivity graph and at the same time provides alternate fallback routes and avoids flow disruption by traffic redirection over a default channel.

This method is incomplete since it neglects interference caused by transmissions that are too weak for the signal to be decoded but still result with degradation of the Signal to Noise Ratio (SNR) on a particular link. The other main drawback of this approach is the scalability since centralized algorithms are used. However it prompts for further investigation since it indicates a 40% performance gain (Ramachandran et al., 2006) in comparison to static assignment.

3.6.4 Comparison of channel assignment schemes

The key issues for the majority of the CAA presented in this chapter are connectivity, topology control, interference minimisation and traffic pattern. To begin with, C-HYA is a centralised, traffic-aware fixed channel allocation scheme. While its distributed version, D-HYA, improves the effect of link revisits, inflexible restrictions were imposed on the topology of the network and therefore, fail to leverage the benefits of multi-path routing in a mesh network. MesTiC is a fixed centralised scheme that in the way as C-HYA and D-HYA, takes traffic load information into account without imposing any strong constraints on the topology. Additionally, it is a greedy algorithm that does not suffer from ripple effects and ensures connectivity via a default radio. On the other hand this common radio for communication between the nodes can create more severe problems than it can solve, such as interference.
LLP and CLICA, even though tried to minimise interference, the effect of traffic patterns on interference was not taken into account. On the other hand, in BFS-CA, it was taken into consideration but only for traffic originating from external wireless networks. Regarding topology control, some algorithms such as CLICA and MICA considered the issue that such a mechanism incurs overheads in the CAA but alleviates the need for an extra radio tuned into a common channel. On the contrary, BFS-CA and MesTiC assume default connectivity by using a separate common channel on a separate radio. Table 3.5 summarises and compares the primary attributes associated with the key CA algorithms presented in this chapter.

<table>
<thead>
<tr>
<th>Proposal Attributes</th>
<th>Raniwala et al., 2004</th>
<th>Ko et al., 2007</th>
<th>Ramachandran et al., 2006</th>
<th>Subramanian et al., 2005</th>
<th>Bahl et al., 2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Algorithm</td>
<td>Distributed and/or Centralised</td>
<td>Self organizing</td>
<td>Hybrid</td>
<td>Hybrid</td>
<td>Dynamic</td>
</tr>
<tr>
<td>Parameters</td>
<td>Interference + Load</td>
<td>Interference</td>
<td>Interference</td>
<td>Interference</td>
<td>Interference</td>
</tr>
<tr>
<td>Dedicated channel</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-orthogonal channels</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Transmmit Power Control</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Scalability</td>
<td>Addressed</td>
<td>Addressed</td>
<td>Not addressed</td>
<td>Partially addressed</td>
<td>Not addressed</td>
</tr>
<tr>
<td>Stability</td>
<td>Not addressed</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Capacity Analysis</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td>Yes</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
</tbody>
</table>

Table 3.5. Comparison of various channel assignment algorithms

## 3.7 Conclusion

Routing is an essential component of communication protocols in ad-hoc networks. The design of the protocols are driven by specific goals and requirements based on particular assumptions about the network properties or application area. In this chapter there was an introduction to routing in networks by presenting the two main categories, distance vector and link state. The main difference between these two lies to the
initiatives that exist during the routing decision as one is based on the distance between the source and the destination and the other one, the link state, disregards the necessity of discovering the shortest route but tries to find the most stable with the minimum delay route, giving great focus on the Quality of Service.

Finding the best possible route in order to transfer data from one node to the other is not always sufficient. In the cases of networks where the nodes operate using a common channel, they suffer from low bandwidth links and often collisions because of the co-channel interference that is created from the common frequency channel. Researchers designed and implemented mechanisms so that the nodes could have one or more radios installed and each one would be able to utilise one or more channels. Such a technique made things more complicated and demanded for the existence of new algorithms to assign the channels to the radios in such a way to guarantee fast and reliable transmissions by minimizing interference.

In the next chapter analyses the idea that this research has proposed. There is an investigation of the needs and the requirements the proposed idea has to serve and what is the best possible solution, according to the author of this work, which can lead to the implementation of such a network by using the appropriate routing protocol incorporated with an efficient and fully cooperative channel assignment algorithm.
4 Reducing CCI Using Segregate Networks

4.1 Introduction

This chapter presents our proposal on wireless ad-hoc network deployed within an industrial environment. One can draw similarities between the system presented here and others presented during the last years (Kumar and Gupta, 2000). The main similarity is the attempt to use multiple wireless channels with multiple radios in order to take advantage of the full spectrum available for 802.11b networks. This translates to the fact that, inside the network the channels used are not non-overlapping but on the contrary they overlap with each other. In the first case the interference that appears inside the network is mainly caused by nodes that operate on exactly the same channel as the rest, the so called co-channel interference. When nodes do not operate on the same channels but in channels that overlap in the spectrum map, the interference produced is called adjacent interference. This chapter will focus on this concept and introduces the network segregation, the division of the network into cells or to be more accurate into subnetworks. The term division does not mean that the network will be physically separated so the static nodes for each subnetwork will be distinguished from all the rest, but actually that the network will be divided into smaller networks setting as criteria the frequency channels that are utilised within each of them. At that point any similarities with previous proposals cease to exist and the steps that are taken to configure the network differ significantly, providing a simpler method and overcoming any technical difficulties and/or complexities.

The literature in the area of multi-channel networks and channel assignment schemes presented solutions to focus on ways to overcome co-channel and adjacent channel interference, as some covered in the previous chapter. The goal of all these proposals is how efficiently the spectrum of 802.11 networks can be better utilised to implement networks with high throughput, low delay and reliable connections between the wireless nodes. One of the differences of the ideas presented in this and the next chapter is the focus that is given to the existence of interference from external sources and can come in the form of thermal and/or ambient noise apart from the interference produced from neighbouring nodes. External sources such as wireless devices often happen to
operate in the same frequencies as an 802.11 network. Although these devices might be placed far from the wireless nodes, the range of their interference can reach the transmission range of a wireless transmitter. These parameters, interference and noise, are very common in industrial environments, such as warehouses oil plants or other areas with metal constructions and thick walls, places well known for their harshness to any form of wireless communication.

The difference between industrial and typical domestic environments is first of all the topology of the network. As domestic ones are mainly implemented in infrastructure mode with limited number of nodes, industrial ones require much larger number of nodes operating into an ad-hoc way and covering larger physical areas. Consequently, more the nodes that operate in a network, stronger the interference produced. There are certain simple steps that could be taken to help reducing to certain extend the problems of co-channel and adjacent channel interference in industrial networks where the density of the wireless nodes is much greater. This chapter sets he basis for the characteristics of the network architecture proposed and upon them a channel assignment algorithm utilising multiple channels and enabling data to travel through multi-hop routes was designed and developed.

4.2 Constraints of network segregation

Network segregation implies the use of multiple overlapping or non-overlapping channels within the network. Using more than one channel in a wireless network requires certain criteria to be met in order to alleviate the negative effects of co-channel or adjacent interference. Network segregation has nothing to do with wireless networks operating into infrastructure mode where access points coordinates the channel decisions of the clients. On the contrary it describes the channel selection procedure that can be taken inside an ad-hoc network in order to improve its behaviour by reducing interference between its nodes. The following sections identify the key problems that exist within a wireless network when deploying multiple channels. They are set as the starting points for the configuration of the enterprise wide network presented later in the chapter. One of the main differences of our proposed network is
that it extends the use of adjacent channels from small scale networks to larger ones with multiple nodes.

4.2.1 The problem of co-channel interference

Consider the scenario of an 802.11 wireless network, consisting of 100 nodes and covering an area of 500x500 meters with all the nodes operating on a common channel. This network is placed in an industrial area with various metal constructions and buildings with thick walls. The wireless nodes are placed randomly within the area some of which are located inside buildings or next to the metal constructions. This network has to play the role of a backbone network transferring data from experiments and measurements, from one side of the plant to a specific location that is located on the other side, for storage and analysis. Since all the nodes operate on the same frequency channel, the routing algorithm sets up the most appropriate route for the transmission to begin. In most cases the physical distance between the starting nodes and the destination nodes is larger than the transmission range, therefore the destination data has to be passed through indirect intermediate nodes. The first node communicates with one of its neighbours as defined by the routing algorithm and the same process is repeated until it reached the destination and all data packets are transmitted successfully (Perkins and Royer, 1999).

During all this process, each time a node transmits to its neighbours, all the nodes that are within its transmission range would not be able to establish any possible connections as the only channel available is occupied. In the best scenario, if the transmission time is short, the neighbouring nodes will be able to use the channel shortly afterwards. The worst scenario is for larger packets where nodes might end up waiting for a longer time before being able to initialise any transmissions. In this case, the 802.11 mechanism of Distributed Coordination Function (DCF) (Mishra et al., 2006) is enforced in order to establish fairness between the transmitting nodes. Nodes wait for an amount of time, the back-off period, and then attempt to transmit again only if the medium, channel, is available.
Although this process brings some balance within the network so all the nodes can transmit almost simultaneously, in the case of large scale networks, it increases significantly the overall delay and reduces throughput. Apart from that since only one channel is being used for transmissions, the remaining bandwidth of the 802.11 spectrum remains unusable. To increase the utilisation of the spectrum, more than one channel within the network has to be deployed. These channels could either be non-overlapping or overlapping channels. The benefits and problems of this are explained in the next section.

4.2.2 Effectiveness of RTS/CTS in single channel networks

In the case of an 802.11 network that uses a single channel for transmission, it has been shown (Xu et al., 2002) that RTS/CTS handshake does not perform as efficiently as it is supposed to. RTS/CTS has an underlying assumption that all hidden nodes are within the transmission range of the receivers. According to Xu’s study, such an assumption might not hold when the distance between the transmitter and the receiver exceeds a certain value. Some nodes that are out of the transmission range of both the transmitter and the receiver may still interfere with the receiver. This phenomenon is quite rare in a wireless network operating in infrastructure mode but in the case of an ad-hoc network, it becomes a serious problem due to the large distribution of nodes and the multi-hop operation. According to the results of the above study, it has been proved that for the open space environment, the interference range of a receiver is 1.78 times the distance between the transmitter and the receiver. Such an assumption implies that RTS/CTS handshake cannot function well when the transmitter-receiver distance is larger than 0.56 (equal to 1/1.78) times the transmission range. For large interference ranges encountered in ad-hoc networks, this is a serious problem and can affect the network capacity as well as the network performance significantly (Gummadi et al, 2007).

In wireless communications there are three different ranges:

- **Transmission Range** \( (R_{tx}) \) – it represents the range within which a packet is successfully received if there is no interference from other radios.
transmission range is mainly determined by transmission power and radio propagation properties such as attenuation.

- **Carrier Sensing Range** ($R_{cs}$) – it is the range within which a transmitter triggers a carrier sense detection. This is usually determined by the antenna sensitivity.

- **Interference Range** ($R_i$) – it is the range within which stations in receive mode will be interfered by an unrelated transmitter resulting in loss of communication.

Nodes within the interference range of a receiver are usually called hidden nodes. When the receiver is receiving a packet, if a hidden node starts a transmission at the same time, a collision will happen at the receiver. As a signal is propagated from a transmitter to a receiver, whether the signal is accepted at the receiver largely depends on the receiving power. Given the transmission power, the receiving power is mostly decided by the path loss over the distance between the transmitter and the receiver. In an open space environment, path loss of a signal is usually modelled as the two-ray ground model. Assuming that $d$ is the distance between the transmitter and the receiver, when this distance is small, within the Fresnel zone (Rappaport, 2002), the receiving signal power is inversely proportional to $d^2$. When $d$ is larger, outside the Fresnel zone, the receiving signal power is inversely proportional to $d^4$. The receiving power of a signal at the receiver can be expressed as:

$$P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4}$$  \hspace{1cm} (4)

Where, $P_t$ is the transmission power, $G_t$ and $G_r$ are the antenna gains of transmitter and receiver respectively and $h_t$ and $h_r$ are the antenna heights. Assuming that all nodes have the same configuration, a signal will be accepted by the receiver if the Signal to Noise Ratio (SNR) is above a certain threshold, called SNR_THRESHOLD. Let $P_i$ be the power of interference from a node that is $r$ meters away from the receiver, the SNR will be expresses as:
\[
SNR = \frac{P_o}{P_i} = \left( \frac{r}{d} \right)^4 \geq SNR\_THRESHOLD
\]  

(5)

Therefore \( r \) can be deduced as follows:

\[
r \geq \frac{1}{4} \sqrt[4]{SNR\_THRESHOLD} \cdot d
\]  

(6)

Equation 6 implies that to successfully receive the signal from the transmitter, any interfering nodes should be \( r \) meters away from receiver and this is defined as the interference range \( R_i \) of the receiver. Authors of (Xu et al., 2002) stated that usually \( SNR\_THRESHOLD \) is equal to 10 yielding to an interference range equal to 1.78 times the distance \( d \). To conclude, when \( d \) is larger than the range of the transmitter, interference range overcomes \( R_i \) and thus the power needed to interrupt a transmission is much smaller than the power needed to successfully deliver a packet. In infrastructure mode it is easier to coordinate the communication of the clients with an access point as the number of the clients is relatively small. On the hand, in an ad-hoc mode, the number of the nodes is much larger, which means more interfering nodes. The process to overcome problems of collisions using the traditional RTS/CTS method becomes a very complex task.

Researchers identified this problem of RTS/CTS and suggested multiple channels to be used within ad-hoc networks. This has reduced the amounts of interference since transmissions are carried out over different frequency channels, however the new challenge was which channels to use. Should they use non-overlapping or adjacent channels? The very same dilemma came into consideration when designing the idea of segregated networks and the decision to go with the concept of multiple adjacent channels is explained in the next section.
4.2.3 Adjacent channel interference

As explained in chapter 2, there are numerous wireless protocols that are currently used in industrial wireless networks offer very low bandwidth and small transmission range, apart from 802.11, so they cannot be used for deploying a high capacity industrial network. By excluding all these “slow” transmission technologies, 802.11 was the only feasible standard. The next step was to identify which of the two basic 802.11 protocols could be used, either 802.11a or 802.11b. The neighbouring channels in the 802.11a standards are organise as shown in Figure 4.1.

