Ph.D. Thesis

Contributions to the Routing of Traffic Flows in Multi-hop IEEE 802.11 Wireless Networks

Ph.D. Candidate: **Miguel Catalán Cid**

Ph.D. Advisors: **Josep Paradells Aspas and Carles Gómez Montenegro**

A thesis submitted in partial fulfillment for the degree of

Doctor of Philosophy in Network Engineering

Department of Network Engineering, Wireless Networks Group

Universitat Politècnica de Catalunya, BarcelonaTech

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

entel

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola de Doctorat

Curs acadèmic:

Acta de qualificació de tesi doctoral

Nom i cognoms
___

Programa de doctorat
___

Unitat estructural responsable del programa
___

Resolució del Tribunal

Reunit el Tribunal designat a l'efecte, el doctorand / la doctoranda exposa el tema de la seva tesi doctoral titulada ____
____.

Acabada la lectura i després de donar resposta a les qüestions formulades pels membres titulars del tribunal, aquest atorga la qualificació:

☐ NO APTE ☐ APROVAT ☐ NOTABLE ☐ EXCEL·LENT

(Nom, cognoms i signatura) President/a	(Nom, cognoms i signatura) Secretari/ària	
(Nom, cognoms i signatura) Vocal	(Nom, cognoms i signatura) Vocal	(Nom, cognoms i signatura) Vocal

______________________, _______ d'/de __________________ de _______________

El resultat de l'escrutini dels vots emesos pels membres titulars del tribunal, efectuat per l'Escola de Doctorat, a instància de la Comissió de Doctorat de la UPC, atorga la MENCIÓ CUM LAUDE:

☐ SÍ ☐ NO

(Nom, cognoms i signatura) President de la Comissió Permanent de l'Escola de Doctorat	(Nom, cognoms i signatura) Secretari de la Comissió Permanent de l'Escola de Doctorat

Barcelona, _______ d'/de ____________________ de _________

Abstract

Multi-hop Wireless Networks have proved their suitability in infrastructureless deployments, providing robust connectivity by means of autonomous mechanisms. In addition, the constant improvements of the IEEE 802.11 standard, along with the high availability and low cost of Wi-Fi devices, has raised the popularity of Multi-hop IEEE 802.11 Wireless Networks (MIWNs) in scenarios which demand better performance and Quality of Service. However, the standard was not initially designed to provide multi-hop capabilities. Due to contention and interference, a data flow can suffer considerable delays and packet losses throughout its path. Also, other phenomena like radio propagation issues, mobility or channel capacity can degrade the performance of the traffics. One approach that can mitigate these limitations relies on routing flows through appropriate paths and channels. Considerable research effort has been devoted to the design of routing protocols, routing metrics and channel assignment strategies which consider some of these issues applying a cross-layer approach. This thesis presents and evaluates novel contributions in this research area with the aim of improving the performance of traffic flows traversing MIWNs.

Keywords: IEEE 802.11, MIWNs, cross-layer, interference models, link quality, route creation, route maintenance, channel assignment, AODV, simulations.

Agradecimientos

Sin lugar a dudas, esta tesis no hubiera visto la luz sin sus directores. Gracias a Josep por su orientación durante todos estos años (que ya van siendo unos cuantos) y por confiar en mi para las diferentes becas, proyectos e incluso trabajos (que también empiezan a ser ya unos cuantos). Ya hasta le estoy cogiendo el gusto a pelearme con cacharros del tamaño de una moneda (creo). Gracias también a Carles por sus propuestas y correcciones (¡muchas correcciones!). Sobre todo por este sprint final durante la revisión de la tesis.

Gracias al resto de la gente del WNG, especialmente a mis compañeros de andanzas durante estos años en el C3. Tampoco estaría escribiendo estas líneas sin las risas, conversaciones y chimpanzadas varias del día a día su lado (¡banana!).

Y antes de dejar el ámbito académico-laboral, gracias también a las entidades que han apoyado de algún modo esta tesis: MEC, AGAUR, UPC, Pi2p e i2CAT. Agradecimiento recortado para las que han hecho recortes.

Entrando ya en lo familiar, pero de hecho aún sin dejar la universidad, muchas gracias a mí hermana Marisa por su apoyo y cariño diario. Y por ese 10% de comida que le habré robado durante todos estos años ☺. Gracias también a mis padres, por todo.

Finalmente, mi agradecimiento infinito a Teresa por hacerme feliz cada día (o noche) que llego a casa. Por aguantar mis silencios pensando en enlaces y transmisiones, los “cuando acabe la tesis…”, las tardes y noches de PC, los mordiscos en los bolis… Te quiero. ¡Esto no se para!

Ph.D. Thesis

Contributions to the Routing of Traffic Flows in Multi-hop IEEE 802.11 Wireless Networks

Ph.D. Candidate: Miguel Catalán Cid

Ph.D. Advisors: Josep Paradells Aspas and Carles Gómez Montenegro

This work was supported in part by the Spanish Government's Ministerio de Economía y Competitividad through project TEC2012-32531 and by the TEC2009-11453 project, FEDER and the FPU MEC fellowship (AP2008-02720).

Contents

List of figures

List of tables

1

Introduction

In recent years, being ubiquitously and permanently connected has become a necessity for modern life. Mobile connectivity has evolved into a fundamental commodity for humans, essential for business and social living. In addition, the Internet of Things (IoT) has defined a new communication paradigm where physical objects also demand Internet connectivity. Indeed, by the end of 2014 the number of active mobile connections surpassed world population for the first time[1], while, according to [1], in 2019 the data traffic from wireless and mobile devices will exceed the traffic from wired ones.

Since its definition in 1997, Wireless Local Area Networks (WLAN) based on the IEEE 802.11 standard [2] has rapidly become one of the most popular ways to provide mobile connectivity. The utilization of unlicensed Industrial Scientific Medical (ISM) frequency bands facilitates and reduces the cost of WLAN deployments, while the constant amendments of the 802.11 standard, in terms of capacity, security or Quality of Service (QoS), among others, have improved its performance in order to comply nowadays user requirements. Also, the appearance of the Wi-Fi Alliance[2] in 1999, a global non-profit industry association which promotes Wi-Fi certification and assures interoperability between devices of different manufacturers, is one of its key success factors. For instance, since 2013 more than 2 billion of Wi-Fi certified devices are sold per year, expecting to reach 4 billion in 2020 [3].

[1] According to https://gsmaintelligence.com/ statistics
[2] http://www.wi-fi.org/

A significant characteristic of the IEEE 802.11standard is its capacity to create different network architectures. The most basic and usual one is the hotspot deployment, where a central node acts as a relay of the communications between the rest of stations and, usually, as a gateway to the Internet. However, ad hoc topologies, which allow direct communication between stations, are also possible. Multi-hop networks can be seen as a special case of ad hoc communications, where the nodes can also act as routers to permit communication between out-of-sight nodes.

The origins of wireless multi-hop networks were military [4][5], as was the case of other networks like the Internet; multi-hop routing permits to configure networks in a dynamic and autonomous way, which facilitates the deployment of temporary infrastructureless networks as is the case of military or emergency scenarios. In recent years, the popularity of the IEEE 802.11 standard and the vast number of cheap off-the-shelf Wi-Fi products available on the market, has increased the commercial and academic interest on this technology [6][7]. This is raising new challenges and research issues [8][9][10][11].

However, the Medium Access Control (MAC) layer of the IEEE 802.11 standard was not initially designed to provide multi-hop capabilities and, therefore, it does not appropriately handle the issues of medium sharing and interference in these environments [12][13][14][15]. Typical drawbacks of wireless communications, like half-duplex behavior or the existence of hidden nodes, become reproduced several times along the multi-hop path, significantly degrading the performance of the flows.

One approach that can mitigate these limitations relies on routing flows through proper paths. Initial routing protocols for multi-hop networks, which were defined by the IETF’s Mobile Ad-Hoc Networks group (MANET)[3], were more devoted to create and maintain network connectivity, being well suited for temporary deployments but less appropriate for cases where certain QoS is demanded. Therefore, considerable research effort has been devoted to enhancing route creation in wireless multi-hop networks [16][17][18]. In particular, due to the impact of Physical (PHY) and MAC layers on traffic performance, cross-layer designs have become an interesting and challenging topic [5][17][18]. Indeed, in recent years a specific amendment of the 802.11 standard for multi-hop networks was defined by the IEEE, 802.11s, which integrates routing procedures in the MAC layer and adopts some of the solutions of the previous research on routing protocols for Multi-Hop IEEE 802.11 Wireless Networks (MIWNs) [2][19][20].

---

[3] https://tools.ietf.org/wg/manet/

On the contrary to route creation procedures, less attention has been paid to the impact of route maintenance on traffic performance. Once the optimal route is created, the quality of the flow during its lifetime should be assured. Routing protocols usually monitor the state of the links in order to react to phenomena like mobility or fading which can lead to route breaks [21][22]. However, the arrival of new flows can also degrade significantly the quality of active ones by increasing the congestion and the interference of the network [13][23][24]. Therefore, route maintenance procedures which react according to the performance of the active flows can entail considerable benefits.

Another way to overcome Wi-Fi limitations in multi-hop networks is the utilization of multi-radio solutions. The high availability of IEEE 802.11 modules, together with their price and size reduction, has favored the appearance of multi-radio nodes. By using the different orthogonal channels defined by the standard, concurrent adjacent transmissions do not incur in interference and the performance of multi-hop networks improves significantly [25][26]. Since the number of channels is usually higher than the number of interfaces of the nodes, channel assignment algorithms should be defined. However, their utilization in multi-hop networks is very challenging because of the dependency between routing and channel assignment [27][28].

The scope of this thesis is focused on the challenges of these two research areas, routing and multi-radio solutions, being its main motivation to improve the performance of traffic flows traversing MIWNs. Next section details the objectives or contributions of this thesis.

1.1 Objectives of this thesis

From the above motivation, the following are the main contributions of this thesis:

- Study on how different phenomena related with PHY and MAC layers affect the performance of the flows in MIWNs.
- Definition of a wireless interference model which weights the interference level of a link according to the relative position of the nodes, the load of the traffics and the characteristics of the links.
- Design and evaluation of a routing protocol which creates on-demand routes in a per-flow basis, permitting a finer granularity in the control of traffic flows.
- Design and evaluation of a routing metric based on contention- and interference-awareness.

- Design and evaluation of a preemptive route maintenance solution for on-demand routing protocols, allowing route recovery according to the monitored performance of the active flows.
- Study of traffic performance in multi-radio scenarios according to different routing protocols, routing metrics and channel assignment algorithms.
- Design and evaluation of a dynamic and distributed channel assignment algorithm based on interference-awareness.
- Design and evaluation of route recovery solution which joins channel assignment and preemptive local repair.

Although the contributions of this thesis are focused on the routing layer, they come from the study of the lower layers in a cross-layer approach. Nevertheless, designed solutions rely on information available at the network layer, so that they are not limited to particular network interface card drivers or hardware. Indeed, although generally being evaluated by means of simulation studies, the contributions presented in this thesis have a practical orientation and the study of solutions which can be applied to actual devices and deployments has been prioritized.

1.2 Structure of this thesis

The structure of this thesis is organized in eight chapters and two appendixes, the first of which is dedicated to this introduction.

- **Chapter 2** presents the main concepts of MIWNs. First, the IEEE 802.11 standard and its amendments are briefly introduced. Then, the basics of its PHY and MAC are described, especially the mechanisms and parameters which may impact the performance of traffic flows. Finally, an overview of multi-hop networks and their applications is given, including details about experimental and simulation platforms.
- **Chapter 3** presents some of the initial analysis and conclusions which motivate the elaboration of the thesis. Different phenomena and issues related with PHY and MAC layers are described, and their impact on multi-hop networks is analyzed. Also, mechanisms to estimate and model their effect on the performance of traffic flows are introduced. In recent years, most research on cross-layer enhancements to multi-hop routing has been focused on some of the topics covered in this chapter.
- **Chapter 4** deals with the route creation procedure, which, logically, determines in a great measure the final performance of a flow. First, the basics of proactive and reactive routing are presented. Then, the relevant research on routing metrics is surveyed. Finally, the

proposed approaches to enhance route creation in MIWNs are described. The Flow-based Ad-hoc On-demand Distance Vector routing protocol (FB-AODV) permits to create routes in a per-flow basis, instead of the classic routing procedure based on destinations. On the other hand, the Weighted Contention and Interference routing Metric (WCIM) uses contention- and interference-awareness in order to obtain the best route for a determined route. The benefits of both mechanisms are analyzed and compared to other state-of-the-art solutions.

- **Chapter 5** describes and analyzes a preemptive solution for on-demand routing, which aims to detect performance degradations on active routes and recover the affected flows. While state-of-the art preemptive approaches are devoted to anticipate link breaks in mobile scenarios, the developed mechanism permits to react to other issues which impact traffic performance, like congestion or interference.
- **Chapter 6** deals with channel assignment in MIWNs. Although multi-radio devices can make use of orthogonal channels to decrease interference between adjacent flows, a proper channel distribution is necessary in order to maximize performance without compromising the connectivity of the network. In this chapter the different benefits, problems and trade-offs of channel assignment solutions are discussed. Also, two distributed and dynamic channel assignment algorithms are proposed and analyzed.
- **Chapter 7** presents the conclusions and contributions of this thesis. Also, it gives a brief overview on some possible ways to extend this work in the near future.
- **Appendixes I and II** describe two research projects related to the topics of this thesis. The first one motivated the elaboration of this thesis, while the second one is a practical application of a multi-radio solution.

2

Multi-hop IEEE 802.11 Wireless Networks

This chapter introduces the main concepts, characteristics and mechanisms of Multi-hop IEEE 802.11 Wireless Networks (MIWNs).

First of all, the basics of the IEEE 802.11 standard are described, paying special attention to the Physical (PHY) and Medium Access Layer (MAC) characteristics and methods which have an impact on the performance of traffic flows in multi-hop networks.

The second section of this chapter gives a brief overview of the actual applications of MIWNs. Also, since a significant part of the contributions of this thesis are supported by simulation results, this section includes a discussion about simulation models, parameters and characteristics.