![Figure 4.1. Non overlapping channels of 802.11a (IEEE 802.11a, 2003)](image)

The channels in 802.11a do not overlap with each other and for example channel 1, 6 and 11 could be used in a multi-channel wireless network without any interference disruptions during their simultaneous operation even when their transmission range $R_n$ overlap. These channels are called non-overlapping channels. On the other hand, in the 802.11b standard channels are organised as shown in Figure 4.2.
In 802.11b there are three overlapping channels, which when utilised inside a wireless network would not create interference with each other. In contrast, channels 1 and 3 partially overlap and the implication of such construction is that simultaneous transmissions on these two channels within close physical proximity will cause interference. Such channels are called partially overlapping channels or adjacent channels. When two nodes operate on adjacent channels and are in close proximity, they cause a level of interference, which is called adjacent channel interference. The effects of adjacent interference when compared to co-channel interference are much lesser because channels do not overlap completely but only partially. Of course the level of adjacent interference between two transmitting nodes depends on the amount of overlapping within the frequency domain between the two channels.

The co-channel interference in networks with a single channel can be directly detected and handled up to a point through contention resolution mechanisms such as the RTS/CTS handshake explained previously in the chapter. In the case of adjacent channel interference, it often contributes to background noise and cannot be handled in an explicit manner by a channel contention technique. Due to the detrimental effects of such type of interference, the majority of previous attempts (Raniwala et al., 2004, So and Vaidya, 2005a,) on channel assignment techniques, as discussed in chapter 3, used only non-overlapping channels. Many of them (Alicherry et al., 2005, Kodialam
and Nandagopal, 2005) defined a frequency channel similar to a path of information flow that is perfectly isolated from other paths.

Before proceeding further to the analysis and presentation of the proposed segregated network and its architecture, there were still three questions that had to be answered and would influence the development of this network. The first one is related to channel spacing and specifically how far apart should usable channels be spaced in the frequency domain given that each channel in a specific technology occupies a fixed bandwidth. To answer this question we had first to examine the relationship between the energy of a transmitted signal and the information capacity of a wireless channel. While the exact nature of this relationship depends on the precise choice of physical layer modulation scheme, it is essential to consider the upper bound on information capacity of a wireless channel as it is defined by Shannon in equation 7.

\[
C = B \log_2 (1 + SNR)
\]

In the above equation, \(C\) is the data capacity, \(B\) is the channel bandwidth and \(SNR\) is the signal to noise ratio. As the signal energy increases, the values of \(SNR\) increases and consequently so does \(C\). Each wireless technology defines precise limits on the transmitter’s output power for each frequency within its channels. Therefore, to achieve maximum utilisation of the capacity of a given channel within the transmit power bound, a transmitter should emit the maximum permitted power in all frequencies of the channel. The transmit spectrum mask that is used by the transmitter to limit the output level on different frequencies will require to emulate an ideal band-pass filter. In such an ideal mechanism, neighbouring channels would be non-overlapping and thus no interference between the various channels (Mishra et al., 2005b). The only constraint to this achievement is that the design of such ideal transmit mask is not possible in practice. In more realistic scenarios, transmit masks are not ideal and the best possible output they can give is similar to that of Figure 4.1, which implies that capacities are lower in this case as it would be in an ideal transmit mask.

The second question was related to non-overlapping channels and how efficiently they could utilise the spectrum when only such channels were used. The answer to this
question was pretty easy, as it is obvious from Figure 4.1 that the use of non-overlapping channels only, actually is a waste of bandwidth and subsequently waste of capacity. According to Shannon’s theorem and equation 7, non-overlapped channels and the practical limits on the shape of transmit spectrum masks imply that there are many frequencies in which the transmitted power is lower than the maximum permitted limit that decreases \( SNR \) and hence the maximising the capacity (Mishra et al., 2006).

Since the spectrum cannot be utilised to the maximum from non-overlapping channels, the last question focused on the ability of adjacent/partially overlapping channels to achieve a much better utilisation. This third issue was taken into consideration and proved to be the basis for the proposed idea of this thesis and required further investigation through experiments, which are presented in Chapter 5, to identify if the use of partially overlapping channels could actually achieve better performance within ad-hoc wireless network. There has been very limited work on this idea (Mishra et al., 2005b, Mishra et al., 2006); the known ones mainly concentrate on wireless networks operating in infrastructure mode, examining the problems of interference between access points and clients. There are references on wireless mesh networks regarding link’s capacity when overlapping and non-overlapping channels are used and they mainly focus on small scale networks. The experiments performed did not quite apply to a generic approach but on the other hand it specialised on specific hardware and modulation techniques. The work presented next in the chapter focuses only on ad-hoc networks, as infrastructure networks have been proven less capable due to their operational and configuration characteristics, using a more generic hardware, which is commercially available. It excludes certain hardware parameters that could lead to acquiring experimental results that would not be eligible for a broader application in various scenarios and topologies. Last but not least, the characteristic that cannot be found in the majority of related work is the effect of the environmental noise, which can appear in the form of background noise including both ambient and thermal noise, to the overall performance of the network. More information about noise can be found in chapter 4 (4.4.4).
4.3 Network segregation and its benefits

Summing up the above mentioned constraints of network segregation, it was shown in theory that network segregation is definitely feasible but is accompanied with some serious considerations. As mentioned at the beginning of the chapter, the proposed network architecture is a wireless network with nodes operating in ad-hoc mode and these nodes are responsible to transfer larger volumes of data in a fast and reliable, with the minimum possible link failures, way from one side of an industrial factory to the other.

4.3.1 Mission and physical characteristics of the segregated network

Consider a large area made from buildings, metal constructions and thick walls separating dangerous areas from human access. Inside this area there are machinery and testing equipment that measures various parameters of the tasks that take place inside the area. This machinery is mainly sensors that gather information from various functions such as temperature and all the information that is generated has to be gathered and send over to a specific area, a storage computing facility for example. At the facility data will be collected, stored and analysed according to the needs of the company. The first clarification to be made is that the proposed network does not include of wired or wireless sensors responsible for data collection so it is not considered to be a wireless sensor network (WSN), although it can be used as an intermediate platform for a WSN. Secondly, the storage and the analysis of the data is also not part of this research and thus are not investigated.

Out of these two clarifications, the only part left is actually the basic mission of the proposed network, the transfer of the collected data until a certain point just before the storage facility. The collected data from the sensors is transferred to some temporary storage equipment called cubicles until its transmission through the 802.11 network. These cubicles are equipped with wireless radios and once data starts to arrive from the sensors or any other possible source, the transmission triggers. It should be noted that the flow of data once the sensors start collecting are continuous, and the amount of the data produced depends on the number of sensors activated during the probable execution of an operation or experiment. That is why two scenarios were taken into
consideration during the testing phase of the proposed network and the associated algorithms, a light load scenario and a heavy load scenario, where the high load scenario is actually twice the light load.

The proposed segregate network is composed of 802.11b nodes operating at a speed of 11Mbps in ad-hoc mode, so every node is able to listen and communicate with one or more neighbouring nodes. During the network testing, nodes are placed in a random manner over the area in an attempt mainly to provide better coverage of the area and nodes. Another reason is that the nodes which operate on the same frequency channel are equally distributed within the industrial area in an attempt to minimise co-channel interference due to low density. Because of these two characteristics, it is possible to produce a more generic approach regarding network topology and at the same time avoid the essence of performing a Radio Frequency (RF) site survey, something that would restrict possible future deployment areas of the network.

4.3.2 Operational characteristics of the segregated network

The idea of network segregation is not something new in the area of computer networks. Network segregation is related to network security and up to now it was used as a mechanism of controlling the security of large networks by dividing them into separate logical network domains. In WLAN, network segregation provides a way to separate the “untrusted” WLANs from the more “trusted” portions. WLANs usually are connected to a wired network at some point to facilitate Internet or Intranet communications, and the convergence of these networks should be separated by a gateway so that wireless communications are not required to traverse the wired network unless necessary. Segregating the network will lessen the burden of security controls in areas with open access requirements and high tolerance for downtime, yet will strengthen security for those areas that need additional protection and high availability. Getting the idea from wired/wireless network security, we applied it to wireless ad-hoc networks aiming to achieve simultaneous multiple independent transmissions.

There are some particular operating characteristics that are followed all along the experiments that are presented in this and the next chapter and are kept unchanged to
provide the most accurate results. Any change to one these characteristics would alter the behaviour of the network either in a positive or a negative way. It should be noted that the same concept applies to the physical characteristics of the network. The number of wireless nodes inside the network varies from scenario to scenario.

In every network, there are a number of nodes who are called the side nodes and all the traffic is sourced from them. To be more specific, the data starts to be transmitted from one side of the network and the receivers are placed on the other side so data travels through the intermediate nodes, following a particular route that is decided by a routing protocol. The number of the side nodes depends from the amount of data that has to be sent, light or high load, and also on the number of the channels that are utilised within the segregate network. In reality the side nodes are wireless enabled cubicles, which always to listen to all the channels that might happen to be used in each scenario. To achieve this, the number of radio interfaces they are equipped with, equals to the number of channels they have to listen to. Another characteristic of the side nodes is that they can transmit to two or more subnetworks simultaneously, since they are equipped with multiple radio interfaces. To better understand the network segregation, Figure 4.3 represents graphically as produced from the simulator, the GlomoSim (UCLA, 1999), the placement of the nodes within the simulated area. It should be clarified once more that nodes aren’t physically separated in groups but actually within a unit area there might exist nodes from all the existing subnetworks.

Figure 4.3. A three segregated network utilising 3 channels
In Figure 4.3, there are 24 nodes listening to a single channel, they are segregated into 3 groups and each one operates under a different channel. The role of the side nodes is assigned to nodes with addresses 0 and 23. Data is sent from node 0, travels through one or more subnetworks until they reach destination node 23. All nodes are stationary and the selection of their operating channel is done randomly. To operate fairly the nodes are evenly distributed among the existing subnetworks, although some can dynamically swap channels depending on the traffic constraints in the system. For example in Figure 4.3, there are 7 nodes operating in channel $C_0$, another 7 in channel $C_2$ and finally 8 nodes operate in $C_1$. This rule should never be broken as it ensures the equality between the subnetworks in terms of available routes and total amount of adjacent interference.

The power of transmission for every node is considered to be the same so each node produces the same amount of interference. In single channel networks, if there are two pairs of nodes and their transmission ranges overlap, the first pair’s transmission collides with the other pair’s since each one’s range of transmitted power acts as interference to the other pair.

### 4.3.3 Features of network segregation

There are numerous benefits in network segregation and these are based mainly on two important features, the ability to utilise multiple channels and these channels could either be non-overlapping or partially overlapping. The benefits are:

- Co-channel interference is minimised as multiple channels are used within the network. In this case the amount of interference is less as the number of nodes operating on the same channel is also reduced.

- The segregation provides multiple routes for data transmission, as each subnetwork can form its own routing table and maintain their independence from the rest of the subnetworks. This is useful for harsh environments, when multiple copies of the same data are required, to overcome external interference.
The network by using partially overlapping channels avoids the waste of the available bandwidth in the 802.11 spectrum, increasing the overall throughput.

Simultaneous transmissions can take place because of the independency of the subnetworks and their availability in routes, increasing the overall capacity of the network.

The minimisation of interference provides more reliable links between the nodes resulting to less collisions/retransmissions, shorter paths to the destination and less end-to-end delay.

The multiple routes can also be used in cases of data duplication aiming to reliable transmissions with no loss of data. Data aggregation can also be achieved by utilising special mechanisms in an attempt to minimise load on certain links.

The next section, describes the results of the simulations to demonstrate the usefulness of network segregation without the consideration of any special channel assignment algorithm. The maximum number of channels utilised within the simulations were set to 5. The reason for this limitation is that the given transmission range of the deployed nodes in the simulations, any further segregation of the network will decrease the density of the nodes for each subnetwork. This decrease in density and in relation to their transmission range, nodes are too far apart from each other, resulting in loss of connectivity and no transmissions can be performed.


Up to this point, we have analysed the design process of network segregation and the theoretical benefits derived from it. The rest of the chapter focuses on scenarios that prove in practice the benefits of network segregation compared to other proposed architectures from the literature. The selection of AODV as the routing algorithm is also explained and justified. The comparing metrics used for the results were the average end-to-end delay of the network, the average throughput, the average delivery ratio of
transmitted packets and the number of retransmissions that happened to occur during these experiments. Later in the experiments, the presence of background noise in the form of ambient or thermal noise, which is not considered in most of the related works, is introduced into the simulation model and its impact on the performance of segregate networks is analysed.

4.4.1 Selection of the routing algorithm

As discussed in chapter 3, there are numerous algorithms for ad-hoc networks and each has its advantages and disadvantages. Ad-hoc networks are mainly related to mobile wireless nodes and their performance is evaluated on the ability to overcome the problems that might appear from this feature. The network architecture proposed and evaluated in this thesis does not include any mobility as it is not relevant to the operational environment of this work. So the selection of the appropriate protocol is based on its performance to the environment of a segregate network. The target of this work is to select one of the basic routing protocols and tune it to the needs of network segregation by enriching it with a new channel assignment mechanism to improve its behaviour in a multi-channel environment. The candidates for the most appropriate routing algorithm were a mix of reactive, proactive and hybrid protocols, in an attempt to include as many options as possible.

The network configuration included various numbers of nodes, ranging between 10 and 200 because this work focuses on medium scale nodes and any more nodes would not be useful to be included. The size of the simulated area, 200x200 meters, was also selected to represent the size of a medium scale network. All nodes operated on the same channel and the experimenting area was kept the same in order to be able to examine the behaviour of the available routing algorithms in a single channel multi-hop network, for variable number of hops in each scenario. At this point, it should be pointed out that as the number of nodes increased the transmission power and consequently the transmission range was decreased. In this way, the routing algorithms were forced to change the routing path and include new and more nodes in their routing path. Otherwise if the transmission range was kept the same, any extra nodes would not be used by the routing algorithm and we would keep getting the same results over and
over. The data produced was a Constant Bit Rate (CBR) flow of packets of 250KB and the total transmission lasted for 15 minutes, simulation time. To ensure the reliability of the results, the same scenario has also been tried for 3 hours of simulation time and the results followed the same trend. The metric for the performance evaluation was the average delivery ratio of the transmitted data and it was selected because it’s the best way to describe the reliability of the network as for each scenario, more intermediate nodes take part to the routing. The five routing algorithms tested were, AODV, DSR, WRP, FSR and Bellman Ford and the simulator used was GlomoSim (UCLA, 1999). More information about GlomoSim can be found in the appendices, chapter 7.2.

![Performance of Routing Algorithms](image)

Figure 4.4. Evaluation of various routing algorithms

From Figure 4.4, it can be concluded that AODV is the best performer based on the delivery ratio for multi-hop network. AODV and DSR seem to behave better while the rest of the protocols see their performance dropping faster as the number of nodes exceeds 80-90. WRP was not tested for more than 100 nodes due to implementation limitations from the side of the simulator. It is noticeable that its performance drops
significantly as nodes increase. The presence of co-channel interference was selected in order to identify which protocol would be able to perform better against it. Adjacent channel interference although it should not be considered something minor, it can cause less problems within a network as the channels overlap partially and not completely. Apart from that, another important factor for choosing AODV is that it selects mainly the shortest path to the destination. This is desirable as due to the segregation distribution of nodes less of intermediate nodes on the routing path between the transmitter and the receiver.