2.1 IEEE 802.11 standard

IEEE 802.11 standard is the de-facto radio interface for Wireless Local Area Networks (WLANs) and is one of the most popular wireless technologies due to the free utilization of the industrial, scientific and medical (ISM) radio bands. The standards, developed by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802), define the Wireless LAN MAC and PHY Specifications. First published in 1999 (802.11-legacy), it has experienced two main modifications, 802.11-2007 and 802.11-2012 [2], which incorporate new approved amendments. Table 2.2 summarizes the amendments contained in the last revision of the standard, 802.11-2012, while Table 2.3 describes the actually approved amendments to be included in the next revision of the standard, which is expected in 2015. Finally, Table 2.4 introduces the possible future amendments to the 802.11 standard, which are currently in the draft phase. As shown in these tables, due to the different amendments, IEEE 802.11 has experienced a constant improvement of capabilities [29]: higher data rates, higher security, QoS support, new operation bands, etc.

Amendment	Description
802.11a	**High-speed Physical Layer in the 5 GHz Band (revision 2007)** Uses Orthogonal Frequency-Division Multiplexing (OFDM) in the 5 GHz ISM band. Permits link rates from 6 Mbps up to 54 Mbps.
802.11b	**Higher Speed Physical Layer Extension in the 2.4 GHz band (revision 2007)** Enhances the Direct-Sequence Spread Spectrum (DSSS) PHY of 802.11-legacy to allow 5.5 Mbps and 11 Mbps link rates.
802.11d	**Additional regulatory domains (revision 2007)** Adds support for operation in countries not included in the actual standard and permits the interoperation of devices from different countries.
802.11g	**Further Higher Data Rate Extension in the 2.4 GHz Band (revision 2007)** Defines an OFDM-based PHY in the 2.4 GHz ISM band. Permits link rates from 6 Mbps up to 54 Mbps. Implements backward compatibility with 802.11b by using the DSSS-based PHY (link rates from 1 Mbps up to 11 Mbps).
802.11h	**Spectrum Managed 802.11a (revision 2007)** Provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) capabilities to 802.11a in order to minimize interference with radar and satellite systems working on the 5 GHz band.
802.11i	**Enhanced Security (revision 2007)** Overcomes the security problems of the previous scheme, Wired Equivalent Privacy (WEP), by using more robust algorithms. Its implementation is also known as Wi-Fi Protected Access 2 (WPA2).
802.11j	**4.9 GHz - 5 GHz Operation in Japan (revision 2007)** Adds channels and frequencies to permit the operation of 802.11a in Japan's 4.9 GHz and 5 GHz bands.
802.11e	**Enhanced Quality of Service (revision 2007)** Modifies the MAC layer in order to allow the prioritization of traffic flows in the MAC procedures.
802.11k	**Radio Resource Measurement of Wireless LANs (revision 2012)** Defines and provides radio channel information.
802.11r	**Fast Basic Service Set Transition (revision 2012)** Improves client’s handoffs between access points.

Table 2.1: Amendments included in the IEEE 802.11-2012 standard (part 1).

Amendment	Description
802.11y	**3650–3700 MHz Operation in USA (revision 2012)** Permits the operation of 802.11a in the 3650–3700 MHz in USA. Devices in this band can use higher transmit power than in the ISM band.
802.11w	**Protected Management Frame (revision 2012)** Extends 802.11i enhancements to management frames.
802.11n	**Enhancements for Higher Throughput (revision 2012)** Obtains data dates up to 600 Mbps by using Multiple-Input Multiple-Output (MIMO), increasing the channel width and allowing frame aggregation.
802.11p	**Wireless Access in Vehicular Environment (revision 2012)** Modifies 802.11a to allow longer ranges of communication (up to 1 km) and high speed vehicles (up to 200 km/h).
802.11z	**Extensions to Direct-Link Setup (revision 2012)** Permits direct data transfer between two Wi-Fi clients that are part of the same network.
802.11v	**Management (revision 2012)** Permits the configuration of client devices while connected to wireless networks.
802.11u	**Interworking with External Networks (revision 2012)** Provides a framework for interworking with external networks, as GSM.
802.11s	**Mesh Networking (revision 2012)** Modifies 802.11 in order to permit the creation of multi-hop networks at the MAC layer.

Table 2.2: Amendments included in the IEEE 802.11-2012 standard (part 2).

Amendment	Description
802.11aa	**Enhancements for Robust Audio/Video Streaming** Enhances the QoS support of 802.11e for improving the performance of audio and video streaming.
802.11ac	**Enhancements for Very High Throughput for Operation in Bands below 6 GHz.** Enhances 802.11n in order to obtain link rates of the order of gigabits per second.
802.11ad	**Enhancements for Very High Throughput in the 60 GHz Band** Permits link rates of the order of gigabits per second in short range line-of-sight communications (around 10 meters).
802.11ae	**Prioritization of Management Frames** Enhances 802.11e to permit the prioritization of management frames.
802.11af	**Television White Spaces Operation** Allows operation in TV white space spectrum in the VHF and UHF bands between 54 and 790 MHz. Uses cognitive technology in order to avoid busy channels.

Table 2.3: Amendments to the IEEE 802.11-2012 standard, which will be included in the next revision.

Amendment	Description
802.11ah	**Sub 1 GHz License Exempt Operation** Permits operation in license-exempt bands under 1 GHz. Well-suited for IoT and M2M since it provides long transmission ranges and low energy consumption for short and infrequent one-hop communications.
802.11ai	**Fast Initial Link Setup** Improves different operations related with the initial link setup. For instance, it provides a faster authentication and roaming, and decreases signaling overhead.
802.11aj	**Enhancements for Very High Throughput to support Chinese millimeter wave frequency bands** Permits the operation of 802.11ad in the 45 GHz band, which is unlicensed in some countries like China.
802.11ak	**Enhancements For Transit Links Within Bridged Networks** Improves bridging between Wi-Fi and Ethernet for media communications.
802.11aq	**Pre-Association Discovery** Provides mechanisms to advertise services at the MAC layer in order to discover them in the pre-association phase.
802.11ax	**Enhancements for High Efficiency WLAN** Improves 802.11ac in order to obtain link rates of the order of tens of gigabits per second.
802.11ay	**Enhanced Throughput for Operation in License-Exempt Bands Above 45 GHz** Improves 802.11ad by extending its capacity (up to 20 Gbps) and range.
802.11az	**Enhancements for Positioning** Permits a Station to identify its absolute and relative position to another station or stations it's either associated or unassociated with.

Table 2.4: Draft amendments to the IEEE 802.11 standard.

The main application of the standard is the hotspot deployment, where client stations (STAs) work in infrastructure mode and associate to an Access Point (AP). The AP acts as centralized intermediary of the communications between clients and, most usually, as a gateway to the Internet. In addition to this case, the standard permits the creation of ad hoc networks, where direct communication between STAs is allowed. Multi-hop IEEE 802.11 networks make use of the ad hoc mode and the routing capabilities of the STAs to allow the creation of multi-hop topologies.

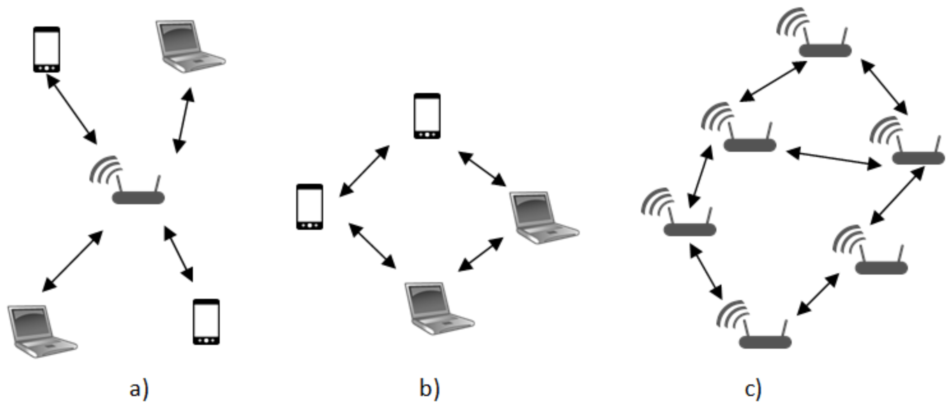


Fig. 2.1: IEEE 802.11 topologies: (a) Infrastructure, (b) Ad Hoc and (c) Multi-hop

Although the IEEE 802.11 standard was not initially designed to provide multi-hop capabilities, as will be analyzed in the next chapter, the constant increase of bandwidth and the availability of multiple channels reduce the impact of the increasing and uncontrolled contention and interference in the shared channel. In addition, the vast number of cheap, commercial, off-the-shelf IEEE 802.11 products available on the market, has fueled the popularity of IEEE 802.11-based multi-hop networking, which nowadays is the forerunner in topic research, product development and network deployment of wireless multi-hop MANs and LANs. Therefore, in 2004 the IEEE started a Task Group to propose a Mesh Networking amendment, 802.11s, which was finalized in 2011 and added to the standard revision of 2012 [2].

The following sections deal with processes and characteristics of the IEEE 802.11 standard which impact the performance of MIWNs. Section 2.1.1 introduces some characteristics of the PHY layer, while Section 2.1.2 details the processes of the MAC layer. Without loss of generality, these two sections are focused on 802.l1a/b/g amendments, which nowadays still are the most common technologies in multi-hop networks. Finally, Section 2.1.3 introduces multi-hop and multi-channel MAC proposals, including 802.11s.

2.1.1 Physical Layer

The Physical layer of 802.11 defines two main transmission techniques: Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency-Division Multiplexing (OFDM) [2]. DSSS was defined in the initial standard and actually is only used in the 2.4 GHz band by 802.11b and 802.11g, this last for assuring backward compatibility. On the other hand, OFDM, which was initially defined in 802.11a, has been also adopted by later amendments like 802.11g, 802.11n and 802.11ac. Some of the main advantages of OFDM are its high spectral efficiency, its robustness to channel fading and interference, and its fast and low cost implementation using Digital Signal Processing (DSP).

The following sections introduce some details about the Physical layer of the standard, focusing on bit rates, available channels, frames format and carrier sensing.

2.1.1.1 Modulations and bit rates

The original standard, 802.11-legacy, specifies DSSS radios which make use of a Barker sequence of 11 bits (+1−1+1+1−1+1+1+1−1−1−1) to spread the signal. I.e., each data symbol is transmitted as a sequence of 11 bits. Since the symbol rate is 11 Mega Symbols per second (MSps), depending on the modulating selected, Differential Binary Phase Shift Keying (DBPSK) or Differential Quadrature Phase Shift Keying (DQPSK), 802.11-legacy allows bit rates of 1 Mbps and 2 Mbps, respectively. The 802.11b amendment introduces two additional bit rates by using Complementary Code Keying (CCK) as modulation scheme. CCK improves the coding rate, thus allowing 5.5 Mbps and 11 Mbps bit rates. In order to be compatible with 802.11b devices, 802.11g also implements DSSS.

Modulation	Bits per Symbol	Coding Rate	Bit rate
DBPSK	1	1/11	1 Mbps
DQPSK	2	1/11	2 Mbps
CCK	1	4/8	5.5 Mbps
CCK	2	4/8	11 Mbps

Table 2.5: DSSS-based PHY bit rates (802.11b/g)

On the other hand, 802.11a defines OFDM as radio technology. It uses 64 sub-carriers, where 48 of them are available for data transferring. I.e., 48 bits are paralleled transmitted during the symbol duration of 4 microseconds, leading to a symbol rate of 12 MSps. As shown in Table 2.6, depending on the modulation and the coding rate, 802.11a allows bit rates from 6 Mbps up to 54 Mbps. Later amendments as 802.11g, 802.11n and 802.11ac also adopted OFDM as radio technology. While 802.11g basically adapts 802.11a in the 2.4 GHz band, 802.11n and 802.11ac make use of wider channels, parallel spatial streams using MIMO and additional modulations, in order to obtain higher bit rates.

Modulation	Bits per Symbol	Coding Rate	Bit rate
BPSK	1	1/2	6 Mbps
BPSK	1	3/4	9 Mbps
QPSK	2	1/2	12 Mbps
QPSK	2	3/4	18 Mbps
QAM-16	4	1/2	24 Mbps
QAM-16	4	3/4	36 Mbps
QAM-64	6	2/3	48 Mbps
QAM-64	6	3/4	54 Mbps

Table 2.6: OFDM-based PHY bit rates (802.11a/g)

The IEEE 802.11 standard does not define any method to determine and set the best bit rate for a transmission. Higher bit rates are desirable, but as they use more bits per symbol and less redundancy, they are less robust to noise and interference. I.e. they need a higher Signal to Interference plus Noise Ratio (SINR) to obtain an acceptable Bit Error Ratio (BER)[1]. Since the wireless medium is very variable, driver's manufacturers implement Rate Adaptation Algorithms (RAAs) [30][31]. Basically, there are two main types of RAAs:

- **Trial and error:** the driver constantly tries to change the bit rate of the interface. If several consecutive transmissions are successful, the rate is increased. If several frames are erroneous, the rate is decreased. This is the case of the first published RAA, called Automatic Rate Fallback (ARF) [32].
- **Monitoring and testing:** the driver monitors the statistics of the transmitted packets and uses probe packets to test different rates of the one being used. Periodically, it applies an algorithm to decide which rate offers the best performance. The *mac80211* framework[2], which is the main framework to implement IEEE 802.11 drivers for Linux kernels, implements one RAAs of this type, which is called Minstrel [33][34].

2.1.1.2 Channels

IEEE 802.11 defines a Multi-Channel Architecture (MCA), where multiple channels are available to perform a communication [2]. The number of available channels depends on the ISM band and

1 In wireless LAN applications, a BER better than 10e-5 is considered acceptable.
2 https://wireless.wiki.kernel.org/en/developers/documentation/mac80211

the regulatory domain. Without loss of generality, hereinafter Europe's regulation will be considered.

The 2.4 GHz band defines 13 channels, which central frequencies are separated by 5 MHz; the first channel is centered in 2.417 GHz and the last one, channel 13, in 2.472 GHz. In the case of the 5 GHz band, the separation between adjacent channels is 20 MHz and 19 channels are available in Europe. Since the use of this band can interfere with radar applications, the band is divided in three frequency ranges with different conditions of use:

- 5150 - 5250 MHz (channels 36, 40, 44 and 48): Indoor deployments.
- 5250 - 5350 MHz (channels 52, 56, 60 and 64): Indoor deployments, DFS and TPC are mandatory (802.11h).
- 5470 - 5725 MHz (channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140): Indoor or outdoor deployments, DFS and TPC are mandatory (802.11h).