From now on, AODV will be adopted as the only routing in the remaining simulations. In chapter 5, where each subnetwork of the segregation will utilise more than one channel, AODV will be improved with a new channel assignment algorithm (Paraskelidis and Adda, 2007b) to take advantage of the full frequency spectrum. The problem of adjacent channel interference between its subnetwork co-members is also addressed.

### 4.4.2 Network delay over network segregation

In this section we simulate the first segregated wireless network by dividing the network into a number of subnetworks. The nodes within each subnetwork would use a single channel and each subnetwork would have a different channel than the others. This method would create adjacent channel interference between the nodes of each subnetwork and co-channel interference between the members of a subnetwork. Non-overlapping and overlapping channels between the different subnetworks were selected to compare the results accurately with other related works and to build a framework for other proposals. Non-overlapping channels were used for up to 3 segregate networks because the 802.11 has only three. When the network had more than three subnetworks then the channels used were overlapping partially. The simulated area is 300x300 meters, the number of nodes varies between 50 and 130, nodes have a transmission range of 50 meters and the generated traffic is 5 flows of CBR, injecting in the network packets at the rate of 1460 Bytes per second. The protocol used is 802.11b with a rate of transfer of 11Mbps. The transmitter is equipped with multiple radios, which means that it can transmit simultaneously to all available channels.
In this scenario, the average end-to-end delay was evaluated and compared for two network configurations. The first one was the simplest form of a wireless network with various numbers of nodes able to relay data from one side to the other by using a single channel. This approach is used only for benchmark reasons in order to be able to decide if any improvement has been achieved. Routing protocol used is AODV and co-channel interference is automatically present in the network due to the single channel configuration.

The second approach is carried out by segregating the network into smaller subnetworks. The single channel network is divided into smaller networks and each one utilises a different channel. Since no changes to transmission range are permitted, the upper bound of subnetworks is set to 5. If the total number of nodes was small, each subnetwork would have few nodes and these would be out of the transmission range of the rest resulting in no communication. In both approaches the data produced were five data flows of CBR from a single transmitter to three different receivers, ensuring this way that in the case of 5 segregate networks, all available networks would be used. Let’s describe a segregated network with the help of the parameters that affect it. First, $S$ is a segregated network, $n$ the total number of nodes, $g$ the number of subnetworks.
and finally $k$ the number of channels for each subnetwork, which in this scenario is always 1, then $S$ would be expressed as:

$$S(n, g, k)$$

(8)

The total number of channels $T_k$ utilised equals to,

$$T_k = g^* k$$

(9)

and the number of available nodes within every subnetwork $T_n$ equals,

$$T_n = \frac{n}{g}$$

(10)

The results show that the increase rate of delay is reduced as the network is segregated into more subnetworks. The reason behind this is the smaller density $\lambda$ of nodes that operate in the same channel. Whereas in the single channel network there were 50 nodes on the same frequency, network segregation decreased $\lambda$ of nodes operating on the same channel within a unit area and consequently decreased the possibility of two or more nodes to be affected by co-channel interference. Let $n$ be the number of nodes listening to the same channel and $\alpha$ the size of the simulated area then $\lambda$ would be expressed as 11.

$$\lambda = \frac{g}{a} = \frac{n}{\alpha^* g}$$

(11)

The density of a single node network $\lambda_s$, with transmission range $R_{tx}$ is

$$\lambda_s = \frac{1}{\pi R_{tx}^2}$$

(12)
From equations 11 and 12 we define the density and the number of segregate networks to maintain connectivity between the nodes of each segregate network

\[ \lambda \geq \lambda_s \Rightarrow \lambda \geq \frac{1}{\pi R_{tx}^2} \Rightarrow \frac{n}{\alpha \cdot g} \geq \frac{1}{\pi R_{tx}^2} \Rightarrow g \leq \frac{n \pi R_{tx}^2}{\alpha} \]  

(13)

According to the results in Figure 4.5, for 50 nodes and 6 segregated networks the connectivity is lost and it is only achieved when there are 90 nodes in the network.

The initial results were quite promising and showed that network segregation could reduce the effects of co-channel interference and thus improve the network’s performance, in this case being the delay. The question then was how this reduction can be compared to other multichannel approaches and this is explained below.

### 4.4.3 GRID technology against network segregation

Instead of having a single channel network where all nodes operated on the same channel, the network could utilise more channels and the channel allocation would be decided according to the location of the nodes, using the GRID architecture. GRID (Tseng et al., 2006) is a location-aware routing and channel protocol that enables each node to be aware of its position, through a GPS device attached on each node, at any time as it moves around and it uses the appropriate channel according to its position. In our case we leave out the mobility and use only fixed nodes.

The GRID is a multi-channel MAC protocol able to access multiple nodes increasing the available bandwidth within the wireless network and also reducing the possibilities of contention/collision. The idea of GRID is first of all to divide the physical area of the wireless network into smaller squares called grids, something similar to the cellular structure in GSM communications. The number of channels used within the network, depend on the number of grids. The example provided in Figure 4.6 below has 6 grids for axis X and 6 grids for axis Y and totally there are 36 grids. The network uses 9 so
the first 3 grids in both axes use the 9 channels and afterwards the pattern is being repeated.

Each grid is assigned a default frequency channel for the nodes to operate in. Every node that is within this grid uses this single channel. Since the node facilitates a GPS device on it, it is aware of its position and assigns its channel according to the principles of the grid. There might be more than one node within each grid. According to this pattern there is no possibility that a node will have a neighbouring grid operating at the same channel, thus reducing interference.

Figure 4.6. Assignment of channels in GRID. Number of channels n=9. In each grid the top number is the channel number and the ones in the bottom are the grid co-ordinates. (Tseng et al., 2006)

The area simulated is an area of 200 meters by 200 meters, with variable number of nodes. A single transmitter was deployed with 4 radios so it can communicate with all the 4 subnetworks and two different data flows were transmitting packets of 1460 Bytes length every 1 second. The size of the grids was decided to be so that we will not have to use many channels. The grid size was given two different values and testing has been implemented for grid size of \( d_1 = 10 \) and \( d_2 = 40 \) meters, keeping the same total area dimension \( \alpha \), and channels \( k = 4 \) for both the GRID and the segregate scenarios.
In GRID technology the number of grids and the number of channels used are relevant and depended from each other. In both networks, GRID and Segregated, the same density is kept. Since GRID uses only 4 channels in both of its scenarios, the segregated will be considered with 4 subnetworks with single channel each. During the simulations all the nodes were placed randomly inside the area $\alpha$. The GRID protocol divided the area into smaller grids and placed the nodes randomly. Some of the grids might have more than one node inside and other might be empty. As the number of nodes $n$ increases more grids get occupied by at least one or more nodes.

When the initial simulations were performed we came up with an important issue that forced us to change the procedure of the simulations. The problem was that although the number of nodes was increasing, in the 4 segregated network delay was not affected and looked as in Figure 4.7.

![Average Delay](image)

**Figure 4.7. The average end-to-end delay over number of nodes**

The reason behind this issue was the transmission power of the nodes. To be more accurate, for a 20 node network the transmission power was initially set to $P_t = -2$ dBm. This $P_t$, ensured the minimum possible communication of the transmitter with its neighbours so data could successfully reach the destination. But while more nodes were added to the network, $P_t$ remained static and the routing algorithm seemed not to
utilise more intermediate hops. The problem was that due to the high $P_i$, AODV kept using the same nodes in every simulation since they formed the shortest path to the destination and any new nodes remained inactive. The solution was simple and straightforward by reducing $P_i$ every time more nodes were deployed in the network in order to achieve the minimum connectivity. Decreasing the $P_i$, affected the $R_{tx}$ which was also decreasing, so AODV could not use the same routes but new ones had to be discovered and therefore more hops were included to the new route. Adding more hops to the routing path forced the network delay to increase. By the end of the simulations $P_i$ was assigned values between -2dBm for small number of nodes and increased up to -6dBm for more dense networks. The similar problem did not only affect delay but also throughput and delivery ratio.

Both network architectures were tested and results collected were based on three metrics, average delay, average throughput and the delivery ratio of transmitted packets over the received packets at the destination (Paraskelidis and Adda, 2007a).

![Delay](image)

**Figure 4.8. The average delay of the networks for a variable number of nodes.**

As presented in Figure 4.8, the average delay of the segregate network is slightly higher than the delay of GRID technology. Although AODV does perform pretty well within a single-receiver node network, in a multichannel segregate network its
performance is not the best possible as nodes have to face more co-channel interference, whereas GRID manages to encounter this issue more efficiently. The results indicate that the difference is really small, about 3-4 milliseconds. This difference was something expected as our network configuration is pretty basic without any mechanisms to improve the QoS.

Since the data has to go through many routes, in case of congestion in one route there is no way for the route to be relayed to another sub-network where the load is quite lower. The network would possibly function better if there were more channels available within each subnetwork and a channel assignment scheme would minimise interference. Nevertheless even at the current form the results are quite promising regarding the delay parameter.

![Average Throughput](image)

**Figure 4.9. The average throughput of the networks for variable number of nodes.**

As shown in Figure 4.9, one of the main advantages of segregated networks is the increase of the throughput within the network during transmission. A segregate network provides an increased throughput for the same sending/receiving configuration. This happens mainly because the multiple routes provided by the sub-networks. Figure 4.9 should be used only for comparing the throughput difference between the two simulated scenarios. Throughputs seem to be double the traffic injected to the network and the explanation is that the side nodes can transmit simultaneously the two flows from two
different radios sending them through different subnetworks, thus doubling the throughput at the receiver. Also, the lines in Figure 4.9 are the linear trendlines of the simulated results and due to the difference between segregate and GRID it is difficult to examine the effect of node increase to throughput. Figures 4.10 and 4.11 represent the throughputs of the two scenarios independently.

![Average Throughput](image1)

**Figure 4.10. The average throughput of the segregated network**

![Average Throughput](image2)

**Figure 4.11. Average Throughput of the GRID networks**

It should be noticed that at the moment a maximum load overflow has not been defined, which would result in routing the data through another path in case a subnetwork is
facing heavy load. If load overflow mechanisms were set and data was routed through less congested sub-networks, then a slight increase to the throughput would be observed by having a better utilization of the different sub-networks and a decrease in the delay.

![Delivery Ratio](image)

**Figure 4.12. The delivery ratio of the networks for variable number of nodes**

In Figure 4.12, the reliability of the segregate network is compared to the GRID by comparing the delivery ratio. Delivery ratio is the sent/received ratio during the simulation process. It indicates the number of packets that were transmitted and did not manage to reach the destination because of collision or high interference. As it is shown above, the ratio of segregate network is quite constant and does not have big deviation as the nodes increase. GRID on the other hand witnesses its reliability to fall as nodes increase.

As seen from the results, GRID manages to surpass the concept of segregated networks, something that was expected as GRID is enhanced with a channel assignment algorithm and manages to distribute more efficiently all the available channels in the network. On the other hand a segregate network sets a simplified distribution to the utilised channels and the point where segregation overpasses GRID
in throughput and partially in delivery ratio because of the multiple simultaneous transmissions through different routes.

The benefits of network segregation is that it uses a more simple approach, the participating nodes do not require to be aware of their location using a GPS device which adds complexity and increases the cost of the network’s implementation.

### 4.4.4 Network segregation in noisy environments

Until now, segregated networks were tested in an environment with normal noise levels. The term noise $N_o$ is related to the background noise combining the two forms of ambient and thermal noise. The simulator is modelling a general background noise and calculates it by multiplying the Boltzmann Constant (Mohr et al, 2008) with a variable noise figure $N_o$ and the temperature of the simulated area. In the simulator the noise figure takes any positive integer values, but setting large values for it would decrease the SNR resulting in inability of transmissions. Finally, when simulations were performed it was decided to set the noise figure values between 6, considering this a non-noisy environment, and 18 setting it as the noisiest environment that could exist in our experiments by incrementing its value by two accomplishing more precision. If $N_o$ was set over 18, the network nodes did not manage to establish connections with their neighbours due to the high background noise. Equation 14 shows the background $N_B$ and is calculated into dBm.

$$N_B = BOLTZMANN\_CONSTANT*Temperature*N_o*1000 \tag{14}$$

In our case, temperatures levels are kept the same during all of the simulations and the only changing value is the noise-figure, thus we refer to the general background noise as noise $N_o$.

#### 4.4.4.1 Delay in a noisy environment

Previously it was shown that the delay of a wireless network decreases as it is segregated into smaller subnetworks. This section identifies the effect that noise has on
a segregated network for various $N_o$ levels. The network characteristics for all the following scenarios are the same with the ones already presented.

![Figure 4.13. The average delay of a 1 channel segregated network over noise](image)

In Figure 4.13, we examine the drop of the delay as we divide the network into subnetworks and at the same time the noise figure is increased from level 6 to level 18 (Paraskelidis and Adda, 2009a). It is seen that the delay has benefited from the network segregation despite an increase in the level of noise. It should be noted that if the network is segregated into more than 6 subnetworks, delay starts to increase again. The explanation on this issue is given in previous section (4.4.2). This happens because of the low density of each subnetwork as the total number of nodes deployed is 90 and segregating the network into more than 6 subnetworks reduced significantly the connectivity between the nodes in each subnetwork. The success of this scenario is that the network still manages to achieve a reduction in delay even when the harshness of the network, expressed in $N_o$, has significantly increased. There is no reference to the simple 1 channel network and how it would behave in the noisy environment, as it has been disregarded because of the results obtained in Figure 4.5, implying that even in the most ideal environment it would not be able to reach the performance achieved by segregated networks.
4.4.4.2 Network collisions

The next metric evaluated was the number of collisions that occurred inside the network because of adjacent channel interference and the increase of noise. The target of this scenario was to examine if the network segregation could actually decrease the number of collisions when compared to a simple 1 channel ad-hoc network (Paraskelidis and Adda, 2008). The number of nodes deployed in each network was 90 and the network was segregated up to 5 subnetworks. As explained in the previous sections, any further segregation would reduce the connectivity between the nodes. The amount of collisions for the particular networks when noise has its minimum value is shown in Figure 4.14, according to the simulator parameters (UCLA, 1999), and this figure sets the base for the comparisons with Figure 4.15.

![Collisions for Noise Level 6](image)

**Figure 4.14. The number of collisions for noise level equal to 6**
Figure 4.15. Collision increase over noise for 1 channel

Figure 4.15 shows that network segregation improves the reliability of the network for various levels of noise $N_o$. As expected, the simple 1 channel network (represented as “No Seg” in the graph) suffers mostly from the collisions within each network during data transmission. On the other hand, network segregation manages to reduce the number of collisions because co-channel interference is reduced. Therefore any collisions that occur are the result of adjacent channel interference and noise increase. With the increase in noise levels, the frequency of collisions also increases because the links tend to fail more frequently due to the environmental harshness. It is noticeable though that the lowest ratio of increase in collisions is achieved when the network is divided into 4 subnetworks. An explanation to this could be that the density in this configuration provides the best connectivity between the nodes and also the co-channel interference for the members of the same subnetwork is minimised because of the distances between them.

### 4.4.4.3 Retransmissions over noise for high load traffic

The last metric to be explored through simulations was the number of retransmissions that took place inside the network. The first network configuration to be tested was the simple 1 channel network that was set as the basis for the evaluation of the segregated
configuration and any improvement of the networks reliability for the latter one would be easier to identify. There are some important differences from the previous scenarios and are related to the type and amount of traffic that has to be sent over the network. The connections established are single-TCP connections as in the case of HTTP protocol. The aim of the simulations is to test the QoS that the network offers for connections that require confirmation that a packet was received from the receiver. On the contrary, CBR that was used before did not require any acknowledgments (ACK) for the packets sent as it was only flooding the network with packets without checking if they reached the receiver. The total number of TCP transmissions initiated equals to 10, far more than the three transmissions used before for CBR. This way the network is loaded heavily and proves its ability to deliver all the transmitted packets to receiver.

![Graph showing retransmissions with 1 channel network over noise increase](image.png)

Figure 4.16. Retransmissions for a single channel network over noise increase

Figure 4.16 represents the retransmission that take place inside the network as the noise level is being increased from the low value up to the maximum supported by the simulator, 18. During this increase the harshness of the environment results in an increase of the collisions that take place so a large number of retransmissions take place. Operating only 1 channel in the network shows that even RTS/CTS has a difficult task to perform because of the high levels of co-channel interference and noise.
Figure 4.17 gives an overview of the retransmissions that happened in the network for various levels of noise and number of subnetworks when only one channel is utilised within each one. The first thing to notice was that compared to Figure 4.16, there is a significant drop in the number of retransmissions even for a two-segregated network. As it is divided into more subnetworks the amount of retransmissions declines. This is one more proof that network segregation could improve the reliability of the overall network as it manages to reduce the total number retransmissions within the network resulting to less loaded links and consequently a reduction to the overall delay of the network as already shown in Figure 4.13.
Figure 4.18. The average delay in seconds of a 1 channel segregated network over noise increase

In Figure 4.18 network segregation improves the end-to-end delay of network when this is flooded with 10 simultaneous traffic flows even though it reached much higher values because of the high load. In the case of a simple 1 channel network, the co-channel interference degrades severely its performance as it cannot cope with increased traffic that tries to go through. Once the network is segregated into two parts, there is significant decrease of the delay and it keeps decreasing as the segregation continues. The rate of reduction is not significant once the packets arrive inside the subnetworks where only one channel is utilised and the coordination in the channel use is done through RTS/CTS. Network segregation proves its ability to better distribute, compared to a single channel network, the incoming traffic through the available subnetworks.

4.5 Conclusion

The concept of network segregation was introduced in this chapter by pointing out first of all the problems that exist in wireless networks, the co-channel and adjacent channel interferences. The first one is met with networks that operate with only one frequency throughout the network and its effects are expressed in terms of increased network delay, lower throughput and finally increased retransmissions because of collisions.
On the other hand, network segregation divides the network into smaller subnetworks and each one operates with a single different channel, and it was shown that a decrease in co-channel interference is achieved as fewer nodes operate on the same channel, but introduces the effect of adjacent channel interference as it utilises overlapping frequency channels for the subnetworks. Adjacent channel interference and its effects on a network have not yet been examined in depth and there are fewer works that provide ways to overcome it. These proposals are focusing mainly on networks that operate in infrastructure mode with the use of access point and there is little mentioning for use on ad-hoc networks. On the other hand, segregate networks are entirely based on ad-hoc architecture and prove that with the help of a certain channel assignment mechanism it is possible to minimise the impact of adjacent channel interference on the network’s performance.

Through a series of simulated scenarios, it was shown that network segregation outperforms a wireless network that utilises only one channel. The benefits that have been mentioned in this chapter are beginning to prove with the help of the results presented. These results set the base on which further improvements on the concept of network segregation are introduced and are evaluated as will be shown in the next chapter. The segregated networks presented use only one channel within each subnetwork, whereas in the next chapter this limit is relaxed and more channels will be added per subnetwork. The addition of extra channels required the introduction of a channel assignment algorithm the Modulo (Adda et al., 2005) into AODV aiming to efficiently co-ordinate the channel decisions made between the nodes and minimise the effects of the use of overlapping channels and maximise the use of the 802.11b frequency spectrum.
5 Modulo Channel Assignment Algorithm

5.1 Introduction

The focus point of this thesis is the deployment of multihop and multi-channel wireless ad-hoc networks in noisy areas, such as an industrial environment. Single channel networks operate efficiently only when they are deployed in infrastructure mode, this means the use of access points and when the number of the client nodes is relatively small. Ad-hoc networks with a single channel for data transmission in larger deployments are facing poor performance because of the co-channel interference produced by the single channel utilisation.

The usage of more than one frequency channels tends to better utilise the frequency spectrum available and improve the throughput. In the case of the 802.11b standard there are 12 channels available that can be used for transmission. Due to the way the 802.11b was designed (4.2.3), these channels tend to overlap one into to the other apart from three (1, 6 and 12), which can operate inside a network without causing co-channel interference during simultaneous transmissions from neighbouring nodes. These three channels proved to work satisfactorily in real life scenarios but their most important disadvantage proved to be the waste of bandwidth.

This misuse of the available bandwidth urged the need to use more channels that tend to overlap only partially in order to take advantage of the whole frequency spectrum available. The majority of previous researches tended to use only non-overlapping channels and the proposals based on overlapping channels, were limited and mainly focusing on wireless infrastructure mode networks with little reference on ad-hoc networks as discussed in chapter 3 (3.6).

The use of multiple channels within a network, either overlapping or/and non-overlapping, require the existence of algorithms that will define the procedures for assigning channels to nodes and the way on how each node in the network relay data to the next node until data reaches the destination. Based on the concept of network segregation, introduced in chapter 4, the network was divided into smaller subnetworks
and the nodes within every subnetwork used a channel different from the rest of the subnetworks. The number of channels used varied from 2 to 5 and consequently there were 2 to 5 subnetworks. In this way, we managed to reduce the effect of co-channel interference.

As seen in Figure 5.1, there are 52 nodes in the network and the four purple nodes are the side nodes, representing the traffic generators and the traffic sinker. The network is divided in 4 segregate networks (subnetworks) and each one operates with a different channel. The different colours show the different channels. The data produced from the side nodes is routed through the various subnetworks until it reaches the destination. Although this network configuration offers multiple routes and also decreases the co-channel interference, it doesn’t however remove it completely. For example, all the blue nodes operate on the same channel frequency.

As explained above, the use of multiple channels within each subnetwork was the only way to overcome co-channel interference. Another problem we need to address with this proposal was how would nodes manage these channels and switch from one channel to the other. Since the channels used are overlapping, adjacent channel interference would be present and have effects on the nodes that operate on these channels. The task of channel assignment is related to the routing algorithm and in our
case it is the responsibility of AODV to take the decisions based on certain criteria. The problem with AODV is that it was not designed to handle multiple channels and although it was modified in the concept of segregated networks, the decisions in assigning channels was completely random. Thus AODV required further modifications to take these decisions and it was achieved with the introduction of the modulo channel assignment algorithm (Adda et al., 2005).

5.2 Modulo in multi-hop networks

Modulo is a dynamic channel assignment algorithm and it operates inside a multichannel and multihop network forcing the nodes that belong to a particular routing path to take certain decisions every time they receive or transmit data. It enables multi-radio nodes to operate as transmitter and receivers simultaneously as it applies alternative frequencies between receiving and transmitting disciplines using partially overlapping channels.

5.2.1 Operational characteristics of modulo

![Figure 5.2. Modulo channel allocation using three channels](image)

The main difference from the proposed algorithms described in Chapter 3 is that instead of using only non-overlapping channels, modulo operates using partially
overlapping channels. In order to better understand the way modulo works, consider the
scenario shown in Figure 5.2. The transmitter on the far left wants to send data to the
far right node, but since the receiver is out of its transmission range $R_t$, it has to relay
the data through the intermediate nodes. All participating nodes can operate on all three
available frequencies and they could receive and send the data by choosing which
channel they will use randomly. The worst case scenario would be to choose the same
channel for receiving and transmitting the data and in this case, the advantage of
simultaneous transmissions would be lost due to collisions. A less catastrophic scenario
would be one where neighbours within the transmission range use the same channel
and again transmission would be disrupted because of interference.

Modulo on the other hand (Paraskelidis and Adda, 2007b), obligates the participating
nodes in the data flow link to select channels that would help to avoid the two problems
mentioned above. When a transmission initiates, a random channel $k$ is used to avoid
any possibility that any other node will start transmitting at the same one. A node, upon
receiving data packet on channel $k$, will transmit it on channel $k+1$ and so on. When $k+1$
is larger than the number of available channels, the cycle starts again and the initial
channel zero is used. As shown in Figure 5.2, the transmitter starts sending the data
using channel $C_0$ and data reaches the next-hop node. The second node in the path,
since it receives the data in $C_0$, it starts transmitting at the same time in channel $C_1$. The
third node starts receiving data using channel $C_1$ and forwards it by using channel $C_2$.
Finally, the fourth node in the chain receives the data on $C_2$ but since there are no
more channels to use in the channel pool, it reuses the firstly used channel and that
is $C_0$. This way it manages to use all available overlapping channels utilising the full
frequency spectrum provided by them and doesn’t require only non-overlapping
channels for better transmission. The whole process of channel decision is described
by equation 15, where $n$ is the hop number, $k$ is the starting channel and $c$ is the pool of
available channels.

$$C_n = (n + k) \mod c$$  \hspace{1cm} (15)
5.2.2 Modulo in chain topology

Modulo was firstly introduced in an attempt to investigate the advantages of multi-hop networks for data transfer over that of a single hop. In a single hop scenario both nodes will have to radiate more power to propagate the data the same distance, and as a result suffer more from the radio propagation and contention issues that limit bandwidth. In a multi-hop scenario nodes use lower power radios, reducing the likelihood of radio propagation issues and collisions with other nodes (Adda et al., 2005).

In multi-hop ad hoc networks, frames travel along a chain of relay nodes toward the destination. Due to the broadcasting nature of the communications, nodes within range of each other interfere, and hence diminish the amount of concurrency in the transmission. As shown in Figure 5.3, a transmission from the node 1 can be affected by a simultaneous transmission from node 2. The reception at the node 2 from node 1 can also be affected by a transmission from node 3. Even worse, interferences from node 4 may go way beyond its communication range affecting the reception at node 2, hence preventing node 1 from transmitting successfully to node 2.

Figure 5.3. Interference range in a chain of an ad-hoc network
5.2.2.1 Power issues in a multi-hop network

The first issue to be investigated was the power consumption and the differences between a single-hop and a multi-hop network. In ad hoc networks nodes consume power for both processing tasks and transmission routing, even in the absence of any immediate communication. To make the matters worse, nodes consume more power to overcome free space loss and signal dispersions as it emerges with longer distances, especially with large-scale networks. The power consumption is certainly a major issue in such environments.

It was shown (Adda et al., 2005) that the overall end-to-end conserved power $C_p$ in a multi-hop over a single hop ad hoc network is considerably high and is expressed in equation 16 for a number of $n$ nodes, separated in $n$-1 hops and the path loss parameter $\alpha$, that in theory it equals to 2 but in realistic environments it can takes values of 3.5 or 4.

$$C_p = (n-1)^{\alpha-1}$$ (16)

There is a great benefit in controlling power over short-range transmissions, which can also reduce the total level of interference in homogeneous multi-hop ad-hoc networks under fixed traffic conditions. It has been stated (Ericsson, 2000) that the level of interference can itself be reduced by the same amount as the transmitted power. Equation 16, does not take into consideration retransmissions, fading and uneven ranges between network cells. In the case of transmissions in segregate networks, when reducing the number of nodes that operate in same channel we could consequently reduce the level of interference. Figure 5.4 represents graphically the relation in power conservation for multi-hop over single-hop networks for various numbers of nodes which are in the routing path and are used to relay the data from the transmitter to the receiver and for the three possible values of $\alpha$. 
The benefit of short-range transmissions in a multi-hop network is that nodes can reduce their power of transmission $P_i$ and relay the data through other intermediate nodes until reaches the destination. Another benefit is that by the use of multiple channels the same transmission could also reduce the end-to-end delay.

### 5.2.2.2 End-to-end delay in multi-hop and multi-radio networks

End-to-end delay in a multi-hop network depends on several factors: length of the frame transmitted, routing deployed, connectivity, link capacity, acknowledgment policies, and retransmissions. The latency increases as the frame travels over several hops. The two scenarios that were considered in this analysis were a single channel and a multi-channel network over a multi-hop chain of nodes as shown in Figure 5.4. The single channel network uses the same channel over the whole communication procedure whereas the multi-channel switches frequencies in order to avoid collisions.

For the single channel network, it was shown that the end-to-end delay increases with the number of hops and due to the power issues and environment interferences, the single hop seems to loose link capacity. As the first node transmits a packet to the
second node, the second one will send an acknowledgment back to the first node ensuring that the packet was receiving successfully. Afterwards, the second node will transmit the packet to the third node waiting for an acknowledgment. Since only one channel is used it is impossible for concurrent transmissions to happen as the first three nodes are within the same transmission range and before any new transmission to happen nodes have to wait the so called back off time. Node one will be able to send a new packet as soon as the first packet reached and is acknowledged by node 5.

In the case of the multi-channel network, it is assumed that that every node transmits packets received from the application with the carrier $C_0$. Any frame received from the network with a carrier $C_1$ requiring further routing will be forwarded with the carrier ($C_1 + 1$). The number of nodes that can receive and send packets concurrently depend on the number of hops and the number of channels used. In the case of two utilised channels, only the first three nodes can operate simultaneously. Compared to the single channel network, within the same amount of time more packets would be transmitted over, increasing the link capacity of the chain and thus reducing the delay during the transmission. When the utilised channels are 3, node 4 outside its communication range interferes with node 2 while receiving from node 1. Finally, when there are 4 channels available for the nodes to switch, all nodes in the critical path of the interference will use different channels hence removing any potential collisions.