In order to reduce the interference between adjacent channels, the standard specifies a spectral mask in transmissions and sets limits on the maximum out-of-band power relative to the peak power level. In the case of 802.11b, as shown in Fig. 2.2a, the signal must be attenuated at least by 30 dB from its peak power level at ±11 MHz from the center frequency, leading to an effective channel width of 22 MHz. Therefore, taking into account the channel width and the separation between adjacent channels, the theoretical number of non-overlapping channels in the 2.4 GHz band is 3 (channels 1, 6 and 11), as show in Fig. 2.2b.

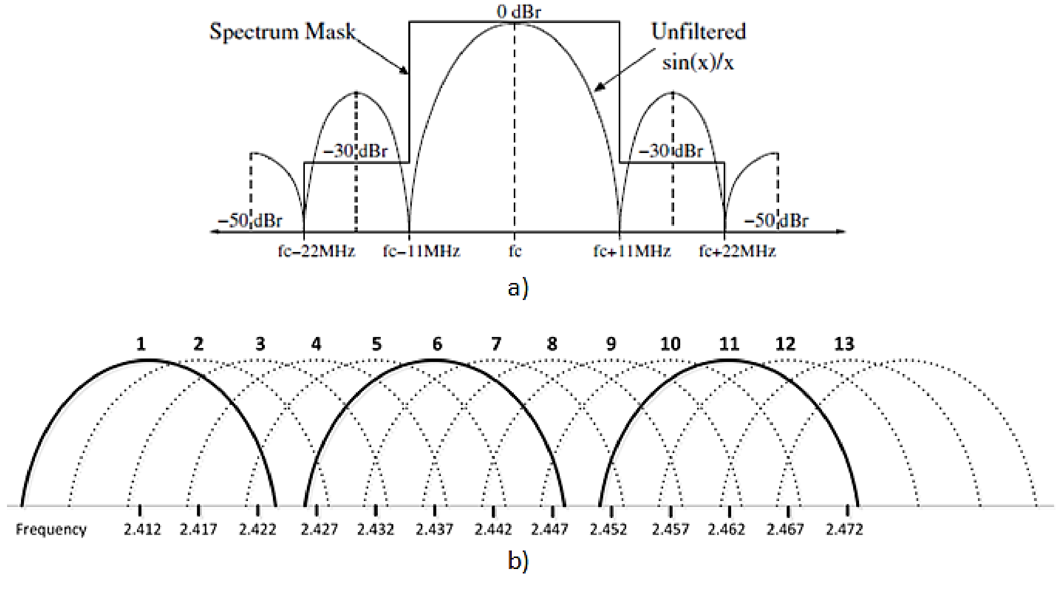


Fig. 2.2: 802.11b/g: (a) Spectral mask and (b) channels overlap

In the case of 802.11a/g, where channel width is 20 MHz, the attenuation at ±11 MHz must be at least 20 dB. Indeed, in OFDM 12 of the 64 sub-carriers are set to 0 in order to reduce interference, thus, the effective channel width is about 16.5 MHz. As shown in Fig. 2.3, using 802.11a/g in the 5 GHz band, all 19 channels are orthogonal.

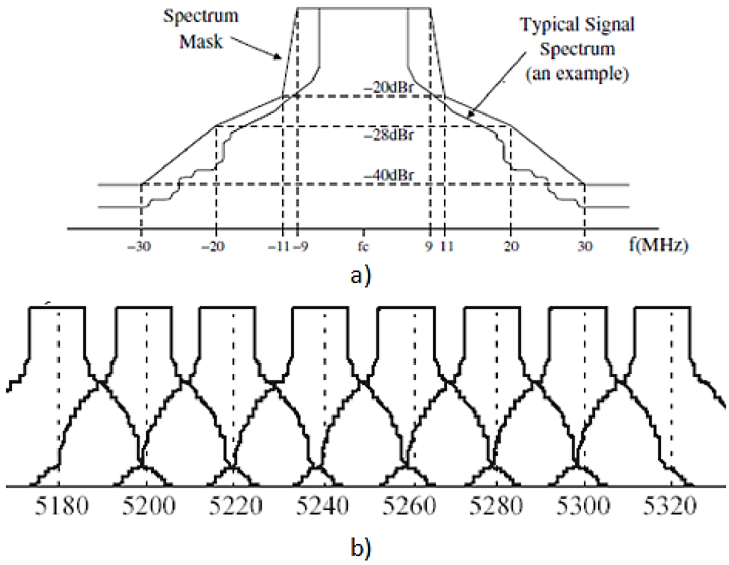


Fig. 2.3: 802.11a/g: (a) Spectral mask and (b) channels overlap

Later amendments, like 802.11n (2.4 GHz and 5GHz band) and 802.11ac (5GHz band), permit wider channels in order to obtain higher bit rates, thus reducing the number of orthogonal channels. While 802.11n can use bandwidths of 40 MHz, 802.11ac can use 80 MHz and even 160 MHz wide channels [35], leading to a Single-Channel Architecture (SCA) where the whole frequency range is occupied by a single channel.

As in the bit rate case, the standard does not define any mechanism to decide and assign the best channel for a communication. 802.11h specifies DFS, but it is oriented to avoid interfering on radar deployments. Thus, external Channel Assignment Algorithms (CAAs) are necessary.

2.1.1.3 Physical Frames

The PHY frame of the IEEE 802.11 standard, the so-called Physical Layer Convergence Procedure (PLCP) Protocol Data Unit (PPDU), basically consists on a small preamble, a header and the data from the higher layers (PSDU) [2].

Fig. 2.4 shows the format of the PPDU for the DSSS-based PHY. The SYNC field is a string of 0's and 1's and is used by the receivers to detect the frame and perform synchronization. The SFD field defines the beginning of the frame with a predefined sequence of bits. Regarding the PLCP Header, the Signal field identifies the bit rate or modulation of the PSDU; the Service field gives additional information about the modulation and permits to extend the length field; the Length field is the length of the PSDU; and the CRC is the checksum of the PLCP Header.

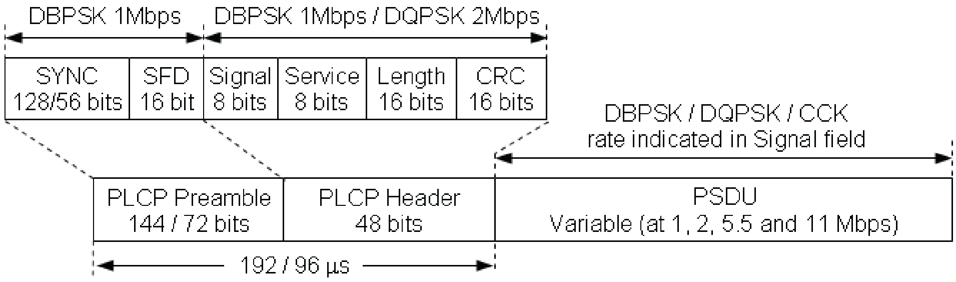


Fig. 2.4: DSSS-based PHY PPDU (802.11b/g)

Fig. 2.5 shows the format of the PPDU for the OFDM-based PHY. As in the DSSS case, the PLCP Preamble is used for detection and synchronization, while the PLCP Header carries the PSDU rate and length, among other parameters needed for frame decoding.

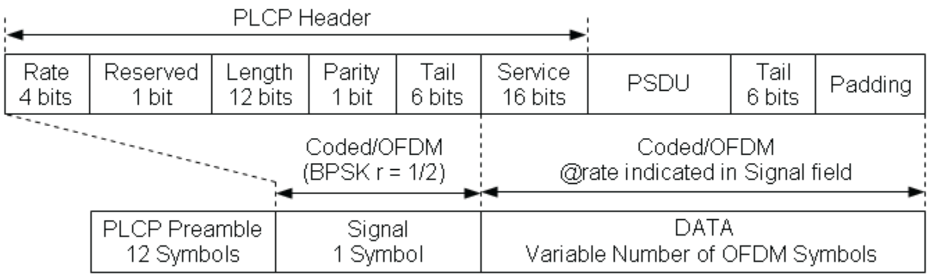


Fig. 2.5: OFDM-based PHY PPDU (802.11a/g)

While the PSDU is transmitted using the actual bit rate of the interface, the PLCP Preamble and Header must be transmitted using the lowest bit rate of the technology in order to assure that all the nodes which receive the frame are capable to decode them, since both are in order to avoid collisions. As will be detailed next section, Preamble Detection (PD) is used in order to detect an active transmission and the PSDU rate and length is used to compute its duration.

Finally, since the PLCP Preamble and Header increase the overhead of each transmitted PSDU, 802.11b/g permits the use of a short preamble and a higher data rate for the PLCP Header. This way, the overhead of the PLCP frame using the short preamble is reduced from 192 microseconds to 96 microseconds. In the case of 802.11a/g, the overhead per frame consists on a fixed part of 52 microseconds (13 Symbols) and a variable overhead of 22 bits plus the padding bits transmitted at the PSDU bit rate.

2.1.1.4 Carrier Sensing

As will be detailed in Section 2.1.2, in order to avoid collisions the MAC layer of IEEE 802.11 needs to know the status of the channel; if it is idle, transmission is permitted; if it is busy, transmission is deferred. Therefore, the standard defines the Clear Channel Assessment (CCA) function, which permits two PHY mechanisms in order to sense channel status: Preamble Detection (PD) and Energy Detection (ED) [36].

- **Preamble Detection**: When a preamble is detected, the CCA indicates a busy status to the MAC layer, which will defer any transmission or initiate reception if the node is the destination of the frame. The duration of the busy status is determined using the rate and length fields of the PLCL Header. Even if a loss of carrier occurs, the CCA will indicate a busy status for the intended duration of the received frame.
- **Energy Detection**: Using Energy Detection the channel can be sensed as busy if the Received Signal Strength Indication (RSSI) measured is greater than a defined threshold.

In 802.11a both methods are mandatory and the ED threshold is defined as 20 dB above the sensitivity of the minimum bit rate, i.e. -62 dBm [2]. On the other hand, IEEE 802.11b standard specifies that the nodes be capable of doing CCA either by PD or ED or a combination of both; the ED threshold is a value between -80 dBm and -70 dBm, depending on the transmission power, while the typical sensitivity at the minimum rate is around -95 dBm [2].

In conclusion, since preambles are transmitted at the minimum bit rate, if PD is active, ED is only needed when preambles are missed, what is very unusual in 802.11 since the radio is usually always active, or if there is a cumulative interference of simultaneous transmitters.

2.1.2 Medium Access Control Layer

The IEEE 802.11 standard defines two mechanisms to manage the access to the shared wireless medium: Point Coordination Function (PCF) and Distributed Coordination Function (DCF) [2]. The PCF method works only in infrastructure mode; it is coordinated by the AP, which polls the different stations in order to exchange data. Since it is not mandatory in the standard and is not included in the Wi-Fi certification, its implementation is marginal.

On the other hand, DCF defines a distributed method for coordinating the access to the medium, which basic mechanism is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Next Section describes the basic characteristics of CSMA/CA, while Section 2.1.2.2 presents two significant optional mechanisms or extensions: the Virtual Carrier Sensing and the QoS enhancements of 802.11e.

2.1.2.1 CSMA/CA basic access

CSMA/CA uses physical carrier sensing to determine the status of the medium and avoid collisions, as introduced in Section 2.1.1.4. Before attempting a transmission, nodes sense the medium and wait until it becomes idle for a period of time called DCF Interframe Space (DIFS). Then, each node waits for a random time using an exponential backoff algorithm in order to avoid simultaneous transmissions. The backoff time is computed as x times the *aSlotTime* value of the technology, where x is a pseudorandom integer drawn from a uniform distribution over the interval *[0, Contention Window (CW)]*. If the medium becomes busy during the backoff delay, the timer is paused and resumed when the medium becomes idle again. When the timer ends, the node is able to transmit the frame. Fig. 2.6 resumes this procedure.

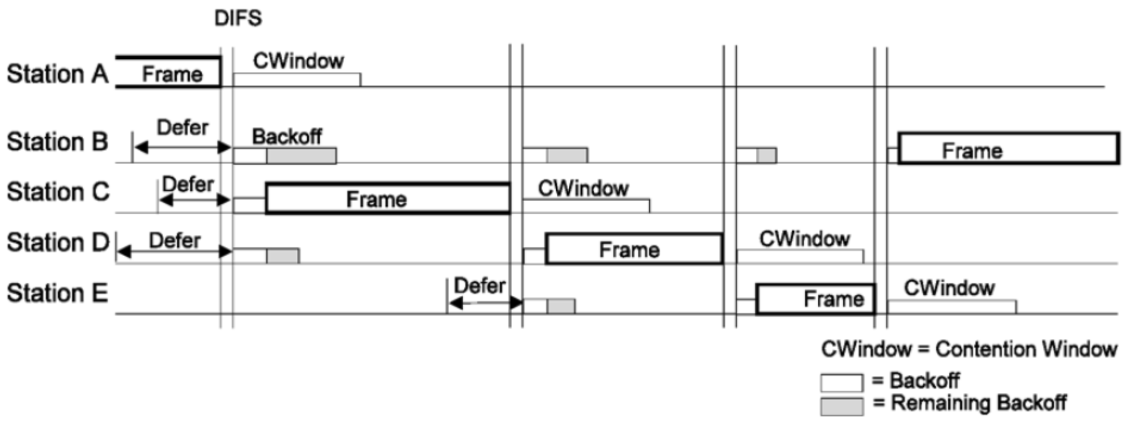


Fig. 2.6: Backoff procedure example [2]

In order to detect erroneous transmissions, the receiver sends a small acknowledgment frame (ACK) to the sender. The ACK is sent after a Short Interframe Space (SIFS) period, which is shorter than the DIFS in order to prevent deferred nodes to send its frames before the ACK. If the ACK is received by the sender, its CW value is reset to CW_{min}. If not, the CW value is doubled (until it reaches CW_{max} value), and, before attempting a retransmission, the sender must wait the channel to be idle during an Extended Interframe Space (EIFS) period, which is longer than the DIFS period.