A multi-hop scenario with 4 channels provides an improved delay than single channel networks as the length of data that can be transmitted over the same amount of time is larger and this is expressed in equation 17. $R_i$ is defined as the ratio of the latency of a single-hop to a multi-hop network, $n$ the number of nodes, $b$ the number of gaps between each fragment to allow nodes in the chain to transmit without interference, $F$ is the fragment size, $L$ is the data frame and $\alpha$ remains the path loss parameter.

$$R_i = (1 + (\alpha - 1) \ln(n - 1) / \ln(SNR)) / (b + (n - (1 + b)F / L)) \quad (17)$$

In this equation, we ignore the overheads introduced by RTS/CLS, Short Interframe Space (SIFS) and Distributed Interframe Space DIFS of Wi-Fi protocols. The results
from the two scenarios prove the difference between the two scenarios described above and show the improvement of delay in a multi-channel network over a single one.

![Ratio of Delay - high SNR](image)

**Figure 5.5. Ratio of the delay between single hop and multi-hop network with high SNR**

In Figure 5.5 is shown the delay ratio between a single-hop and a multi-hop network including the hop interference in a non-noisy environment, having a $SNR$ ratio of 251, the path loss parameter is set to 3.5 and the data fragment is 1/200 of the data packet.

In Figure 5.6 the same parameters are used and the only difference is that the $SNR$ is low at a ratio of 5, implying that the environment is noisier.
Figure 5.6. Ratio of the delay between single hop and multi-hop network with low SNR

Figure 5.7. Ratio of the delay between single hop and multi-hop network with high SNR
In Figure 5.7 is represented the ratio of the delay between a single channel and a multi-channel network for various numbers of channels available. The environment is not noisy, the SNR ratio is 251 the path loss parameter equals to 3.5 and the data fragment is 1/200 of the data packet.

![Ratio of Delay - low SNR](image)

**Figure 5.8. Ratio of the delay between single hop and multi-hop network with low SNR**

Finally, Figure 5.8 shows the ratio of the delay between a single channel and a multi-channel network for various numbers of channels available. The environment is not noisy, the path loss parameter is set to 3.5 and the data fragment is 1/200 of the data packet. In the last two figures, figures 5.7 and 5.8, it is shown that when the multi-channel network utilises either 2 or 3 channels there is no difference to the delay ratio because the extra channel, according to the tested scenario did not provide any increase to the capacity of the network.

The presented work above is based on theoretical assumptions made from existing mathematical models (Li et al, 2003) and describes the behaviour of wireless networks. Single-hop and multi-hop networks are two different types of networks that serve particular services and applications. They have their strengths and their weaknesses depending on the environment they operate in and the functionalities they have to
provide. Multi-hop networks were developed later than the single-hop networks and they were designed for particular reasons. New technologies and applications were created that required the transmission of data over longer distances and an increased capacity. The single-hop networks failed to perform efficiently under these circumstances due to their limitations on their transmission ranges and the capacity they offered. On the other hand, multi-hop networks managed to overcome the transmission range issue by relaying the transmitted data over intermediate nodes until they reach the destination. As it was shown in this section, the problem that appeared for multi-hop networks using a single channel for all connections between the nodes is the drop of the links capacity and accordingly the end-to-end delay of the network.

5.2.3 Theoretical analysis of modulo

This section gives a theoretical approach to modulo operations and the process of the hop-by-hop transmission. Modulo adopts a store and forward packet transmission mechanism for every single packet that travels through the multi-hop path defined by AODV and this mechanism is show in figure 5.9.

![Figure 5.9. Store and forward packet transmission](image)

S is the source node, D is the destination node and all the rest are the intermediate nodes between source and destination. R-f is the last node that interferes with the transmission of S and after the R-f node all remaining nodes can transmit using the same frequency with S without interfering. The position of R-f depends on the transmission range and the location of S.
Let denote $T_h$ the transmission time between two adjacent nodes as $R1$ and $R2$ or $S$ and $R1$ and let assume that there are $m$ chain nodes distributed randomly within the subnetwork of a segregated network $S$ ($n, g, k$), where $g$ is the number of segregated networks and $k$ the number of channels in each subnetwork. The value of $m$ is a number smaller or equal to the number of member nodes of a single subnetwork.

$$m \leq \frac{n}{g} \quad (18)$$

The source station is sending $N_p$ number of packets of length $L$ (bytes). The packet may be segmented into fragments $F$ with each fragment being acknowledged by an acknowledgement packet $A$. If no acknowledgment is required, then a fragmentation is not required and $L$ is equal to $A$. With $S$ being the only injection of traffic source, the end-to-end delay is

$$T = (m + 1) \cdot T_h \quad (19)$$

The total transmission time of $N_p$ packets will equal to,

$$T_s = m \cdot T_h + (N_p + f \left( \left\lfloor \frac{N_p}{k} \right\rfloor - 1 \right)) \cdot (T_h + T_a) \quad (20)$$

where $T_h$ is the transmission delay for one packet within a single hop, $T_a$ is the transmission delay of a single acknowledgment packet (34 bytes), $f$ describes R-f as explained above, $k$ is the number of channels utilised in the subnetwork. Equation 20 shows the dependency between the number of packets that have to be transmitted, the amount of channels utilised within each segregate network and finally the interference range. This equation applies to every segregate network separately and not to the whole network. The upper limit indicator ensures that the outcome of the division between $N_p$ and $k$ is always an integer. Since modulo technique is trying to achieve concurrent transmissions in a chain of nodes, the maximum achievable number of
these concurrent transmissions are related to how many packets have to be sent. The number of channels which are available and how many of them will actually be used is related to the interference range $f$. Consider the scenario where four packets have to be transmitted, there are two channels available the interference range is equal to two and the total nodes in the chain equals to eight. Equation 20 shows that once the first two packets are transmitted, they should be two hops away with the aim of achieving another two concurrent transmissions for the next packets in the queue. Having eight nodes in the chain, modulo can achieve four concurrent transmissions of the four packets. If interference range was larger than two, then the concurrent transmissions for the whole length of the chain would be less.

Finally, the capacity $C_s$ of the transmission measured in packets/second is calculated as,

$$C_s = \frac{N_p}{T_s}$$  \hspace{1cm} (21)

Each time $S$ transmits a packet to node $R1$ on channel $k$, the packet is stored temporarily in the node and an acknowledgment (ACK) is sent to the source node. Once the ACK is received, the packet is transmitted to node $R2$ on channel $k+1$ and at the same time node $S$ sends the next packet to node $R1$. This way all nodes can transmit simultaneously only if there are enough available channels for utilisation. If there are only two channels available then only two nodes can communicate simultaneously. The transmissions of ACKs do not affect the network’s performance as long as multiple channels are used.

In an attempt to evaluate equations 20 and 21, consider the following scenario by calculating the throughput over a chain of nodes for variable numbers of transmitted packets $N_p$ and variable utilised channels $k$. The rate of transmission is set to 11Mbps, and initially $m$ is set to 6 nodes and $f$ equals to 4 nodes, although this values may change for comparison reasons. No ACKs are required and a single packet is 1375
Bytes long, resulting to $T_n$ of 1 msec and finally $N_p$ gets values of 6000, 9500 and 13000 packets respectively.

![Throughput improvement over variable Np and f=4 m=6](image)

**Figure 5.10. Throughput improvement over utilised channels for f=4 and m=6**

Figure 5.10 presents the improvement of the throughput of a single chain of nodes utilising variable numbers of channels while $f$ is equal to 4 nodes and there are 6 nodes in the chain used for the transmission. With the utilisation of a second channel in the chain, the throughput is improved significantly, and this improvement continues with the addition of extra channels, although with a smaller rate. At the end, with the use of 5 channels, throughput has achieved an improvement of 255 packets/sec over the single channel scenario.
The next scenario is an examination of the performance of the network when $f$ is reduced and since it is related to the transmission range of the nodes, this reduction also corresponds to a reduction of the transmission power of the nodes. This reduction appears to play a major role on the chain’s throughput as fewer nodes are affected due to reduced transmission interference and consequently throughput is increased. Even for a single channel, the chain’s throughput was improved notably when compared to the previous scenario. Previously the achieved throughput was 200 packets/sec and now the single channel manages to transmit at the rate of 250 packets/sec. Finally, the throughput for $k=5$ reach a faster rate of 625 packets/sec compared to the 555 packets/sec of the previous scenario.

Figure 5.12 presents the throughput of the chain when the number of interfering neighbours is 4 while more nodes are added in the chain. The member nodes are increased from 6 to 8, so now the packet has to hop through extra 2 nodes until it reaches the destination. According to the results, the effect of the extra hops in the routing path is minimal when compared to the first scenario and actually this addition of nodes decreases the throughput of the chain very slightly.
Figure 5.12. Throughput improvement over utilised channels for f=4 and m=8

The conclusion from the proposed theoretical approach is that when nodes are deployed in a chain topology, as it is performed in a segregated network, the use of extra channels for switching from hop to hop increases the throughput of the chain. When multiple chains are deployed using different channels then the improvement of the throughput is multiple. Apart from the utilised channels, the reduction in the transmission range of the nodes improves significantly the chain’s throughput. This reduction of the transmission range has a double positive impact, as less power is required for transmission and more packets can travel through the chain by using less energy. On the other hand, the decrease of the intermediate nodes in the chain doesn’t provide a noteworthy throughput increase because of the multiple channels deployed and the reduced interference from the adjacent nodes.

5.2.4 Modulo and network segregation

Multi-hop networks should address the limitation set by the use of a single channel and thus embrace multiple channels as the best option. As seen from the results given previously, the use of multiple channels over multi-hop networks, manages to overcome the capacity problems. Great focus was given on the fact that more the intermediate
nodes between the transmitter and the receiver, larger number of channels have to be used in order to minimise any interference from neighbouring nodes. From the work presented in the previous section there are some points that need to be clarified. All the assumptions made and the mathematical models presented for the multi-hop networks are based on static nodes that operate in ad-hoc configuration and are placed in a chain topology and the channels used were not clarified if they were non-overlapping or partially overlapping.

The work that is presented in the remaining of this chapter is based on the assumptions that were previously presented (Adda et al., 2005) regarding the end-to-end delay and extend the comparison between single and multi channel networks in other metrics such as calculating the collisions and the retransmissions that occur within a segregate network, metrics that widely describe a network’s QoS. Modulo enters the concept of segregate networks in order to co-ordinate the channel decisions made. The network segregation concept used until now, was that a whole single channel multi-hop network is divided into smaller subnetworks and the member nodes of every subnetwork use a different channel from the rest subnetworks. The channels used were either non-overlapping, when up to three channels were used or partially overlapping channels when more than three channels were deployed. The later approach attempts to take full advantage of the spectrum they were using and at the same time allows simultaneous transmissions through any available subnetwork. The problem with simple segregate networks was that the member of each subnetwork used a single channel for communication, inheriting all the problems, as explained previously, of a single channel network but in a smaller scale. For this reason, multiple partially overlapping channels are utilised inside each subnetwork in an attempt to completely eliminate existence of co-channel interference inside the network. The implementation of modulo within a segregated network would benefit the performance of the network as it would take advantage of a larger portion of the available frequency spectrum in 802.11b protocol. The first attempts of modulo in a segregated follows in the next section and its performance is examined in a non-noisy environment.
5.3 Modulo in non-noisy segregate networks

The introduction of modulo into a segregated network is achieved through its encapsulation into the routing algorithm, the AODV. It was shown in the previous chapter (4.4.1) that AODV performs better than other ad-hoc routing protocols for the network configuration presented in this thesis. Apart from that there are three more factors that established AODV as the best solution for the proposed approach.

5.3.1 Routing and channel assignment

During the routing set up AODV selects the shortest routes to the destination and according to the network requirements the nodes have to transfer data from one side of the industrial area to the other. AODV is forced to select one of the available segregated networks in order to set up its route and since the number of nodes inside the subnetwork is limited due to segregation, it uses less intermediate nodes until data reaches the destination. The second factor is that modulo operates better into an almost chain topology. Considering the first factor, the shortest path will select the nodes that directly lead to the destination, so chain topology is achieved. The final factor is that AODV is a reactive protocol, which means that it initiates the ROUTE_DISCOVERY process only when a route fails completely. Unlike to proactive protocols, AODV will need to flood the network with messages requesting a new route to be found fewer times and since the nodes are not mobile there is less chance for nodes to lose communication with their neighbours and the link to fail.

Nodes are equipped with multiple radios and each one operates on a single channel. The number of radio frequencies for each node varies and according to the designed scenarios their number lies between 2 and 5 and the channel use is decided by the routing algorithm. The process of the routing set up and channel usage are shown in the next two figures.
Figure 5.13. A segregated network utilising modulo

Figure 5.13 shows the routing paths for three data flows that are routed through a 3 segregated network and which have been established by AODV finding the shortest possible path to the receivers. Each subnetwork utilises three channels so the total number of channels used in the network is 9. The left side node establishes three different data flows, by utilising three radio, for the right side nodes with the help of AODV. In reality the number of side nodes would equal to the total number of segregate networks for better distribution of utilised channels and flows from the side nodes. Data is routed using only the members of each subnetwork and modulo defines the channels to be used. Assuming that the total channels used are from $C_1$ until $C_9$, these will be distributed equally between each subnetwork. Consequently, the blue nodes are assigned to operate in a pool of channels ($C_1, C_2$ and $C_3$), red nodes operate in channel pool ($C_4, C_5$ and $C_6$) and finally green nodes use the channel pool ($C_7, C_8$ and $C_9$). The side (purple) nodes can listen to all the channels available in the network and so can communicate with any subnetwork.

Once the transmissions starts, a side node will transmit simultaneously to the three subnetworks in three different channels. The same node station will transmit on all of its radio interfaces at the same time, similarly to having three stations with one radio interface each working and transmitting concurrently. As shown in Figure 5.15, the communication with the blue coloured subnetwork will start on $C_1$, with the red subnetwork on $C_4$ and with the green on channel $C_7$. Since these three transmissions
do not use the same channel and their channels overlap partially, they can occur concurrently. The next hops on the routing paths receive the packets using the same frequency they were transmitted and forward them by transmitting on the next channels in the channel pools and these are $C_2$, $C_5$ and $C_8$ respectively. The same process will be repeated on the second hop by using the corresponding channels. Once this is completed, the next hop resets the channel value and reuses the first available channel. Depending on the routing path and the number of intermediate nodes this channel reuse can be repeated or not. The gain from this approach is to achieve simultaneous transmissions on partially overlapping channels and minimise the ACI interference from neighbouring nodes. Figure 5.14 represents the operation of modulo algorithm used for a network with 2 subnetworks, $g=2$, and 2 channel $k=2$ utilized inside each one.

```
1 If NodesAddress(a) >= n(1) and NodeAddress(a) =<n(1+x)
2 then they belong to subnetwork g(0)
3 If ReceiveChannel(k)
4 then TransmitChannel (k+1)
5 else if ReceiveChannel (k+1)
6 then TransmitChannel (k)
7 Else if NodesAddress(a) >= n(x+2) and NodeAddress(a) =<n(x+y)
8 then they belong to subnetwork g(1)
9 If ReceiveChannel (k+2)
10 then TransmitChannel (k+3)
11 else if ReceiveChannel (k+3)
12 then TransmitChannel (k+2)
```

Figure 5.14. Pseudocode of modulo choosing a channel according to the address of a node

Figure 5.14 describes the operation of modulo for two segregate networks with 3 channels each. The channel selection for the nodes is done according to their address in the network and the segregate network they belong to. The addressing of the intermediate nodes starts for n(1) and every node whose address is equal or smaller than n(x+1), the node belongs to subnetwork g(0). Regarding its member nodes, they utilise three channels $k$, $k+1$ and $k+2$. Subnetwork g(1) is the second subnetwork and includes nodes whose addresses are a number between n(x+2) and n(x+y). The
variables $x$ and $y$ are related to the total number of nodes of the network and in the case of a 2 segregated network they are equal and correspond to the number of members of each subnetwork.

![Figure 5.15. Channel assignment using 9 channels in a 3 segregated network](image)

By using multiple channels through the multi-hop routes, the network is taking advantage of the benefit of modulo algorithm. More the channels utilised inside this route larger the distance is covered until the same channel to be reused. So for example the left side node uses $C_i$ to reach the first blue node, by the time a node reuses the same channel, its transmission range will not overlap with the transmission range of the left side node. Regarding the transmission power $P_i$ of the nodes, every node should have the same $P_i$ in order to keep homogeneity within the network.

Regarding adjacent channel interference (ACI) and the number of channels in the network, there were some considerations regarding the efficiency of partially overlapping channels and the effects that ACI would have on the transmissions by creating collisions during the transmissions. In theory it was shown (Adda et al., 2005) that when there is enough spacing between the overlapping channels the network’s performance is guaranteed and outperforms that of a single channel. In the case of segregated networks, where the network is divided up to three subnetworks and the total number of channels used reaches the maximum of 15, the spacing between them is large enough, according to the 802.11b structure, and ACI is kept at low levels. The
question was what would happen for 4 or 5 segregated networks using 5 channels in every subnetwork. In this case the level of interference caused by ACI could degrade the network’s performance and would set limits on the numbers of segregate networks and channel usage. The only way to estimate this effect was by performing the required simulations and the results would reveal if the considerations were truthful. The results presented in the next sections are performed into an environment with both low and high levels of ambient/thermal noise $N_o$ as defined by the simulator (UCLA, 1999).

### 5.3.2 End-to-end delay and modulo

The first metric to be investigated (Paraskelidis and Adda, 2007b), was the end-to-end delay of the network when a particular number of flows are crossing through it and data leaves the transmitter until it reaches the destination. The network follows the set up as shown in Figure 5.15, where the nodes are static and are placed randomly in order to achieve an equal spread across the physical area and network configuration is given in Table 5.1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrain</td>
<td>300x300 m</td>
<td>No of Nodes</td>
<td>50→130</td>
</tr>
<tr>
<td>Propagation</td>
<td>Two-ray</td>
<td>Number of Segregates</td>
<td>1→5</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>50 m</td>
<td>Number of Channels</td>
<td>1→25</td>
</tr>
<tr>
<td>Mobility</td>
<td>None</td>
<td>Simulation Time</td>
<td>2 hours</td>
</tr>
<tr>
<td>Rate</td>
<td>11 Mbps</td>
<td>Protocol</td>
<td>IEEE 802.11b</td>
</tr>
</tbody>
</table>

**Table 5.1. The parameters of the simulations**

### 5.3.2.1 Network configuration

The simulated area’s dimensions are 300x300 meters and inside are placed various number of nodes starting from 50 and they reach up to 130. The generated traffic consists of 5 Constant Bit Rate (CBR) flows that flood the network with packets of 1460 bytes every second and these flows last for the whole duration of the simulation without pausing at any point in time. For noise levels $N_o$, the simulator provided a scale from 6
to 18 where 6 was the lowest possible and 18 the maximum it could appear in the network. In the simulations noise level was kept low having a value of 10. By keeping low the noise, the only parameter that affects the network’s performance is ACI.

The aim of the simulations is to better understand the relation between the number of segregate networks and the number of channels utilised within each of them and how this relation affects the network’s performance. For the forthcoming simulations $n$ is set to be constant (90 nodes), and so we disregard it and maintain only the number of subnetworks $g$ and channels $k$.

$$S(g, k) \quad \quad (22)$$

In this chapter, with the introduction of modulo, the number of channels $k$ changes and takes values from 1 till 5. Since the environment is not noisy, the spacing between the partially overlapping channels and the expected number of neighbours $E_n$ within the network, mainly defines the network’s performance for high values of $g$ and $k$. Equation 23 calculates the number of possible neighbours of one node out of the total number $n$. These neighbours do not have to belong in the same segregate network and operate on the same channel.

$$E_n = \frac{n \pi r^2}{\alpha} - 1 \quad \quad (23)$$

According to equation 23, $E_n$ is related to the total number of nodes $n$ in the network, the radius $r$ of the transmission range $R_{tx}$ and $\alpha$ is the total simulated area. Finally, within the transmission range $R_{tx}$ of a node and the estimated number of neighbours $E_n$, one can calculate $E_c$, the number of nodes which possibly use the same channel pool.

$$E_c = \frac{E_n}{g} \quad \quad (24)$$
The importance of these parameters on the network's performance is demonstrated and explained in the simulation results presented in the following sections.

### 5.3.2.2 Simulation results

![Graph](image)

**Figure 5.16. The average delay in milliseconds of a 2 part segregated network utilizing two or more channels**

Figure 5.16, describes the trend of the end-to-end delay of the network when it is segregated into two subnetworks and every subnetwork utilises two to five channels. The decrease of the delay is obvious when compared with Figure 4.5 in chapter 4 (4.4.2), while the delay never dropped below the 10ms barrier, now it achieves values below that. The side node has the option to transmit through different routes where the channels transmit and receive into alternate frequency channels, resulting to less ACI interference. As the total number of nodes $n$ increases, AODV finds new routes with more hops, the delay also increases and this is expected because of the ACI that appears in the network. The trend of the delay for $S (2, 5)$ follows a smaller ratio of increase compared to other values of $S$. When data is relayed over a chain of nodes, the interference from other nodes in the chain is reduced because of the channel
switching from hop to hop. This means that when the channel pool for a subnetwork has 5 channels, the node that might reuse the first channel in the pool will be way out of the interference range of the first transmitted node.

![Graph showing delay versus number of nodes for different number of channels in a 3-part segregated network.](image)

**Figure 5.17. The average delay in milliseconds of a 3 part segregated network utilizing two or more channels.**

In the above scenario the network is divided into 3 parts and again modulo is used for the channel allocation. The delay is decreased even more and gets the value of 7.1ms. Of course as the number of nodes increase, the delay increases. It is clear that every time five channels are used within each subnetwork, delay always gets the smaller possible values. Once more the increase ratio for $S(3, 5)$ is the smallest one and with a noticeable difference from $S(3, 4)$. The main reason for the reduction of the delay is the reduction of density $\lambda$ of the nodes that operate on the same channel pool and consequently the reduction of $E_c$. 
In Figure 5.18 the network is divided into 4 subnetworks for various numbers of $k$. Once more modulo contributes to the decrease of the average delay inside the network as the number of the channels increased. Although the decrease might not be significant, the lowest value of the delay drops just over the 6msec. It’s worth mentioning that the difference gap between the scenarios is increasing and this has to do with the increase of channels used within each subnetwork and the number of segregated networks. The question that rises is, can delay further be improved? This is explained in Figure 5.19.
Figure 5.19. The average delay in milliseconds of a 2 part segregated network utilizing two or more channels

Figure 5.19 shows the best results regarding the end-to-end delay in the network having a value just below of 5ms. Even though the network gets the minimum delay for $S(5,5)$, the difference from $S(5,4)$ is quite minimal. This shows that the improvements of modulo reach their limits as the total number of channels utilised for the whole network has been increased significantly. In the case of $S(5,5)$ there are 25 channels in total in the network which of course cannot fit within the frequency spectrum of 802.11b. For this reason we had to extend its spectrum slightly and at the same time reduce the spacing between channels. In the case of the spectrum increase, although it cannot apply in reality due to hardware restrictions, it was performed for experimental purposes only to show how more channels can affect the ACI on the transmissions. The use of the extra channels actually did not improve further the performance of the network in a very noisy environment. Although the channel spacing, in 802.11b it is 20 MHz between neighbouring channels, this was reduced to 15MHz in order to limit as much as possible the extra extension of the 802.11b spectrum. The assumption from the last simulation results show that by increasing the overlapping area between two or more neighbouring channels, the ACI increases.
This overlapping area between two or more channels can be calculated as shown in equation 25. Let’s define $\Delta C$ the overlapping area between two channels $C_x$ and $C_y$ that happen to be close enough to each other, then the overlapping area (bandwidth) between the two channels is calculated accordingly.

$$\Delta C_{x+y} = |C_x - C_y|$$  \hspace{1cm} (25)

This overlap between the channels is an absolute number and it increases if the spacing $C_{sp}$ between two channels $x$ and $y$ decreases. This overlapping of the channels creates additional noise between the two nodes use these channels and is expressed as shown in equation 26.

$$C_{sp}^{x+y} = \frac{1}{\Delta C_{x+y}}$$  \hspace{1cm} (26)

This type of noise is called $N_{\Delta C}$, is expressed in the form of ACI and reduces the SNR of a transmitter and accordingly the transmission range $R_{tx}$. Any further increase to the network segregation would reduce the density $\lambda$ of the nodes that operate in the same channel with small number of nodes and thus the distance between the neighbours will increase which results in a limited connectivity between them. As a result, the channel capacity between the hops will drop as shown in (Adda et al., 2005) and in the worst case there will be some loss of connectivity in noisy environments. This scenario is investigated in the next section.

The results from the integration of modulo inside a segregated network prove useful and fully agree with the theoretical assumption presented in (Adda et al., 2005). Due to spectrum limitation, the spacing of channels had to be reduced and consequently the channels resulted in an increase of $\Delta C$. From the theoretical point of view the delay gets the minimum values for $S (5, 5)$. But in a real life scenario in an attempt to minimise the network complexity and cost, an $S (5, 3)$ configuration would be selected.
Next section introduces the external noise $N_o$ and this increases the harshness in the network when combined with the ACI already present.

### 5.4 Modulo in noisy segregate networks

The scenario of a noisy environment simulates as accurately as possible the environment of an industrial area. While previous simulation results have assumed that the network was operating into a normal environment with $N_o$ value equal to 10, the results in this chapter will present the behaviour of the network for various values of $N_o$, contributing to the overall noise level of the physical area making the transmissions more vulnerable to errors and loss of connectivity as there is a drop to the SNR.

The network follows the same configuration as described in the previous section with two differences. The total number of nodes $n$ is set to 90 nodes. This value was selected because it captures an average reflection of the network’s performance and it is a more realistic value given the total simulated area. Another scenario investigated and which was mentioned in the previous chapter is the case of over segregating the network. Table 5.2 presents the network parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrain</td>
<td>300x300 m</td>
<td>No of Nodes</td>
<td>90</td>
</tr>
<tr>
<td>Propagation</td>
<td>Two-ray</td>
<td>Number of Segregates</td>
<td>1→6</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>50 m</td>
<td>Total Number of Channels</td>
<td>1→25</td>
</tr>
<tr>
<td>Mobility</td>
<td>None</td>
<td>Simulation Time</td>
<td>2 hours</td>
</tr>
<tr>
<td>Rate</td>
<td>11 Mbps</td>
<td>Protocol</td>
<td>IEEE 802.11b</td>
</tr>
<tr>
<td>Noise Level</td>
<td>6→18</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.2. The parameters of the simulations
5.4.1 Delay of segregated network over noise using modulo

The benefits of network segregation for a noisy environment are evaluated and presented based on the simulations performed in (Paraskelidis and Adda, 2009a), in an attempt to further evaluate them with the assistance of modulo technique. Network over-segregation is also examined and the results show the negative effect it can have on a network’s operation. In the following scenarios, the generated traffic are 5 flows that travel from 5 side nodes to the destination side node of the network using the available paths provided by the existing subnetworks. It should be noted that although this amount of traffic is considered relatively light for the network’s designed capacity, the values of the delays presented are quite low. However, it is worth noting that the comparison is against a multi-hop network that utilises a single channel. Similar results for a single channel network and a segregated network with only one channel within each subnetwork were presented in Chapter 4 (section 4.4.4.1).

![Figure 5.20. The average delay in seconds of a 3 channel segregated network over noise increase](image)

The delay is examined against to the network’s segregation and the noise level. The difference from the scenario presented in Chapter 4 (section 4.4.4.1) is that 3 channels are now utilised inside each subnetwork and they are unique. A noticeable conclusion made from figure 5.20 is that for the 90 node network, if it segregated into 6
subnetworks the delay starts to increase again. This happens because the density \( \lambda \) decreases and the transmission power of the nodes is not sufficient enough to keep the connectivity with their neighbouring nodes. With the extra effect imposed by \( N_\alpha \), capacity falls and it requires more time a packet to hop between two nodes. Another conclusion made is that the drop of the delay for \( S(4, 3) \) and \( S(5, 3) \) is minimal, so any extra segregation has not offered anything more to the network’s performance. In this case, it would be preferred to keep the number of channels to be used in the network to a minimum to maintain a better spacing and thus less interference.

![Figure 5.21. The average delay in seconds of a 4 channel segregated network over noise increase](image)

**Figure 5.21.** The average delay in seconds of a 4 channel segregated network over noise increase.
Figures 5.21 and 5.22 present the drop of the end-to-end delay over a various number of segregated networks using 4 and 5 channels within each subnetwork respectively. In the first case where 4 channels are utilised, the segregated network with modulo technique manages to perform efficiently against noise increase. Even though noise gets the highest value, the delay decreases as the network is divided into smaller subnetworks. Once $S$ gets values of $S$ (4, 4), due to the increased total number of channels deployed, $N_o$ and ACI prevent the network from further improvement. Its delay and the values achieved in this case are similar to the ones for $S$ (5, 4). Any further increase to the network segregation simply drops the connectivity between the nodes because of the decrease in the density and resulting in an increase to the delay.