2.1.2.2 Optional mechanisms and extensions

If all the nodes share the same contention domain, i.e. sense all transmissions, the CSMA/CA basic access reduces collisions to the cases where two or more nodes select the same backoff time. However, usually some nodes are hidden to each other, as is the case of multi-hop networks. As shown in Fig. 2.7a, nodes which are not aware of the transmission can interfere the receiver, leading to the well-known hidden-terminal problem. To prevent these cases, the IEEE 802.11

standard defines a Virtual Carrier Sensing (VCS) mechanism in order to extend the contention domain using control frames [2].

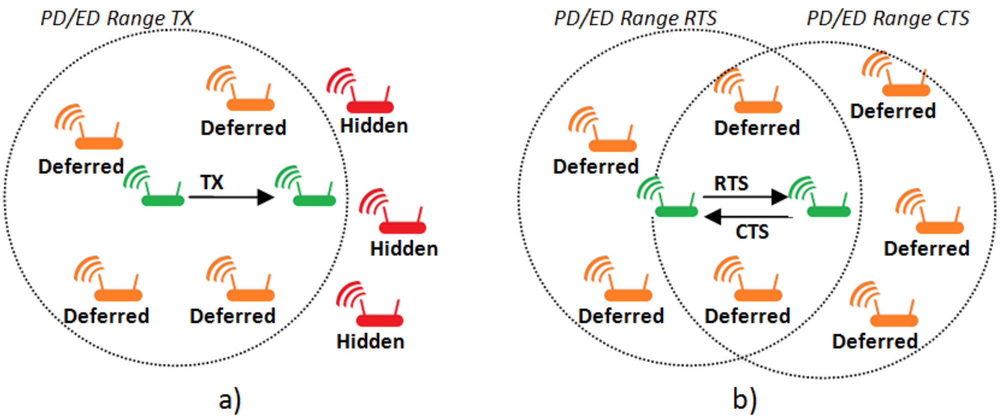


Fig. 2.7: Hidden-terminal scenario: (a) Physical carrier sensing and (b) virtual carrier sensing.

Using VCS, before transmitting a data frame, the sender transmits a Request to Send (RTS) frame. Then, after receiving the frame and waiting for a SIFS period, the receiver answers with a Clear to Send (CTS) if it has also sensed the channel as idle. After receiving the CTS and waiting a SIFS time, the sender can proceed with data transmission. The nodes which overhear the RTS or the CTS frame defer their possible transmissions for a time period specified in one of their fields. This way, as shown in Fig. 2.7b, the hidden-node problem is avoided. However, this mechanism increases the MAC overhead per frame. Thus, when active, it is only used for fames which size exceeds a threshold[3]. In addition, as will be described in the next chapter, its utilization in multi-hop networks can severely degrade the throughput [15].

Another significant extension which aims to increase the performance of the MAC standard in the presence of QoS traffic is the defined by 802.11e [2]. It defines the Enhanced Distributed Channel Access (EDCA) which instead of using DIFS permits waiting different periods of time called Arbitration inter-frame spacing (AIFS) according to data priority. Shorter AIFS periods lead to a higher priority of channel access, thus decreasing the delay of the packet. 802.11e also permits the transmission of consecutive frames avoiding channel contention during a period called Transmit Opportunity (TXOP), thus increasing the throughput. As will be denoted in next section, these characteristics of 802.11e have been included in the Mesh Networking standard 802.11s. Fig. 2.8 resumes the IFS relationships and the backoff procedure of CSMA/CA.

---

[3] Many vendors use a threshold higher than the maximum packet size of Ethernet, thus disabling RTS/CTS in the practice.

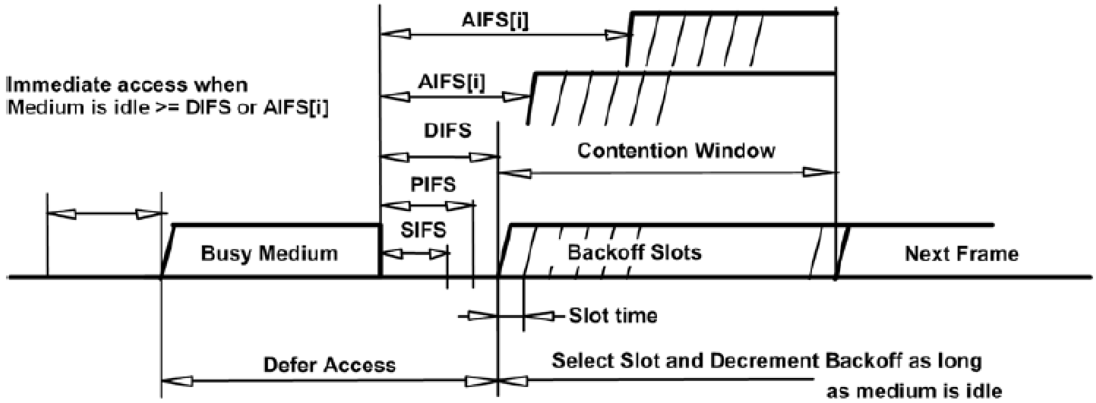


Fig. 2.8: IFS relationships using CSMA/CA [2]

2.1.3 Multi-hop MACs

As aforementioned, application of CSMA/CA in multi-hop networks entails several problems. Multi-hop paths increase the presence of contention periods and collisions due to the interference of other active flows or even due to the transmission of the same flow through different hops; the so-called inter-flow and intra-flow interference, respectively [37]. Thus, different state-of-the-art proposals try to improve the performance of CSMA on multi-hop networks by tuning its parameters or using cross-layer mechanisms [38]. Examples of the first type include modifying CW or backoff mechanisms. On other hand, cross-layer proposals include the modification of carrier sensing thresholds, the control of transmission power or the utilization of directional antennas, in order to increase spatial reuse or decrease the probability of hidden nodes.

MAC enhancements also can make use of the multiple available channels of the standard [39]. Single-radio devices need some type of coordination to assure that transmitters and receivers are in the same channel, like using a common channel to perform RTS/CTS handshake and decide the channel for data transmission, fixing time slots for control and data phases (split phase), applying a coordinated channel hopping scheme or using assigning fixed channels to each node during data reception [39]. Nevertheless, due to the price and size reduction of 802.11 radios, nowadays most multi-channel solutions assume multi-radio devices and a standard MAC layer, where channel assignment is seen as a procedure more related to the higher layers applying a defined algorithm [28].

2.1.3.1 802.11s

The 802.11s standard introduces some modifications to the MAC layer of 802.11 in order to permit routing procedures and improve the performance of multi-hop traffics [2]. The access to the medium is controlled by the Mesh Coordination Function (MCF). MCF has both a contention-based channel access and contention free channel access mechanism [40]. The contention based mechanism is EDCA, defined by 802.11e, while the contention free mechanism is called the MCF Controlled Channel Access (MCCA) and it is optional. With MCCA, nodes reserve TXOPs in advance, which are called MCCA opportunities (MCCAOPs), thus avoiding competition from other nodes during these periods.

Mesh routing is based on the Hybrid Wireless Mesh Protocol (HWMP) protocol, which is a variant of the Ad-hoc On-demand Distance Vector (AODV) routing protocol defined by the IETF's MANET group [41]. While the reactive part is mainly identical to AODV, HWMP protocol also allows a proactive routing procedure based on the formation of spanning trees [42]. The creation of paths utilizes the Airtime Link Metric (ALM), which is based on the transmission time of a link, according to the estimation of its data and error rates. Again, ALM is an adaptation of a state-of-the-art routing metric for multi-hop wireless networks, the Expected Transmission Time (ETT) metric [43]. In fact, although HWMP and ALM are defined as mandatory, 802.11s allows the utilization of different routing protocols and metrics by means of the extensible path selection framework, thus enabling the adaptation of other state-of-the-art proposals [2][20] [42]. Therefore, although an exhaustive analysis and evaluation of 802.11s is out of the scope of this thesis[4], most of its contributions can be adapted to this new standard.

2.2 Multi-hop IEEE 802.11 Wireless Networks

Depending on the characteristics and requirements of the network, the devices and the applications, the following typologies for Multi-hop IEEE 802.11 Wireless Networks can be considered [7]:

- **Mobile Ad Hoc Networks (MANETs):** Originally, any infrastructure-less wireless network was considered to be a MANET; indeed, the IETF working group in charge of routing standardization for wireless routing is also called MANET[5]. Nowadays, MANETs are considered to be dynamic networks, where topology can change frequently due to the mobility or joining/leaving of the nodes. Also, the nodes have heterogeneous characteristics (i.e. mobile phones, laptops, routers…), and their energy and processing

[4] During the realization of this thesis, the author supervised the Final degree project "IEEE 802.11s Mesh Networking Evaluation under NS-3" [44].
[5] http://datatracker.ietf.org/wg/manet/charter/

capacity can be limited [16]. The creation of a MANET is usually not planned and its main applications are military deployments, emergency/rescue operations or local level applications (e.g., information sharing in conferences or classrooms, or communication between home devices). Thus, routing protocols for MANETs should assure an efficient network autoconfiguration in dynamic topologies.

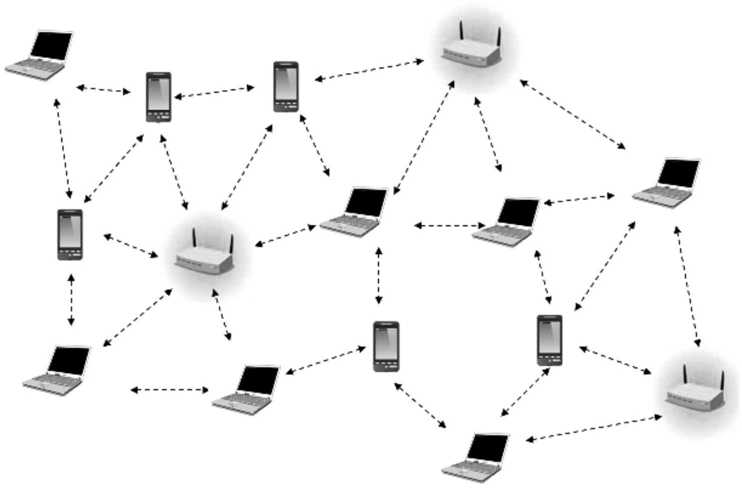


Fig. 2.9: Example of MANET network (extracted from http://www.thelifenetwork.org/)

- **Wireless Mesh Networks (WMNs):** Compared to MANETs, WMNs are more oriented to the formation of a wireless backbone that offers connectivity to wireless clients [7][18]. Mesh nodes are usually fixed, power-affluent and with a relative high processing capacity. The main applications of WMNs are related to the creation of local and metropolitan networks, offering intranet services (e.g. related with Smart Cities) or Internet access to its clients. Thus, routing protocols designed for WMNs should deal with QoS requirements, assuring an efficient routing of flows through the network.

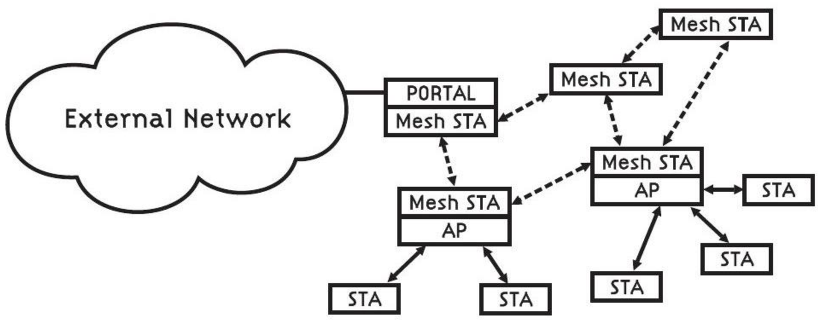


Fig. 2.10: Mesh Network topology as defined by 802.11s: Mesh STA forms the mesh network and, working as APs, offer connectivity to its clients (STA). Mesh STA which also offer connectivity to external networks, as the Internet, are called Portals.

- **Vehicular Ad Hoc Networks (VANET):** The principal characteristic of a VANET is the high mobility the nodes or vehicles that form the network [45]. Thus, routing protocols should deal with very frequent topology changes and link breaks. The main application of these networks is the exchange of information between vehicles and traffic elements in order to improve driving (e.g. avoid congestions, synchronize semaphores, alert of weather conditions or accidents…). Although the 802.11p is an enhancement of the standard for vehicular environments, it does not consider multi-hop routing in contrast to 802.11s case.

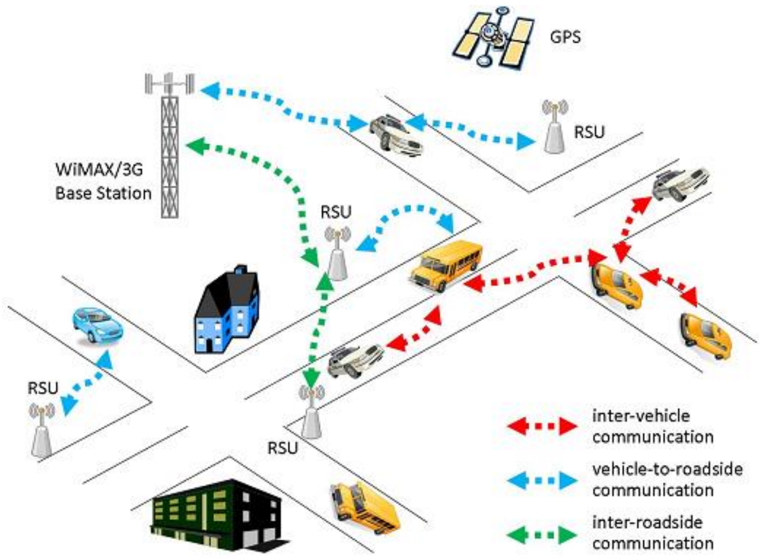


Fig. 2.11: Example of VANET network (extracted from www.cs.nthu.edu.tw)

The contributions of this thesis are oriented to MANET and Wireless Mesh Networks, since the differentiation between both typologies is sometimes vague. The following sections introduce some applications of MANET and WMN networks, including experimental and simulation platforms.

Due to its multi-hop nature, routing is the main mechanism of MIWNs and, thus, considerable research effort has been devoted to this topic [16]. As aforementioned, the MANET working group of IETF is the principal standardization entity related to routing in multi-hop wireless networks. From its origin in 1997, four different routing protocols have been defined and achieved an Experimental RFC status: Ad hoc On-Demand Distance Vector (AODV) [41], Optimized Link State Routing (OLSR) [46], Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [47] and Dynamic Source Routing (DSR) [48]. AODV and OLSR are the most significant and popular proposals and both are actually being revised with new versions: AODVv2 [49] (internet-draft) and OLSRv2 [50] (proposed standard RFC). Most state-of-the-art research and commercial protocols for MIWNs are based on these two protocols, depending on their routing nature: on-demand (AODV) or proactive (OLSR). For instance, as denoted in Section

2.1.3.1, the mandatory routing protocol defined by the 802.11s standard is an adaptation of AODV [2][42].