On the other, hand in Figure 5.21, the delay hops to its minimum, but the rate of dropping is very small when noise level increases. This is due to the existence of ACI and the increased $N_o$ from the environment.

From the results, in a real life scenario the optimum and most cost saving network configuration would be for $S$ (4, 4). The drop of the delay does not justify the use of the extra channels as these create more problems in a noisy environment. However in a
In a non-noisy environment the best solution is $S(5,3)$ and when noise starts increasing, the benefits of modulo are restricted and the optimal solution regarding costs in network setup and complexity would be given by $S(4,4)$. In noisy environments it is proven that lowering the density $\lambda$ of nodes that operate on the same channel degrades the network’s performance. Next parameter to investigate is the number of collisions that take place inside the network for the above mentioned scenarios.

### 5.4.2 Network collisions in a noisy and heavy loaded network

Another metric, which is investigated (Paraskelidis and Adda, 2008) describes the performance of the network in terms of the QoS it provides, can be assessed by the number of collision that occur inside the network. Collisions occur due to low connectivity between the nodes operating on the same routing path. In the case of multi-channel networks, the collisions demonstrate the efficiency of the channel assignment algorithm (CAA) for handling the communications between the nodes that operate on the same channels. In the previous chapter (section 4.4.4.2), it was shown that the network segregation with a unique single channel for every subnetwork was able to reduce the number of collisions against a network with a single channel for the whole number of nodes $n$. The results presented in this section were performed using the same network configuration as set in the previous scenarios.

![Increase of Collisions over 3 channels](image)

**Figure 5.23. Increase of collisions over noise for 3 channels per subnetwork**
The results of Figure 5.23 depict in percentage (%) the increase of the collisions that take place within the simulated area over a single channel network, as presented in (section 4.4.4.2) when $S$ gets values between $S \{2, 3\}$ and $S \{5, 3\}$. These calculated collisions include those that occur between the network nodes by the moment AODV initiates the ROUTE_DISCOVERY process, until when the last data packet reaches the destination node. The different coloured columns represent the level of segregation over three different values of noise. The starting point of the results are the collisions when $N_o$ is equal to 6 and as $N_o$ increases the calculated collisions increase also. For $N_o=10$ the best performer is for $S \{5, 3\}$ but the average percentage of increase is close to the rest as the effect of $N_o$ is not severe. For $N_o=18$, the best performance is achieved again for $S \{5, 3\}$ but the gap from the rest increases and it is about 10% compared to 6% when $N_o=10$. These results come as confirmation to the trend of the results in the previous sections.

![Increase of collisions over 4 channels](image)

**Figure 5.24. Increase of collisions over noise for 4 channels per subnetwork**

In the scenario above, the channels for each subnetwork are set to 4 and $S$ gets values between $S \{2, 4\}$ and $S \{5, 4\}$. For $N_o=10$ the differences for various subnetworks are
small and this happens because the transmissions are not significantly disturbed from $N_o$, and the use of 4 channels within each subnetwork manages to relay successfully the packets. On the other hand, for $N_o=18$, there is a reverse trend on the performance of the network for $S(4, 4)$ when compared to $S(5, 4)$. It was shown in the previous section that the delay of the network for $S(4, 4)$ is low. Thus, one would expect a smaller number of collisions as reported in Figure 5.24. For $S(5, 4)$ the network simply utilises too many channels (20 channels) resulting in an increase of ACI in addition to the noise $N_o$, and the wireless links become too vulnerable to interference thus making them prone to fail.

![Increase of Collisions over 5 channels](image)

**Figure 5.25. Increase of collisions over noise for 5 channels per subnetwork**

In the case of 5 channels per subnetwork, for low $N_o$ the network seems to perform better than any other scenario. The problem appears when $N_o$ increases and starts affecting the quality of the wireless links. It's obvious that the gap between 4 and 5 segregates is very small. This difference keeps getting smaller as noise increases for $N_o=14$ and at the end for $N_o=18$ $S(5, 5)$ takes the lead over $S(4, 5)$ and percentage of increase matches that for $S(3, 5)$. The reason behind this is mainly related to the
large number of channels used in the network and the increase of $N_{AC}$ noise (ACI) due to low channel spacing $C_{sp}$.

### 5.4.3 Nodes retransmissions for a noisy environment

The next metric to be evaluated is the number of retransmissions that take place within the network. There are some important differences from the previous scenarios and are related to the type and amount of traffic that has to be sent over the network. The connections established are single-TCP connections as in the case of HTTP protocol. The aim of the simulations is to assess the QoS that the network offers for connections that require confirmation that a packet was received by the receiver. Unlike, the CBR that was used before does not require any acknowledgments (ACK) for the packets sent as it was only flooding the network with packets without checking if they reached the destination. The total number of TCP transmissions initiated is set to 10, much more than the three transmissions used before by CBR. In this way, the network is loaded heavily and demonstrates its ability to deliver all the transmitted packets to the receiver. The results presented are an extension of the results presented in the Chapter 4 (section 4.4.4.3).

The values for the retransmissions presented in Figure 5.26 include any type of retransmission that took place due to CTS timeouts, ACK timeouts, fragment ACK timeouts and dropped packets because the retransmission time count was exceeded.
Figure 5.26 presents the number of the retransmissions that occurred during the simulation for 2 hours. One observation worth mentioning is the drop of the amount of the retransmissions when compared to the results of the single channel un-segregated network in Chapter 4 (4.4.4.3). In that particular scenario, the number of retransmissions (RTXs) reached very high values despite the existence of RTS/CTS mechanism as the network seems to suffer from the existence of co-channel interference. With the segregation of the network, the number falls dramatically, almost by 43%. As can be seen from Figure 5.26, the use of 3 channels reduces further more the number of RTXs up to 53% for $N_o = 18$. 

![Figure 5.26. Number of retransmissions using 3 channels per segregate network](image)
With the utilisation of 4 channels within each subnetwork and despite of the existence of \( N_o \), the network segregation and modulo achieve even lower levels of RTXs achieving a reduction of 57% for the case \( S(5,4) \).

Figure 5.27. Number of retransmissions using 4 channels per segregate network

Figure 5.28. Number of retransmissions using 5 channels per segregate network
Finally, with the utilisation of 5 channels for every subnetwork, the decrease in the volume of the RTXs is 61% for $N_o = 18$ and compares to the single channel network for the same amount of $N_o$. The best that can be achieved is for $S (4, 5)$ and not for $S (5, 5)$ and the reasons are related to the existence of $N_o$ and have already been explained in the previous sections. Having a closer look on the rate of decrease over the three scenarios, it should be mentioned that this rate becomes smaller as more channels are utilised in every subnetwork. The reason behind this is that the network starts to reach its limits because the spacing between the channels used becomes too small and results in an increase of $N_{\Delta C}$ with more collisions between the nodes.

5.4.4 End-end-delay in a noisy and heavy loaded network

The delay is also studied and depends on the network’s set up. A network is considered to be heavy loaded when it is flooded with 10 TCP connections from multiple side nodes and the number of destination nodes might be similar in size or smaller.

![Figure 5.29. The average delay in seconds of a 3 channel segregated network over noise increase](image-url)
Figure 5.29 shows the end-to-end delay when using three channels within each subnetwork for various numbers of subnetworks when $N_o$ takes three different values. When compared to the results of Figure 4.18 in the previous chapter (section 4.4.4.3), the delay decreases rapidly once the network starts being segregated and with the help of modulo, it is able to achieve an efficient delay. The additional segregate networks help the network to route data faster as the ratio between traffic routes and subnetworks decreases. Traffic routes to subnetworks ratio was initially mentioned in (section 4.4.4.3) and the same scenario was implemented for subnetworks using a single channel.

![Image: 4 Channels Delay Graph](image)

**Figure 5.30. The average delay in seconds of a 4 channel segregated network over noise increase**

The extra channels inside each subnetwork and the additional segregation help the network to improve the end-to-end delay and reduce it much further. It should be noted that the rate decrease of the network delay is greater compared to the results discusses in the previous chapter (section 5.4.1). An explanation to this is that in the case of load scenarios, the traffic flows did not take full advantage of the network’s capacity resulting in a marginal delay reduction. The limits of the capacity of the network have not been investigated within this thesis. Another assumption made out of the results is that in a
very noisy environment, the network suffers from the interference produced by the neighbours and for $S (5, 4)$ the delay is, approximately 87 ms, which is a low value.

![5 Channels](image)

**Figure 5.31.** The average delay in seconds of a 4 channel segregated network over noise increase

In Figure 5.31, the end-to-end delay decrease for the average noise scenarios whereas for $N_o=18$ it is stabilised once $g=4$. This happens because, in addition to the high noise, the multiple transmissions increase the number of channels operating and accordingly the ACI increases. The delay reduction shown by Figure 5.31, when it is compared to Figure 4.18 of Chapter 4 (section 4.4.4.3) is the result of the utilisation of modulo technique and the extra capacity it offers.

**5.5 Conclusion**

The main difference between modulo technique and channel assignment protocols presented in Chapter 3 is its ability to utilise the maximum available spectrum of the 802.11b standard. The use of non-overlapping channels actually wastes the existing bandwidth in the spectrum by avoiding using partially overlapping channels in the fear of the ACI.
The encapsulation of Modulo in AODV and their implementation inside a segregate network is able to increase the network’s performance and QoS when compared to an ad-hoc network that deploys 1 single channel for all nodes. Modulo and network segregation was tested for both noisy and non-noisy environments. In the non-noisy environments, the network’s performance using modulo outperforms a simple single channel network and the segregated networks which do not utilise modulo. First, the end-to-end delay of a segregated network using modulo decreases significantly despite the appearance of ACI from the overlapping channels. The interference of ACI is encountered through the network segregation by reducing the number of nodes density, thus minimising the possibility that within the transmission range of a node, there will exist enough neighbouring nodes that operate in the same pool of channels. Also Modulo and AODV contribute to the general capacity of the network by increasing the available paths and providing multiple simultaneous transmissions.

Since this thesis focuses on wireless networks in noisy environments, the parameter of external noise $N_o$, apart from ACI, was introduced to the simulated scenarios. This type of noise contributes negatively to the SNR of a transmitter resulting in smaller transmission ranges and consequently to less connectivity and weaker links between neighbouring nodes. The GlomoSim simulator was chosen due to its accurate physical layer interference model, which can affect higher layer performance comparisons (Takai et al, 2001). In particular, GlomoSim’s SINR (Signal to Interference-plus-Noise Ratio) calculation taking into account the cumulative interference power from all concurrent senders is very important for measuring the effect of MAC collisions in our simulations.

The end-to-end delay was calculated for various levels of noise as well as other metrics such as the collision numbers and packet retransmissions. QoS was improved for high values of $S(g, k)$, but this improvement was reduced for high levels of $N_o$, resulting in $S$ performing the same for lower number of segregate networks and available channels. When the pool channel includes many channels, the ACI reaches high levels due to the small spacing between the overlapping channels used. This increase in ACI combined with the high level of noise $N_o$, prevented neighbouring nodes from establishing strong
and reliable links. On the other hand, for smaller values of $S$ which can be considered as achievements when combines segregated networks and modulo into a more realistic and plausible approach. Since the network can offer similar (or near) performance for less segregated networks and/or using less channels, this reduces the network’s complexity and at the same time drops the potential cost for a real-life deployment.
6 Conclusions and Further Work

6.1 Conclusions

The thesis has proposed and examined a channel assignment algorithm (Modulo) deployed in segregated noisy environments based on a novel concept. Modulo is a multi-hop multi-channel assignment algorithm that takes advantage of the benefits of network segregation. Network segregation is not a new concept for computer networks as is currently deployed in wired and wireless and used to increase a network’s security. The concept of segregation is adopted inside a multi-channel ad-hoc network by dividing a wireless network into subnetworks and assigning each one with one or more channels to operate.

The simplest form of network segregation uses a single channel for communication between the nodes of the same subnetwork. The remaining subnetworks operate on a different frequency to avoid collisions due to co-channel interference. It was shown that the segregation of a wireless network using just one channel for every subnetwork reduces significantly three important parameters of network performance, end-to-end delay, the number of collisions occurring in the network and finally the retransmissions that have to be performed for lost packets. At the same time it improves the available route paths and offers the flexibility of simultaneous independent transmissions.

Modulo was introduced aiming to enable the interoperability of multiple channels for every subnetwork. Every subnetwork is assigned variable numbers of partially overlapping channels that take advantage of the full spectrum of 802.11b networks in comparison to previous proposals that operated only on non-overlapping channels and they actually wasted the available bandwidth within overlapping channels. The three previous parameters examined for single segregated networks were also examined and the results show a further improvement on network’s performance. Even though the utilisation of partially overlapping channels creates adjacent channel interference to their neighbours, its impact on the quality of wireless links proves to be less severe.
Another parameter introduced to the simulations and which was not conducted in previous works, was the appearance of extra environmental noise affecting the strength of the transmitted signals. Segregated networks with modulo managed to keep the QoS of the network in high levels and minimising the degradation of the network’s operating performance.

Network segregation and modulo provide a simple and generic approach for the configuration of wireless networks that can be adopted in current technologies without requiring any hardware enhancements. Throughout the simulation, a generic hardware was used employing more than one radio and the only enhancement was done on the routing algorithm, the AODV. No changes were performed on the routing discovery and selection aspects of AODV and the only enrichment was on its selection and utilisation of multiple channels as defined by the operating characteristics of Modulo. This concept ensures the backward compatibility of existing technologies thus avoiding new complex implementations that would probably require changes to the hardware characteristics, for example changes to the MAC layer. Next section discusses the future work for Modulo and network segregation in the field of ad-hoc networks.

### 6.2 Future Work

The aim of the work presented in the thesis was to enable the operability of wireless networks in noisy industrial environments by dividing into smaller subnetworks and achieving better network performance utilising multiple channels under the control a channel assignment algorithm called Modulo.

One of the first improvements that could be performed for the proposed network configuration is the deployment of 802.11g protocol. The proposal of the thesis was based on the deployment of 802.11b nodes. Since both protocols are backwards compatible (BT, 2008), the network’s performance can be further improved by taking into account the higher transmission rates of the 802.11g standard.

The proposed network configuration was tested for medium scale industrial areas of about 300x300 meters. The operations of modulo approach are irrelevant to the size of
the simulated area. On the other hand, the network segregation is strongly related to the number of networks deployed and the simulated area. The density of the simulated area plays a major role on the performance of the network and when it is increased, a higher number of segregated networks can be implemented thus providing more available routes for data transmission. A future approach would be to increase the size of the simulated areas and evaluate the benefits of network segregation for larger scale networks that could possibly cover the entire physical area of a company and include more types of traffic, apart from the already mentioned test results from sensors.