Indeed, the design of routing solutions is still an active research area [16][17][18]. While first multi-hop wireless networks were mainly applied to military or emergency deployments, where reliable and rapid network autoconfiguration and multipath discovery were the main requirements, nowadays applications require additional capacities like QoS, scalability, mobility support or energy-awareness, among others. These new applications require routing enhancements and, due to the characteristics of the wireless medium, most of them are based on cross-layer techniques [5][17][18]. On the contrary of wired networks, where traffic performance is basically influenced by the congestion, wireless networks add other uncertainties dependent on physical and MAC layers, like propagation, interference or contention [12][13][37]. In addition, as will be analyzed in Chapter 3, these problems become more complex to deal with in MIWNs because of the lack of a centralized management and the impact of multi-hop routing. Therefore, research on routing in MIWNs is principally centered on enhancing the following procedures:

- **Route creation:** Routing metrics should consider cross-layer parameters affecting the performance of the flows, like the quality of the links or the interference level [37][51][52]. The routing protocol should apply mechanisms in order to improve the quality of the flows, like load balancing or traffic differentiation [52][53].
- **Route maintenance:** A constant monitoring of link-quality and data performance is necessary to detect channel and network variability caused by different phenomena like mobility, external interference, fading or the arrival of new flows [53][54]. Active routes should change according to these variations in order to avoid performance degradations [54][55].
- **Channel assignment:** The utilization of multi-radio devices permits to integrate channel assignment and awareness into the routing decision in order to decrease contention and interference levels [27][56].

2.2.1 Relevant application cases

One of the main commercial applications of WMNs is the creation of wireless backbone networks in municipal or industrial environments [18][57]. Municipality WMNs permit the deployment of Smart City services: municipal internet and intranet access to the citizens or to the municipal workers, security and safety applications like video surveillance, maintenance services based on real-time monitoring, intelligent traffic signal management, etc. In a similar way, industrial WMNs can improve automation applications or workers tasks in mobile or complex environments by permitting data monitoring, M2M communications, Voice and Video over IP communication or remote surveillance. Also, WMNs can be used as connectivity solutions in campus, shopping malls or punctual events like congresses or concerts.

Relevant MIWNs device manufacturers and services integrators in this sector are ABB Tropos[6], Cisco Meraki[7] and Firetide[8], among others. Although their routing solutions are proprietary, requirements and characteristics are similar to the introduced in the previous section:

- The routing protocol of Tropos, called Predictive Wireless Routing Protocol (PWRP), creates routes proactively considering the quality of the links and uses multi-radio routes, including a combination of 2.4 GHz and 5 GHz bands.
- Meraki's routing solution, called SrcRR, is a reactive source-routing protocol based on DSR. The origin of Meraki was the Roofnet project at the Massachusetts Institute of Technology (MIT), which consisted on an experimental WMN formed by 40 nodes [21]. Although the original routing metric was also based on link-quality estimation [59], the actual implementation of SrcRR seems to consider other parameters, like the signal strength, throughput or the multi-path interference [60]. Meraki's multi-radio solution is based on a centralized channel assignment: the nodes use a dedicated radio to monitor the interference of the different channels and send statistics to Meraki's cloud, which assigns to each node the optimal channels and transmit powers [62].
- Since its applications are oriented to safety, one of the strengths of the reactive routing solution of Firetide, called Firetide's Mesh Routing Protocol (FMRP), is its self-healing characteristic during route maintenance [61]. According to the transmission of packets, nodes save different alternative routes. The moment a link or path is not available, the packets are immediately re-routed through the next best available route. In addition, nodes monitor parameters that effect network performance in order to vary active routes.

Due to its easiness of deployment, another significant application of MIWNs is to permit the creation of communication networks in any environment and independently of commercial and/or governmental sectors:

- **Community networks**: Community networks are the most significant non-commercial use of WMNs. Examples of this are the aforementioned Roofnet in Cambridge [21], the

[6] https://www.tropos.com
[7] https://meraki.cisco.com/
[8] http://www.firetide.com/

Freifunk[9] initiative in Germany or the Guifi.net[10] network in Spain. These networks are created in an arbitrary way according to the nodes aggregated by their community members and have the objective of creating a free, neutral and extensible network, sharing their resources like the access to the Internet. OLSR with link-quality based routing metrics is the main routing solution used in these deployments[11], as is for instance the case of Freifunk and Guifi.net.

- **Non-governmental controlled networks:** Due to the attempts of different governments to control the Internet access in their countries, different initiatives have risen in order to assure open and free communications in the world regardless of national boundaries. This is the case of the Open Mesh Project[12], which was created in 2011, after the deliberate attempts by the Egyptian government to shut down the internet. Or of the Open Technology Institute's Commotion Wireless project in the USA[13], which has created an open-source project in order to facilitate the creation of Community networks. Also, during political protests in Hong Kong in 2014, citizens made use of mobile phone application called Firechat[14], which permitted direct ad hoc communication between users without the need of Internet.
- **Emergency and military networks:** MIWNs are especially indicated for complex environments where other technologies are inexistent or damaged. They permit a rapid deployment of first-response disaster and rescue missions, fleet and convoy communications, and surveillance networks. For instance, Concentis Systems[15] offers a commercial solution for these deployments based on OLSR. Also, after the damages caused to Haiti's communication infrastructure by the 2010 earthquake, the Serval project[16] was launched in Australia with the objective to create a disaster-proof wireless network using mobile phones.
- **Developing or rural countries networks**: As in disaster cases, MIWNs are well-suited to create a communication infrastructure in places where other solutions are not available. Thus, several foundations and non-governmental entities make use of this technology in developing or rural countries. The most significant initiative is the One Laptop Per Child project[17], which aims to provide each child with a low-cost connected

[9] http://freifunk.net/
[10] http://guifi.net/
[11] http://www.olsr.org/mediawiki/index.php/Main_Page
[12] http://www.openmeshproject.org/
[13] https://commotionwireless.net/
[14] http://opengarden.com/firechat
[15] http://www.concentris-systems.com/
[16] http://www.servalproject.org/
[17] http://one.laptop.org/

laptop using a routing solution based on 802.11s. Another interesting project is FabFi[18], which uses building materials and off-the-shelf electronics to form MIWNs and enable access to online educational, medical, and other resources. By the moment, it has been implemented in Kenya and Afghanistan.

2.2.2 Experimental platforms

Although almost all commercial MIWNs are based on proprietary routing solutions, there are numerous wireless devices based on Linux which permit the implementation and testing of experimental routing solutions. The most popular Linux distribution for wireless embedded devices is OpenWrt[19], which implements the Linux wireless (IEEE-802.11) subsystem[20]. In fact, the success of Community networks has raised the availability of numerous open-source projects based on OpenWrt which facilitate the creation of MIWNs using popular routing protocols like OLSR[21].

During the realization of this thesis, two main platforms were used: the AccessCube of 4G Systems[22] and the Cambria GW2358-4 of Gateworks[23]. Both use embedded Linux distributions, Nylon and OpenWrt, respectively, and can become multi-radio devices by means of Mini-PCI extensions.

Fig. 2.12: Experimental platforms: MeshCube and Cambria GW2358-4.

Also, Android mobile phones, which are based on Linux kernel, permit the implementation and testing of routing protocols [62][63]. However, ad hoc is not natively supported by actual Android

---

[18] https://code.google.com/p/fabfi/wiki/FabFi
[19] https://openwrt.org/
[20] http://wireless.kernel.org/
[21] http://wiki.openwrt.org/doc/howto/mesh.olsr
[22] http://4g-systems.com/
[23] http://www.gateworks.com/

devices (although it can be activated in some rooted devices or using custom roms). Nowadays smartphones use Wi-Fi Direct as ad-hoc solution, which is more oriented to point-to-point media sharing rather than to multi-hop routing [64].

2.2.3 Simulation platforms

The utilization of network simulators is a common practice in wireless multi-hop research in order to prove the benefits of the solutions in a variety of scenarios and allow the comparison between different alternatives in fixed conditions. However, some studies remark the low credibility of some simulation results due to an excessive simplification of physical and MAC models, a lack of configuration details in order to make simulations repeatable and comparable or a not rigorous statistical validation [65][66][67][68]. Next subsections describe how propagation and interference models are commonly modeled in MIWNs research, since both have a notorious impact on simulation results [69][70]. Finally, the simulator used during the elaboration of this thesis is presented and justified.

2.2.3.1 Wireless propagation models

The propagation of a wireless signal is principally affected by path loss and fading [5]. Path loss defines the average signal power loss during propagation. The simplest model is the Free Space model, which considers a single Line-Of-Sight (LOS) signal component between transmitter and receiver, and divides the transmitted power by the square of the distance between them. This model leads to longer and usually unreal transmission ranges [67].

More realistic path loss models consider the effects of multipath signal components (NLOS) caused by reflection, diffraction or scattering, which often cause distortion in the received signal [5]. For instance, the Two-Ray model considers that the received signal is the sum of the LOS component propagated through free space and a single reflected component off the ground. In case of similar antenna highs, the Two-Ray model basically scales the transmitted power by the fourth power of the distance between transmitter and receiver. Also, there are other propagation models which predict signal loss for a given environment based on empirical measurements, for instance the Okumura model or the Hata model.

In any case, in order to simplify the application of signal propagation models, usually the Simplified Path Loss model is applied [5], which defines the received power as the transmitted power divided by a certain power γ of the distance. The value of γ depends on the environment, following Table 2.7.

Environment	***γ range***
Urban macrocells	3.7-6.5
Urban microcells	2.7-3.5
Office Building (same floor)	1.6-3.5
Office Building (multiple floors)	2-6
Store	1.8-2.2
Factory	1.6-3.3
Home	3

Table 2.7: Typical Path Loss Exponents.

A typical assumption in MIWNs research is to consider only path loss effect on signal propagation, representing the communication range of a node as perfect circle. Using this approximation, based on an Additive White Gaussian Noise (AWGN) model, all radios have an equal range, there is symmetry in communication and the communication is perfect inside the range [69]. However, in real environments obstacles or mobility can produce random and non-distance dependent attenuations on the received signal. This effect is known as fading or shadow fading.

Since the exact variations caused by fading are usually unknown, statistical models are used in order to predict the attenuation of the transmitted signal [5]. In MIWNs, common fading models are based on Rayleigh or Ricean distributions. The Rayleigh distribution is used in environments where only NLOS components are present, while the Ricean distribution considers a dominant LOS component. The Ricean *K* factor is used in order to model the ratio between LOS and NLOS components (e.g. the severity of the fading), where a value of 0 determines a Rayleigh model (very high fading) and an infinite value an AWGN model (no fading).

2.2.3.2 Wireless interference and reception model

How to model the wireless interference is fundamental in MIWNs since it highly impacts the performance of active flows, determining contention in transmission and interference in reception [69][71]. Basically, two different typologies can be considered: additive and non-additive [71].

The additive model considers the thermal noise and the interference of all the signals detected on the channel in order to compute the SINR of the current reception or determine if the channel is occupied by using Energy Detection. This model is the most accurate and similar to the one being applied by commercial drivers [71].

On the other hand, non-additive models are simplifications which only consider one interference source at a time [71]. The Capture Threshold model compares the SINR value with defined thresholds in order to determine if a reception has been interfered or the channel is occupied. The Protocol model considers that interference occurs if the distance between interferer and receiver is shorter than *Δ* times the distance between transmitter and receiver. Finally, the Interference Range model defines fixed ranges and only considers interference or contention if the nodes located in these ranges. These three models, together with some variants, are usually used in simulators, protocol designs and analytical models in order to obtain a simple approximation of interference.

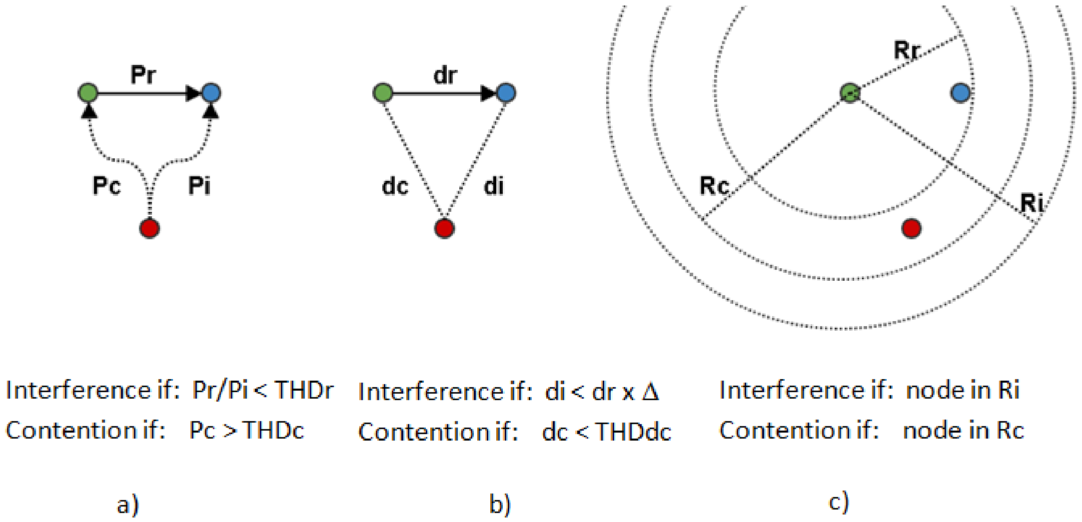


Fig. 2.13: Non-additive interference models: (a) Capture Threshold model, (b) Protocol model and (c) Interference Range model.

Then, in order to decide if a reception is valid, three reception methods (or a combination of them) can be considered: distance-based, SINR-based or BER-based. As shown in Fig. 2.13, the distance-based model is applied in Protocol and Interference Range models and simply checks the distance or location of the receivers, transmitters and interferers. On the other hand, the SINR-based model compares the SINR of the received signal with predefined thresholds and accepts only signals whose SINR values have been above them at any time during the reception. For the different technologies and modulations of the IEEE 802.11 standard it is possible to compute the minimum SINR for a BER better than 10e-5, which is considered as acceptable in Wi-Fi communications. For instance, Table 2.8 gives the values for 802.11a modulations.