The network formation implemented in this thesis follows a static approach of the definition of a segregate network. Currently, the number of segregate networks depends on the total number of nodes deployed in the network. Depending on the number of flows that have to go through the network and after the set up of the routing paths, many of the existing nodes are not utilised and remain idle. There might exist sometimes some subnetworks that are not used at all because there are no sufficient flows to utilise them resulting in a waste of the available channels while they could be used for any existing transmissions.

An improved approach on this issue would be a dynamic network segregation, which would divide the network into subnetworks depending on the number of traffic flows produced by the sources. While in the static approach, there is a specific number of available channels for each subnetwork, with the dynamic approach each subnetwork would be able to use more or even less channels depending on the number of nodes that are included in the routing path. When the number of intermediate nodes increases so will the number of utilised channels for this particular path. In this way, one can reduce the possibility that two nodes operating on the same frequency would actually interfere because of the large physical distance between them. Any shorter routing paths would be assigned less channels because of the small number of intermediate nodes. The dynamic approach could increase significantly the utilisation of the available resources, nodes and channels, when compared to the static approach where the channels assigned to each subnetwork are predefined during the segregation process.
References


BECK AND TEWS, 2008 - Practical attacks against WEP and WPA


EFDA, 2009 - The Joint European Torus team, FROM: http://www.jet.efda.org/ on 13/06/05


EULER, 1741 - Euler L., "The Seven Bridges of Königsberg " Commentarii academiae scientiarum Petropolitanae 8: 12.


IEEE802.11, 2007, FROM: http://standards.ieee.org/getieee802/802.11.html on 26/10/07


162


KO ET AL., 2005 - Ko B. J., Misra V., Padhye J., Rubenstein D., "Distributed Channel Assignment in Multi-Radio 802.11 Mesh Networks", New York, Columbia University, 2005


LOUIS E. FRENZEL 2004 Wireless Industrial Networks—Untether Monitoring And Control http://electronicdesign.com/Articles/ArticleID/8763/8763.html


PROFIBUS Tech, 2002 - PROFIBUS Technology and Application, PROFIBUS Brochure, No.4.0002_v, October 2002.

PROXIM, 2003 - WIRELESS NETWORK SECURITY white paper.


SCOURIAS, 1997 FROM : http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html on 10/11/07


USROBOTICS, 2001 - USRobotics "Virtual Local Area Networks", whitepaper on computer networks by USRobotics, FROM: www.usr.com on 19/10/07


ZIGBEE, 2008 - FROM: The Zigbee Alliance, www.zigbee.org/ on 18/05/07

7 Appendices

7.1 Terminology and notation

This subchapter will describe the terminology and notation used throughout the thesis. A number of other terms and notation will be used but these will be described when the terms are introduced.

**Time:** Time is represented by \( t \) and a number of variables will be denoted as a function of time to indicate that their value changes throughout the simulation.

**Node:** A node is a network device equipped with one or more wireless radios installed depending on the scenario it is deployed in. The nodes are static and randomly placed within the simulated area for better coverage of the simulated area, they have their own power source thus batter starvation is not an issue. The total number of nodes used inside the wireless network is designated by \( n \).

**Neighbour:** A neighbour is described from the point of view of a node. A neighbour of a node is any other node which is in communication range.

**Subnetwork:** A subnetwork is the result of network division and its numbers vary depending on the scenario and the simulation parameters. The number of segregate networks deployed is designated by \( g \).

**Channel:** A channel is defined as the range of frequencies that can be used during the transmission between two neighbouring nodes and they are concentrated around a single centre called the channel centre. Channels are designated by \( c \).

**Noise:** Is the power of interference affecting a single node and is calculated as the sum of all signals on the channel other than being received by the radio.
7.2 Simulation environment

7.2.1 Introduction

Simulations are used throughout the thesis to analyse the performance of various aspects of the proposal and to determine the best practice before moving forward. Simulation is widely used in the ad-hoc networks research community due to the high complexity of modelling such scenarios mathematically (Naoumov and Gross, 2003). Additionally it is prohibitively expensive to provide real world analysis and so simulation is a feasible alternative.

When designing a simulation environment one must consider the real world expected application of any technique. In this thesis, it is assumed that the technique will be used in a medium-scale industrial network such as replacing the wired infrastructure already existed.

7.2.2 Simulator

A number of simulators exist for wireless networks such as DARPA ns-2, Jist/SWANS (Barr, 2004) and Glomosim (UCLA., 1998). Each provides an approximation of a wireless ad hoc network simulating radio frequency propagation, MAC protocols, node mobility, with the difference being that only Glomosim provided the ability to provide a noisier environment through the NOISE-FIGURE parameter included to the configuration file. The algorithm was developed in Glomosim due to its ability to process larger numbers of nodes than similar products. The main drawback of GlomoSim was the lack of a graphical environment for configuring the simulated scenarios. The provided configuration ability was text-based and when the scenarios included large numbers of nodes, segregated networks and utilised channels, made the configuration of the networks a very time consuming process.

The collection of the results was also text-based and in the case of large networks the time consumed was considerable long until they were distinguished and prepared in a presentable format. Due to the range of the metrics used in the simulation, each metric
required the simulations to be performed more than once to finally manage collect the desirable results.

The channel assignment algorithm, modulo, is implemented at the network layer and the code introduced to GlomoSim is considered as an add-on over the existing AODV routing algorithm. This reduces the complexity of the proposed algorithm and maintains the simplicity of the general network concept, avoiding complex and hard to implement solutions in real life scenarios minimising the need of using proprietary hardware.

7.2.3 Simulation parameters

There is a large diversity in the number of simulation parameters used in the various scenarios. There are two general categories when simulating the proposed algorithm. A noisy and a non-noisy were the two general environments used in to evaluate the proposed network architecture and channel assignment algorithm.

For non-noisy environments, the scenarios simulated were mainly related to the number of available nodes inside the whole simulated area for variable transmission ranges. When the number of nodes increases their transmission ranges decreases in an attempt to reduce the interference between them but also to force AODV to use more intermediate nodes for the established routing paths. The numbers of nodes fall within the ranges of 20 up to 130 nodes for a static simulated area and they are placed randomly.

For noisy environments, the main criterion to evaluate the performance of the network was the variable levels of external noise existing in the simulated area. For every simulated scenario, before the presentation of the results, the parameters are presented and explained. A table usually described the general parameters used and any changes to them are explicitly mentioned.
7.2.4 Presentation of results

Most of the results presented in this thesis are presented in scatter graph form with lines of best fit to demonstrate trends. Four simulations are performed of any combination of parameters to ensure validity of the results. The result of these simulations is then presented on the graph as one point.

Because of the diversity of the scenarios and the large variations of the value differences, sometimes presented graphs do not actually manage to represent in detail and accurately the variation between the simulated scenarios. In such cases, trying to avoid any misunderstandings to the presented results, explanatory graphs are used.

7.2.5 GloMoSim 2.03 installation in Windows XP

Before Installation:

GloMoSim requires the following software to run; most of the university owned PCs have all of them installed. However, you need to make sure you have enough access rights of defining the computer environmental variables.

- Microsoft VC++ version 6.0 (Essential)
- JAVA JRE version 1.2 or higher (For VT)
- JAVA SDK version 1.2 or higher (For VT)

Step-by-Step Installation Guide:

1. Download GloMoSim 2.03, unzip and save (say save to "C:\glomosim\glomosim")

2. Go to glomosim/Parsec, open folder 'windows-nt-vc6.0', copy all files into Parsec directory. Delete all other folders under Parsec directory (since they are for other OS)

3. Set pcc environmental variables (For Parsec)
   1) My Computer -> Properties -> Advanced -> Environmental Variables
   2) New "PCC_DIRECTORY", value = "C:\glomosim\parsec"
   3) Set path "C:\glomosim\parsec\bin"
4. Set VC6.0 environmental variables (if default, go to step 5)
   1) Set include: "C:\Program Files\Microsoft Visual Studio\VC98\MFC\Include; C:\Program Files\Microsoft Visual Studio\VC98\Include"
   2) Set lib: "C:\Program Files\Microsoft Visual Studio\VC98\MFC\Lib; C:\Program Files\Microsoft Visual Studio\VC98\Lib"
   3) Set path: "C:\Program Files\Microsoft Visual Studio\Common\MSDev98\Bin"

5. Check pcc environment by "pcc -Cenv" in DOS prompt (cmd)

6. GloMoSim Installation
   1) Go to glomosim\glomosim\main, do "makent.dat"
   2) Go to glomosim\glomosim\bin, find "glomosim.exe"
   3) Test glomosim. Under DOS: "glomosim config.in"
   4) "glomo.stat" is generated after simulation, compare with "glomo.stat.sample"

7. Build GloMoSim Visualisation Tool (VT) "C:\glomosim\glomosim\JAVA_GUI", type "javac *.java", enter

8. GloMoSim is now ready to use.
   Tips for Troubleshooting
   1. Step 6.1, "cl" not recognised
      Go to "\Microsoft Visual Studio\bin", do "vcvars32.bat"
   2. Step 8, "warning LNK4099: PDB, vc60.pdb" was not found

   Local access restrictions, does not affect VT, ignore it

7.3 Gateway nodes

In an attempt to improve the performance of single channel segregate networks and examine if AODV actually selects the shortest path to a destination, the concept of gateway nodes is introduced. While in a WMN gateway nodes are the point of communication between the WMN and the Internet, in a segregated network gateways
play exactly the same role but between the present subnetworks. The idea was, gateway nodes to be able to listen to all available channels operating in the network. This node would interconnect the various subnetworks and relay data from one subnetwork to the other hoping that a shortest route would be found. The role of the gateway could be assigned to every possible node in the network as long as its position was the middle of the area.

The number of gateways can vary but it was decided to test the idea using up to 3 for every subnetwork trying to keep the complexity of the network low and evaluate their performance once the first results were collected. Soon this idea was abandoned because actually the segregate network with its current static form, fails to utilise efficiently the existence of the gateway node. The result of introducing the gateway nodes was actually to convert these nodes into bottlenecks as no restrictions were set to AODV regarding the number of flows that could go through them. Apart from the phenomenon of bottleneck, the general utilisation of the network was dropping even more as fewer nodes were actually active and taking part in the routing paths. Thus the idea was suspended and it will be included to the improved version of segregate networks, the dynamic segregate network.

7.4 Graph theory

The channel selection problem in multi-radio wireless networks because of the existence of interference from neighbouring nodes emerged the essence of a more detailed representation in graph theory. As a result, the graph colouring theory is used as the base for the mathematical modelling of channel assignment problem. In the early days of mobile telephony the channel assignment problem was modelled as an ordinary graph colouring problem and graph colouring algorithms were used to solve it (Katzela and Naghshineh, 1996).

In graph colouring, the color of each vertex represents a non-overlapping channel and the goal of the channel assignment is to cover all vertices with the minimum number of colors such that no two adjacent vertices use the same channel. This type of representation is beneficial only when the node has only one interface and a different
presentation is required in order to capture multiple interfaces on each router. As shown in Figure 7.1, the colors, in this case patterns instead of colors, are assigned to edges instead to vertices. Edge coloring assign a color to each edge so that no two incident edges share the same color.

![Figure 7.1. Graph coloring of a multi-radio wireless network](image)

The theory on graph colouring is extensive and the fundamental definition of weighted colouring problem is given by Diestel: “A proper colouring of a graph G is an assignment of a colour to each vertex so that adjacent vertices receive distinct colours.” (Diestel, 2005) Equivalently, it is a partition of the vertices into stable sets, where a set of vertices in G is stable (or independent) if no two are adjacent. This problem is known to be NP hard (Garey et al., 1974, Garey and Johnson, 1979).

Over the past years there have been numerous publications on attempts to calculate the interference level inside a wireless network using weighted colour graphing. Mishra et al. used weighted colouring graph with the weight calculation based on a number of clients that are affected by the interference of an access point on a particular channel (Mishra et al., 2005a). Another attempt using weighted graph colouring in the form of interference graph was from Leith and Clifford. In their model each vertex was not representing a wireless node but a whole WLAN and each of the edges were used to represent the interference between the corresponding WLANs (Leith and Clifford, 2006). A similar approach to the one of Mishra et al. was presented by Ramachandran et al. and it extended the conflict graph model further into the multi-radio conflict graph (MCG). The main difference from Mishra’s approach was that the new model represented the edges between the radios as vertices instead of representing edges between the wireless nodes as vertices as in the original conflict graph (Ramachandran
et al., 2006). It should be noted that although the models based on graph colouring theory have proven their usefulness in modelling interference on infrastructure WLANs, Raniwala and Chiueh correctly point out that graph colouring models do not sufficiently capture all the constraints, such as partially overlapping channels and interference from external sources, of a multi-radio wireless network (Raniwala and Chiueh, 2005).

Finally, when we are talking about graph theory and multi-radio wireless mesh networks (MR-WMN), there are different ways to represent such a network. Below there is a presentation of the three most common examples of such representations and their relation to the channel selection problem but should not be considered as the optimal solutions. These three examples are the following:

- **Link graph** – In this representation each line between nodes represents a link that exists between interfaces of two nodes. A channel number is used for each link that is assigned.
- **Connectivity graph** – This type of graph each line represents a probable connection between two interfaces only when these two are within each others communication range.
- **Interference graph** – In this case, the edges between the nodes represent the interference between two links. An edge is illustrated for each link that can be a source of interference that is independent of its type, for example physical or contention interference. Therefore such a graph can have no edges if all the channels used are orthogonal to each other.

According to these examples, below there are some graphical representations of various scenarios of MR-WMNs. The complexity of each network varies and can either be a simple network of 2 single interfaces or a more complex network that contains four nodes and each one accommodates 2 interfaces.
In Figure 7.2 is show the three different representations of three WR-WMN varying in number of nodes and number of interfaces on each node. In the first example, there is only one possible link between the two nodes with two interfaces in total operating in channel 6. Their interference graph has no edges since there is no other interfering channel operating within their communication range. In the second example, there are three nodes with 3 single interfaces and they all operate on the same channel, thus there are only three possible links within the network. Also, since all nodes use channel 6 for communication, there is contention interference between them. In the last example, there are three nodes and each node has two interfaces and they all operate in different channels. The connectivity graph is getting more complex because of the dual interfaces on each node and the result is to have 11 possible links between the 3 nodes. On the other hand, the interference graph once more has no edges since as the 3 links operate on orthogonal channels.

From the above examples it can be concluded that even they can capture the contention interference from neighbouring nodes that are within their communication range.
range they really fail to represent any signs of physical interference from external sources or the interference range of other nodes. Such a problem is one of the basic contenders that have to do with the constraints and the challenges in channel assignment and they are explained below.