Rate (Mbps)	SINR (db)
54	24.56
48	24.05
36	18.80
24	17.04
18	10.79
12	9.03
9	7.78
6	6.02

Table 2.8: Minimum SINR values for an acceptable BER using 802.11a

Finally, the BER-based method probabilistically decides if a reception is successful based on the frame length and the computed BER. This method evaluates each segment of the frame every time the interference level changes, thus being more realistic and accurate than the SINR-based model [69].

2.2.3.3 Network simulators

Nowadays, the most common network simulators in MIWNs research are NS (versions 2 and 3)[24] and OMNeT++[25], which are free for academic use. Other significant commercial alternatives, which have not been considered during the elaboration of this thesis, are OPNET[26] or QualNet[27], which is based on GloMoSim, an academic free version which is actually outdated. OMNeT++ has also a commercial version called OMNEST[28].

The simulations of this thesis were performed using OMNeT++ v3.4b2 simulator. OMNeT++ was developed at Department of Telecommunications of the Technical University of Budapest during the early 1990's. It is a discrete event simulator based on hierarchically connecting small and reusable modules, which are written in C/C++, in order to assemble more complex components like IEEE 802.11 radios, routing protocols, applications or nodes. The communication or relationship between modules is based on a high-level language called NEtwork Description (NED). Simulations can be interactive using a Graphical User Interface (GUI) or using command lines, having as output the demanded statistics and parameter values.

---

[24] http://www.nsnam.org/
[25] http://www.omnetpp.org/
[26] http://www.riverbed.com/products/performance-management-control/opnet.html
[27] http://web.scalable-networks.com/content/qualnet
[28] http://www.omnest.com/

Indeed, OMNeT++ is not a network simulator itself, but there are numerous frameworks which implement the different network functionalities. The principal one is the INET framework[29], which contains the models for most wired and wireless networking protocols and technologies, like TCP/IP, IEEE 802.11, MANET routing, Ethernet, etc. There are also other frameworks more oriented to concrete environments, like VEINS[30] for VANETs or MIXIM[31] and Castalia[32] for WSNs.

At the start of this thesis, NS-3 development was still incomplete. Then, although NS-2 was the most used simulator in MIWNs research, OMNeT++ was selected in front of NS-2 for the following main reasons:

- **Propagation and wireless models**: The default version of NS-2 was based on non-additive interference model and didn't implement fading, thus leading to unrealistic simulations [69][71]. By means of frameworks and extensions, OMNeT++ implemented an additive SINR model, shadow fading models and BER computation based on 802.11a/g modulations [72][73].
- **MANET protocols**: OMNeT++ had a framework called INETMANET which implemented AODV, OLSR and DYMO routing protocols [73]. This framework was selected as the basis of the developed implementation.
- **Simulator design:** The modular design of OMNeT++ facilitated the implementation of new protocols or extensions, for instance the creation of multi-radio nodes. On the other hand, the code of NS-2 was more complex to modify.
- **GUI**: At the initial stage of the research, a deep analysis of the procedures of the different protocols was necessary, sometimes in a per-packet basis. The GUI OMNeT++ was more usable and user-friendly, facilitating this task.
- **Statistical validation:** Simulators use pseudorandom number generators (PRNG) to perform uncorrelated simulations. The default cycle length of NS-2 was 2^{31}-1, what did not ensure statistical validation when using several random streams in each simulation [65]. On the other hand, OMNeT++ used random number generators based on the Mersenne Twister with a period of 2^{19937}-1.

[29] http://inet.omnetpp.org/
[30] http://veins.car2x.org/
[31] http://mixim.sourceforge.net/
[32] https://castalia.forge.nicta.com.au

Table 2.9 summarizes the basic PHY and MAC parameters used in the simulations presented in this thesis.

Parameter	Value or Configuration
Propagation model	Two-ray propagation model
Fading	Ricean fading with factor 5
Transmission Power	30 mW
PHY/MAC technology	IEEE 802.11a
Transmission rate of broadcast, preambles and ACKs	6 Mbps
Minimum sensitivity at 6 Mbps **(Carrier sensing range using preamble detection)**	-82dBm in reception (197 meters)
Minimum sensitivity at 12 Mbps **(Max. communication range at 12 Mbps)**	-79dBm in reception (167 meters)
Noise level **(Max. interference range)**	-95dBm in reception (418 meters)
RTS/CTS mode	Off
Random Number Generators (RNG)	4 independent RNGs: application, routing, MAC and PHY layer
Warm Up time **(initial period without flows)**	100-200 seconds
TCP version	Reno

Table 2.9: Basic simulation parameters.

Finally, the basic simulation scenario used during the realization of this thesis consists of 64 nodes located in a 980 m x 980 m grid topology, as detailed in Fig. 2.14. Starting from this scenario, other topologies are tested: node location based on a random uniform distribution, mobile nodes and/or multi-radio and multi-channel nodes.

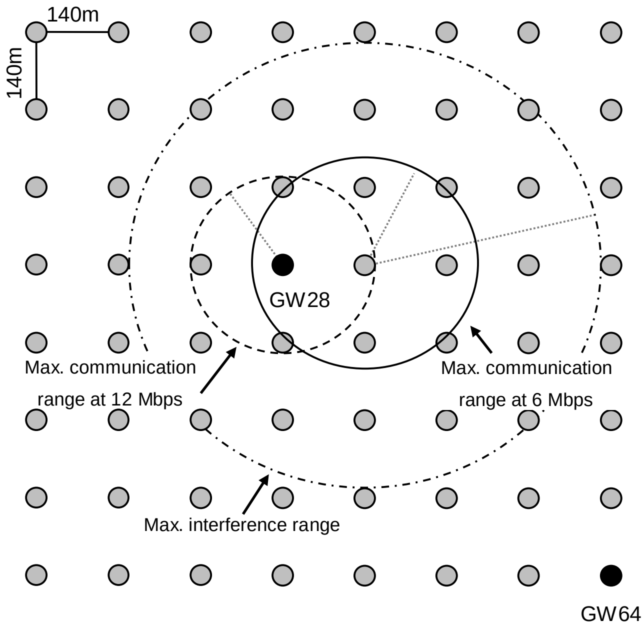


Fig. 2.14: Basic simulation scenario. Nodes marked as GW are used as Gateways in some scenarios (i.e. sinks of traffic).

3

Performance of traffic flows in MIWNs

This chapter analyzes how different phenomena related with physical and MAC layers affect the performance of the flows in MIWNs. As introduced in previous chapter, cross-layer parameters have to be considered in routing protocols in order to correctly characterize the links and find the optimal paths which maximize performance.

Next sections deal with the characterization and estimation of phenomena related to the following aspects: link quality, contention and interference, and the utilization of multiple channels and radios. Their concrete impact on the performance of the flows is analyzed, which can be direct, for instance, in terms of throughput or delay degradations. But also indirect, causing malfunctions to multi-hop routing procedures. In addition, different estimation methodologies and models are analyzed. Finally, the chapter is concluded with a brief discussion on how to enhance routing protocols using these cross-layer parameters, introducing the approach followed in the contributions of this thesis.

The experimental results presented in this chapter were obtained in indoor testbeds using the MeschCube platform, which was introduced in the previous chapter. IEEE 802.11a interfaces with fixed link bit rates were used and Constant Bit Rate (CBR) UDP traffics were generated by means of the Iperf tool[1]. On the other hand, simulation results are based on the PHY and MAC parameters introduced in Table 2.9.

3.1 Link quality

Previous chapter introduced the effect of path loss and fading on wireless propagation, which determines the received signal power of a transmission. In terms of traffic performance, a lower received SNR causes the utilization of lower bit rates (i.e. more robust modulations) or a higher number of packet losses, degrading for instance the throughput or the end-to-end delay of the flows.

Therefore, due to the variability of the wireless channel caused by fading, the quality of the links in terms of link errors and link bit rate should be monitored and integrated into routing procedures in order to create and maintain optimal paths. Although wireless interference also leads to packet losses due to collisions, in this section only the link variability caused by propagation and fading is considered, while the effect of interference will be analyzed in Section 3.2.

3.1.1 Link errors

A link between two nodes cannot be characterized using a binary logic, i.e. the link does exist or does not, since fading causes significant variations of the error rate of a link [5][21][74]. The impact of link errors on the performance of the flows is straightforward; it causes the loss of data or ACK frames, leading, among others, to the following degradations:

- **Information loss:** Although the IEEE 802.11 standard implements retransmissions, packets are discarded after reaching a defined limit [2]. In addition, a high number of retransmissions per packet can cause packets drops at MAC layer due to buffer overflow.
- **Throughout and goodput reduction:** The maximum achievable throughout becomes lower due to packet retransmissions. In addition, the goodput at the receiver is reduced due to packet losses.
- **Delay and jitter increase:** Retransmissions lead to higher and variable delays and jitter levels.

[1] https://iperf.fr/

- **TCP malfunctions:** Packet losses caused by link errors cause a wrong utilization of the congestion control of TCP, since transmission errors are seen as congestion occurrences, leading to very low sending rates of TCP sources [14][75][76].
- **Higher channel utilization:** Due to retransmissions, channel time consumption is higher, leading to an increase of contention and interference levels, thus degrading the performance of other links.
- **Disconnected routes:** Packet losses caused by fading or mobility can cause a link break, which considerably degrades traffic performance. Thus, most routing protocols use periodical signaling, the so-called Hello messages, to detect link unavailability and perform route recovery [76][77][78].

Due to the aforementioned effects on traffic performance, the integration of link error estimation into routing protocol procedures has been widely adopted by state-of-the-art routing solutions [2][59][79][80]. The usual estimation mechanism is based on monitoring the packet success rate of Hello messages [59]. This way, the error rate is computed as the ratio of received messages to the number of expected ones during a defined period. Finally, combining the estimation of both link directions is necessary to consider the reception of ACK messages.

However, this estimation method has two main disadvantages. First, the Hello packets are short, and in MIWNs, they are broadcasted at the lowest and most robust data rate. Therefore, the error rate of data packets, which are usually longer and unicasted at higher bit rates, can differ [77][81]. Second, it depends on the periodicity of the probe packets and the estimation period, which are usually high in order to minimize overhead [41]. However, long periods can be excessive when characterizing highly variable channels [79][81]. Nevertheless, this estimation mechanism has been proven to be beneficial and its utilization is very common in state-of-the-art routing metrics due to its simplicity and lightness [20][37][51].

Finally, another form to estimate the error rate of a link is to passively monitor the data packets being transmitted [54][80]. This way, the aforementioned disadvantages of the broadcasting-based mechanism are avoided. Logically, it can be only applied in links with active traffic, thus another mechanism based on probe packets has to be used in links without active flows.

3.1.2 Link bit rate

As introduced in section 2.1.1.1, the IEEE 802.11 standard defines different bit rates for each technology. Also, the selection of the bit rate depends on the Network Interface Card (NIC) and it can vary in time according to the implemented Rate Adaptation Algorithms (RAA). In fact, since most RAAs are based on the packet delivery ratio [30][31], obtaining the bit rate of a link is another way of qualitatively estimating its error rate: lower rates or more robust modulations are used in longer links or more affected by fading, and vice versa.

However, the utilization of RAAs in multi-hop networks in not proven to be beneficial or reliable [82]. First of all, they are sensitive to packet losses caused by interference, thus leading to bit rate reduction in cases where it is not necessary, which in fact increases congestion due to an increase of channel occupancy. Also, they are designed to obtain the optimal bit rate for a simple link in single-hop scenarios, while in multi-hop networks each node maintains multiple links which can require different bit rates.

In any case, being fixed or controlled by a RAA, an estimation of the link bit rate is necessary. As in the link error case, the bit rate has a straightforward impact on traffic performance; generally, flows being routed through faster links achieve higher throughputs and lower delays. In addition, higher bit rates decrease packet transmission times, thus reducing channel utilization.

The most common link bit rate estimation method is based on sending pairs of probe packets between neighbors [43][83][84]. The source sends two consecutive unicast packets while the receiver uses the delay between the receptions of both packets as a measurement of the transmission time of the second packet, thus obtaining the unicast bit rate. The objective of using two consecutive packets is to isolate the delay caused by other phenomena like contention or buffering, since both packets are expected to experiment the same delay, thus outperforming other estimation techniques based on Round-Trip-Time (RTT) measurements [83][84]. Fig. 3.1 shows the results of an experimental estimation of the nominal rates of an 802.11a link using pairs of probe packets.

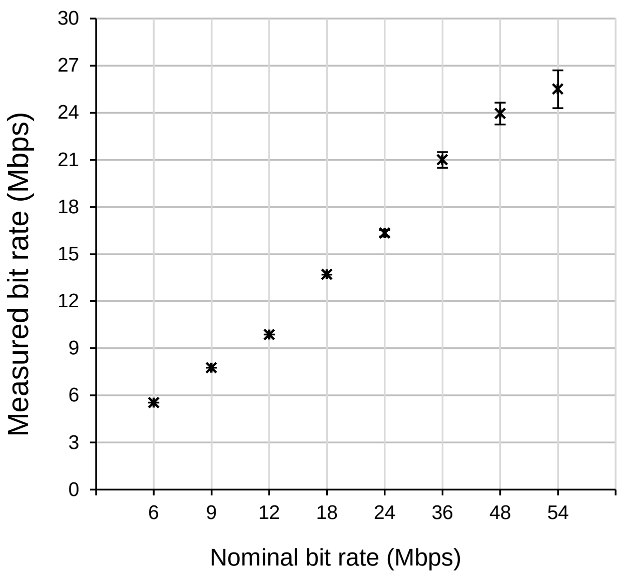


Fig. 3.1: Example of a bit rate estimation experiment using pairs of probe packets through an 802.11a link. The measured bit rate is in fact an estimation of the maximum achievable throughput, which is lower than the nominal bit rate due to PHY and MAC overheads.

Although this solution increases the overhead of the routing protocol, periodical unicast signaling is also very useful in order to assure that the created routes are able to transmit data packets. As aforementioned, some routing protocol procedures, like neighbor maintenance or route creation, are based on broadcasting, thus using the lowest and most robust bit rate of the technology. In some scenarios, this causes that some links are considered as active by the routing protocol, but indeed they are unable to transmit data packets successfully using a less robust unicast rate. This issue is known as the Communications Gray Zone problem and considerably degrades traffic performance [81].

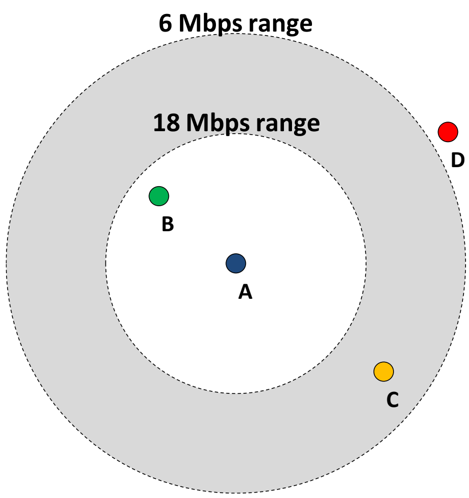


Fig. 3.2: Example of a Communications Gray Zone problem. Node A is using a unicast bit rate of 18 Mbps, while the broadcast bit rate is 6 Mbps (e.g. 802.11a). Node D is not reachable by broadcast messages and therefore it is not considered by the routing protocol as a one-hop neighbor. Node B is achievable both using broadcast and unicast rates, thus data exchange is possible. Finally, node C is considered as a one-hop neighbor, thus being eligible as next hop by a routing protocol, but unicast communications are not possible. Thus, data packets being routed through this link would be lost.

3.2 Contention and interference

The MAC layer of the IEEE 802.11 standard was not initially designed to provide multi-hop capabilities, therefore it does not appropriately handle the issues of medium sharing and interference in these environments [12][13][24]. Collisions are more probable to occur, since traffic is not centralized to an AP. In fact, a single flow traversing a multi-hop route incurs in self- or intra-flow interference due to the transmissions of the different nodes of the path, which leads to the well-known throughput division by the number nodes [13], as illustrated in Fig. 3.3.

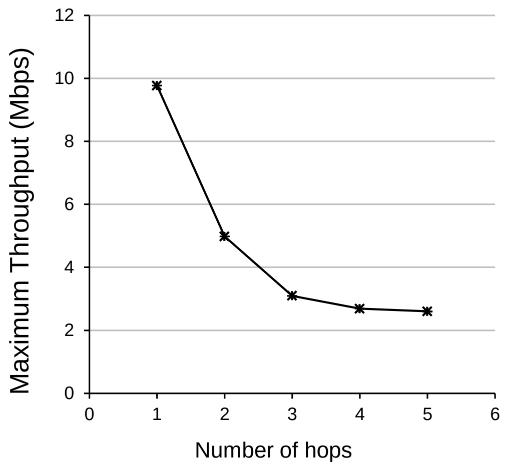


Fig. 3.3: Maximum UDP throughput according to the length of a simulated chain of nodes using a link bit rate of 12 Mbps.

Throughput reduction is principally caused by the multiple hidden node situations that occur during multi-hop routing and has been measured to happen up to 7 hops [13][85]. However, the utilization of the RTS/CTS mechanism, which was designed to deal with this problem in single-hop scenarios, is not reliable in multi-hop networks [15][86]. As shown in Fig. 3.4, using Virtual Carrier Sensing in MIWNs can increase significantly the Exposed Terminal cases, leading to useless waiting and channel time waste.

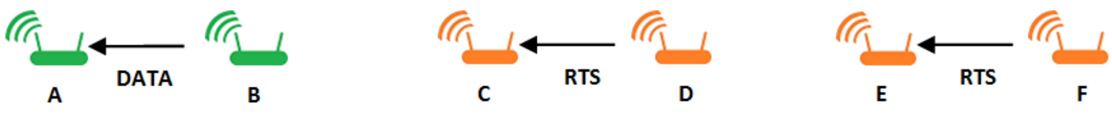


Fig. 3.4: Exposed Terminal problem in MIWNs when using VCS. Node C is blocked by a previous RTS sent by node B, therefore it cannot answer D's RTS. In addition, the RTS of node D also blocks node E, which cannot initiate a communication with F. And so on.

In addition to intra-flow interference, multi-hop flows suffer of inter-flow interference [24], which occurs when several flows being transmitted by close links compete for the same channel. Due to

CSMA/CA mechanism, this leads to an increase of backoff waiting, retransmissions and packet losses. As shown in Fig. 3.5, inter-flow interference can degrade drastically the measured performance of a flow.

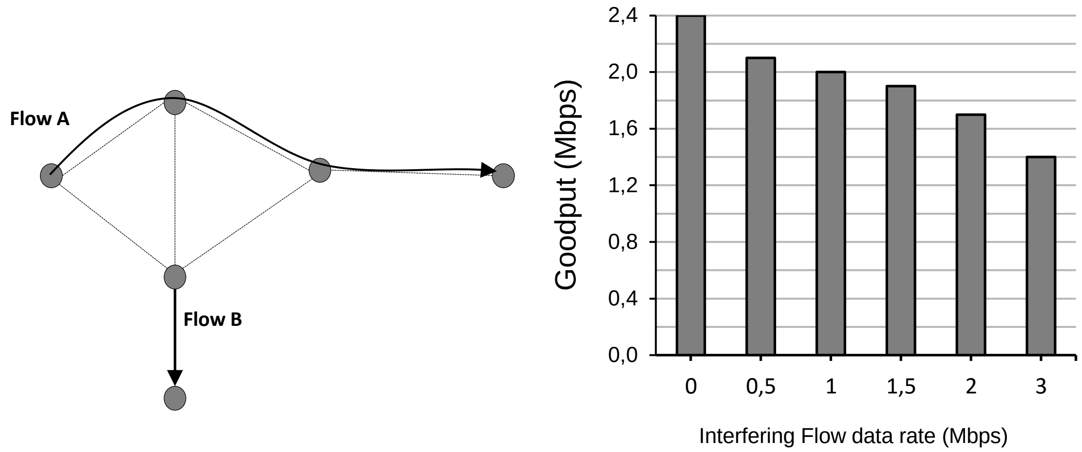


Fig. 3.5: Measured goodput in an experimental testbed due to increasing inter-flow interference. The analyzed flow traversed a chain of 4 nodes (Flow A) and was interfered by a link transmitting UDP traffic at variable data rates (Flow B). The link bit rates of all the links was fixed to 12 Mbps.

Independently of the type of interference, it will impact the performance of the flows being routed, causing contention in transmission or interference in reception. The following sections analyze these two phenomena according to the results of different experiments. Some state-of-the-art proposals take information from the physical and MAC layers in order to estimate contention and interference, using for instance statistics about the amount of time spent in the different states of CSMA/CA (i.e. waiting, collision, backoff and success) [87][88] or monitoring the SNIR level of the NIC [89]. However, since the contributions of this thesis are centered on the network layer, hereinafter only models and estimators which are applicable to this layer will be considered.

3.2.1 Load definition

Node and channel congestion are proportional to the load of the nodes. Some state-of-the-art proposals used simple models to estimate the load of a node, like the number of queued packets [90] or the number of active routes [91]. However, due to wireless channel sharing, the most appropriate way to model node load is to characterize the Channel Occupancy (CO) because of transmissions [15][24][52][87][89][92].

Logically, nodes with lower data rates will consume more channel time, but, as denoted in Section 3.1, link quality should be also considered in the load definition. Links with a high error ratio lead to a high number of retransmissions and channel consumption. Likewise, traffic routed through a slow link captures the channel for a long time in each transmission attempt. Also, it should be considered the channel time consumed by physical and MAC layer overheads [2], like preambles, ACK transmissions, RTC/CTS, IFS delays, etc. Fig. 3.6 shows an experimental example on how the maximum achievable goodput of a flow varies according to the link bit rate of the interfering link.

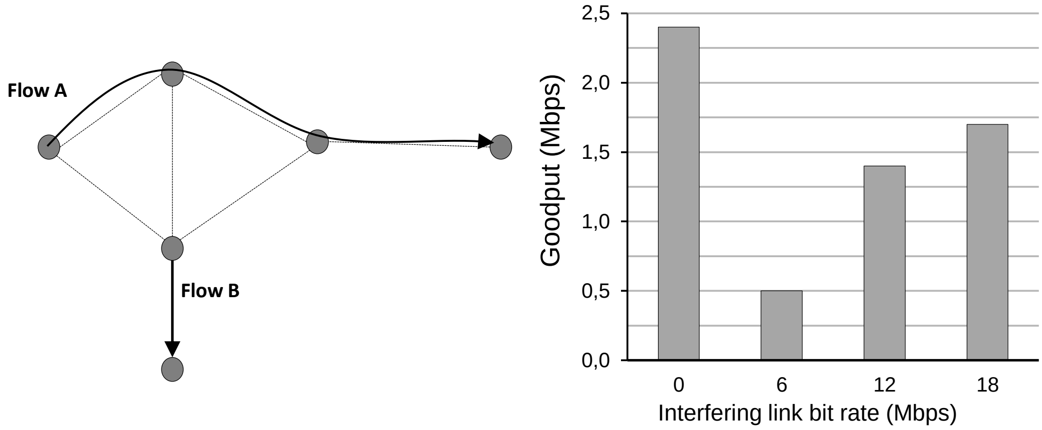


Fig. 3.6: Effect of different link bit rates on the available bandwidth of 802.11a nodes. The analyzed flow traversed a chain of 3 links at 12 Mbps (Flow A) and was interfered by a link transmitting UDP data at 3 Mbps using different link bit rates (Flow B) . The 0 case stands for no interference.

Indeed, the definition of load in terms of channel occupancy has the objective to better model the interference perceived by a link [24][92]. Fig. 3.7 shows, in the case of two contending transmitters, how the throughput of link A varies according to the bit rates of the links and the throughput of flow B. The perceived load is computed as the maximum achievable throughput by link A (without interference) minus the throughput that flow A is really able to achieve in this case without decreasing the throughput of B (i.e. avoiding saturation case). Since the load of B is expressed in terms of throughput, in the cases with different link bit rates, node A perceives interference levels which do not fit with the throughput of B, which are remarked in the figures as inflations or deflations.

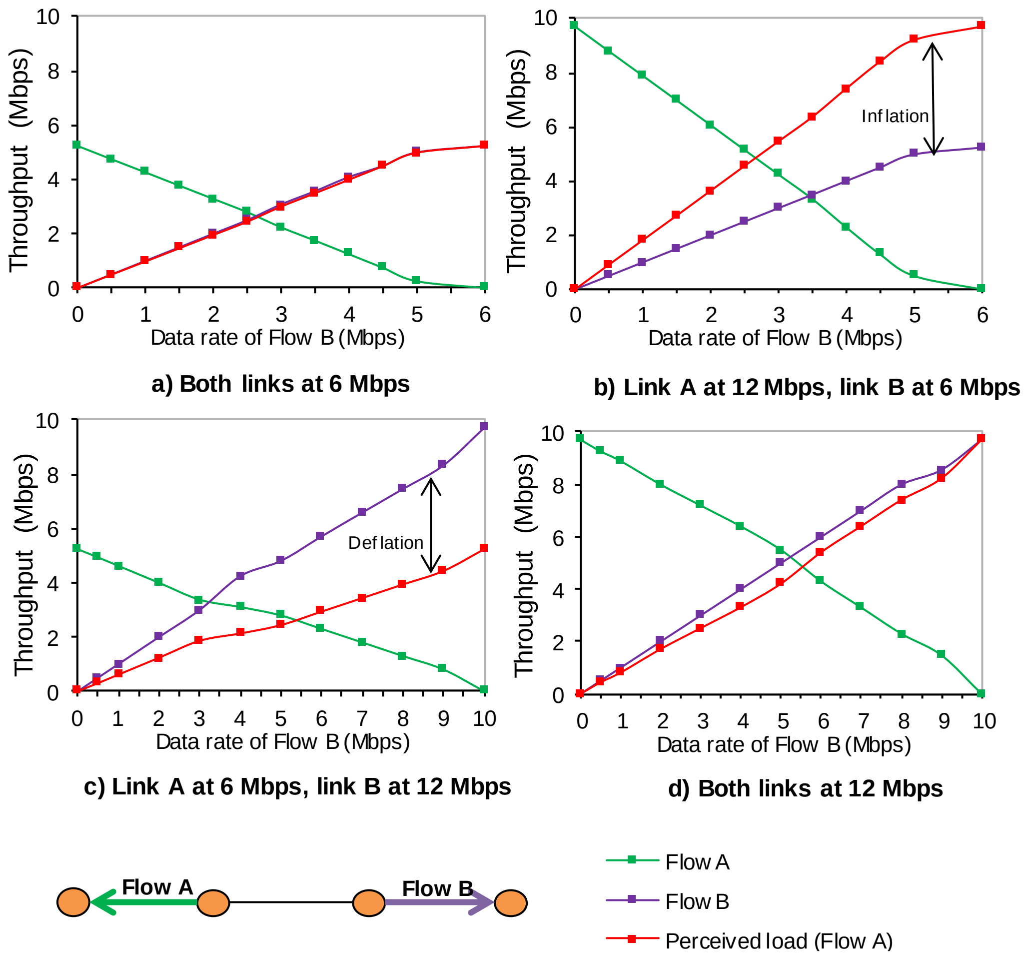


Fig. 3.7: Perceived channel occupancy according to the bit rate of the links in a simulated scenario. Transmitters sensed each other, leading to contention.

On the other hand, Fig. 3.8 shows that defining the load of B in terms of Channel Occupancy (CO), i.e. considering its link rate, leads to a better estimation of the perceived interference in the previous scenario.

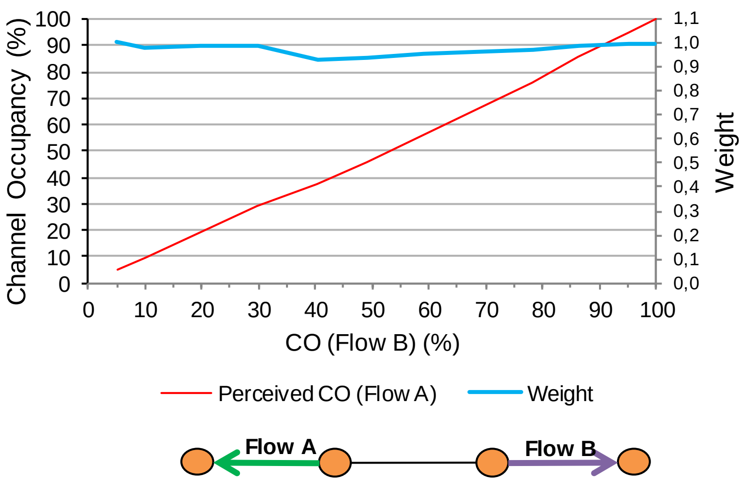


Fig. 3.8: Real vs perceived channel occupancy in a simulated scenario with two contending flows. The Weight parameter is defined as the ratio between perceived and real CO.

Using this load definition, the following sections will analyze how the Weight parameter, which is defined as the ratio between perceived and real CO, varies according to the position of the interfering nodes and can be used in order to obtain an estimation of the interference level of a node.

3.2.2 Contention in transmission

CSMA/CA usually leads to a fair distribution of the channel time if all contending transmitters sense each other [24]. As was shown in Fig. 3.8, this leads to a Weight parameter of the order of 1, since CSMA/CA only permits one node to transmit at a given time; i.e., the perceived channel occupancy by a node is basically the sum of the CO of all the other contenders. Fig. 3.9 shows the simulations results of a scenario with three contending nodes using variable link and data rates also leading to a Weight factor close to 1.

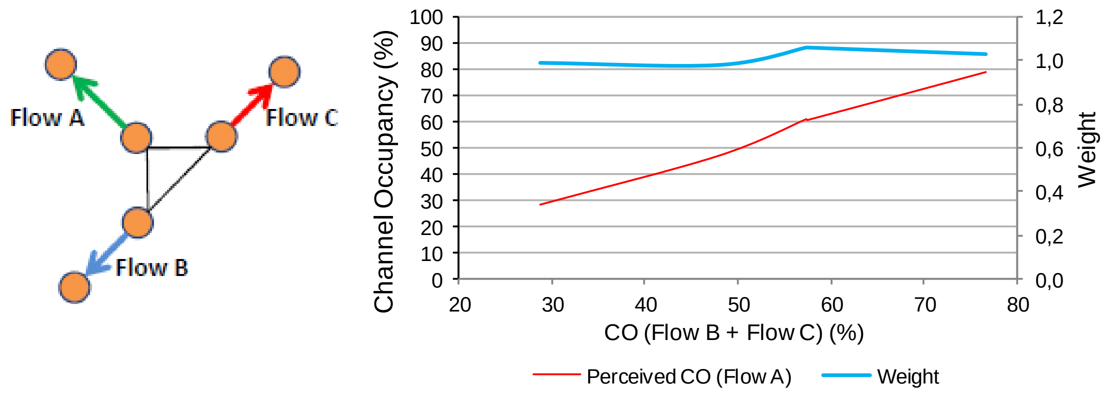


Fig. 3.9: Simulation of a scenario with contention between three pairs of nodes with non-saturated traffic. The link bit rates were varied between 6, 12 and 18 Mbps, while the data rates of Flow B and Flow C were varied between 0.5, 1, 2 and 3 Mbps.

However, in unbalanced scenarios unfair channel time distribution can occur. In saturation cases, nodes with a lower number of contenders will have a higher probability of gaining channel access, while nodes sensing more transmitters will have less transmission chances [12][24][92][93]. On the other hand, in non-saturated cases, the effect of unbalanced carrier sensing is not so severe [24]. Fig. 3.10 shows the simulation results of an unbalanced contention scenario with non-saturated traffic. In fact, since the external nodes sometimes transmit simultaneously, the CO perceived by the central node is even lower than the aggregated CO of both contending nodes (i.e. a Weight factor lower than 1).

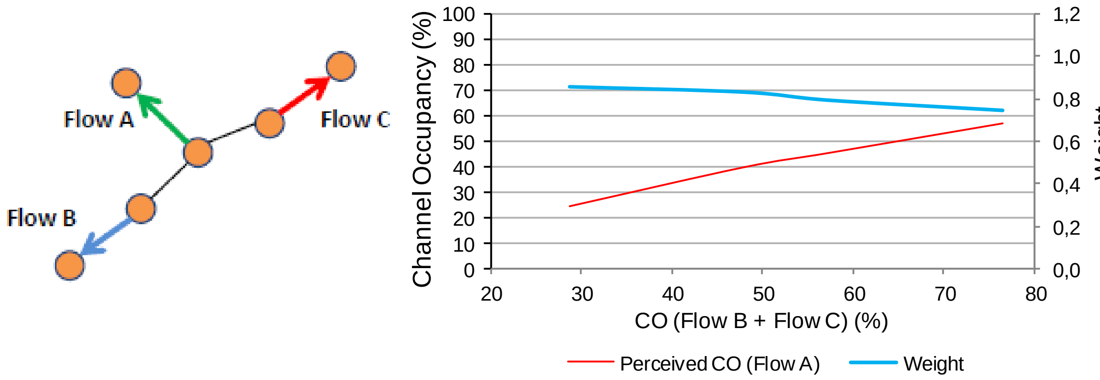


Fig. 3.10: Simulation of a scenario with an unbalanced contention between three pairs of nodes with non-saturated traffic. The link bit rates were varied between 6, 12 and 18 Mbps, while the data rates of Flow B and Flow C were varied between 0.5, 1, 2 and 3 Mbps. The transmitters of Flow B and Flow C did not sense each other and their transmissions did not interfere.

In any case, the effect of carrier sensing on the CO perceived by a node can be considered to be of the order of the aggregated CO of its contending nodes. In saturation cases, the perceived CO will be the 100%; i.e. the channel is fully occupied and new flows should try to avoid using it. Indeed, using saturation scenario is not recommended in MIWNs since, as has been shown in Fig. 3.3, the maximum achievable throughput is limited by the number of hops of the path. Using data rates higher than this limit is useless and harmful for the performance of the network and even of the flow itself, while rate-controlled traffics obtains better results [12][13][24][85]. For instance, in the case of TCP flows, it is recommended to set the Congestion Window Limit (CWL) to a low value in order to avoid heavy congestion at the MAC layer [75].

Finally, in order to obtain the contention level of a node at the routing layer, the contending nodes should be detected. Routing protocols usually broadcast periodical Hello messages in order to discover one-hop neighbors. Since broadcasting is done at the minimum transmission bit rate, as is the case of IEEE 802.11 preambles, any transmission of a node which has been detected as a one-hop neighbor will be surely detected by the PD mechanism. On the other hand, any transmission of a node whose Hellos cannot be correctly decoded will not be detected either by PD or by ED mechanisms, as described in Section 2.1.1.4. Thus, the Carrier Sensing range of node can be modeled as its one-hop neighborhood. This model only ignores the situations whereby the aggregated SNIR of two or more nodes out of the one-hop neighborhood are detected by the ED. However, this will rarely occur since the ED threshold in 802.11 is significantly higher than the minimum sensitivity, for instance 20 dB above it in 802.11a [2][89]. As was defined in Section 2.2.3.2, this approximation is known as the capture threshold model or protocol model [71].

3.2.3 Interference in reception

Interference in reception is caused by the arrival of other transmissions during the reception of a packet, causing a collision and the packet corruption. Interference is difficult to model at the network layer, since it depends on several physical parameters and phenomena, such as distance between nodes, transmission power, wireless propagation, receiver sensitivity, SNIR, data modulation and capture effect [24][71][89][94].

Two different types of interferers are considered. Hidden nodes are nodes in the transmission range of the receiver, but not of the sender; i.e., the typical scenario that justifies the usage of RTS/CTS. Hidden node transmissions can cause a collision if they occur during an active reception or can capture the radio of the receiver if they occur before the useful packet arrives, although some NICs permit to discard the interfering frame and capture the most powerful one [94]. On the other hand, the interference of more remote nodes depends more on the aforementioned physical parameters. Thus, its characterization is more complex.

Fig. 3.11 shows the simulation results of different hidden node scenarios in terms of perceived Channel Occupancy. While in the contention case the perceived CO is related to the time spent in wait and backoff states, being of the order of the aggregated CO of the contenders, in this case collisions cause a significant inflation due to packet retransmissions and losses.

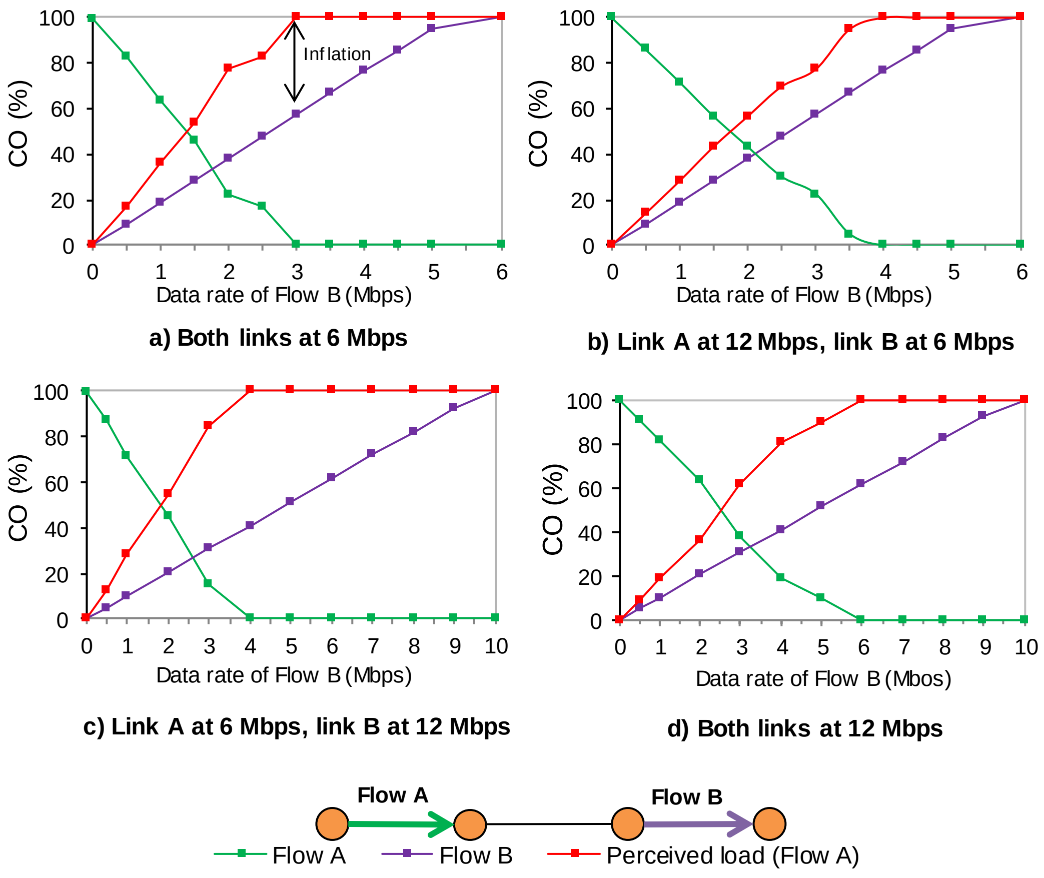


Fig. 3.11: Simulation of different hidden node scenarios. The rate of Flow B was varied between 0 to 6 Mbps in cases a) and b), and between 0 and 10 Mbps in cases c) and d). The distance between consecutive nodes was the same.

Fig. 3.12 summarizes these results and shows the Weight parameter for the analyzed scenarios. Based on the perceived CO, three differentiated zones can be considered:

- **Starvation [95]:** In all the analyzed cases, an interfering flow B which occupies more than the 70% of the channel time, leads to a perceived CO of the 100%. I.e., almost all transmissions of flow A do collide.
- **Highly interfered channel:** The perceived CO is greater than the 75%, thus leading to a high probability of collisions. The Weight parameter is between 1.5 and 2.
- **Medium to low interfered channel:** The perceived CO is lower than the 75% and collisions are less probable. The Weight parameter is around 2.

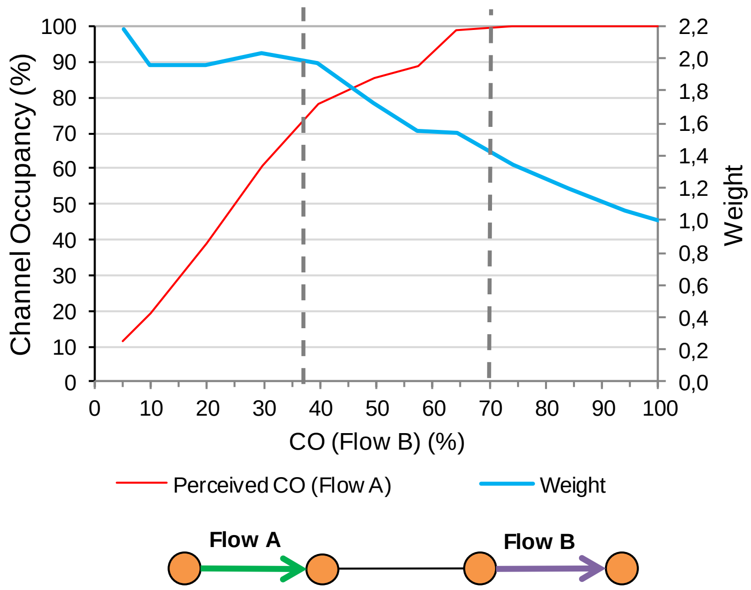


Fig. 3.12 Real vs perceived channel occupancy in the simulated hidden node scenarios.

As in the contention case, in order to avoid starvation, the CO of a single node usually will be situated in the second and third zones, thus leading to a Weight factor of the order of 1.5-2. Authors in [92] get similar results in an experimental testbed, obtaining an inflation average of 1.7. Also, intuitively, it seems logical to consider the impact of the hidden nodes on interference to be higher than the impact of contending nodes due to the retransmissions and packet losses caused by collisions.

In the case of the interference of more remote nodes, Fig. 3.13 summarizes the results of different scenarios varying the link bit rate of the analyzed flow and the number and distance of interfering nodes. The distance is denoted as a factor of the maximum transmission range at 6 Mbps. As expected, the interference decreases with the distance, while it increases with the number of interfering nodes. Also, the cases using a less robust modulation suffer from interference at longer distances. In conclusion, in these scenarios the Weight factor is very variable due the dependency of the interference level on distance, modulations and the number of interfering nodes.

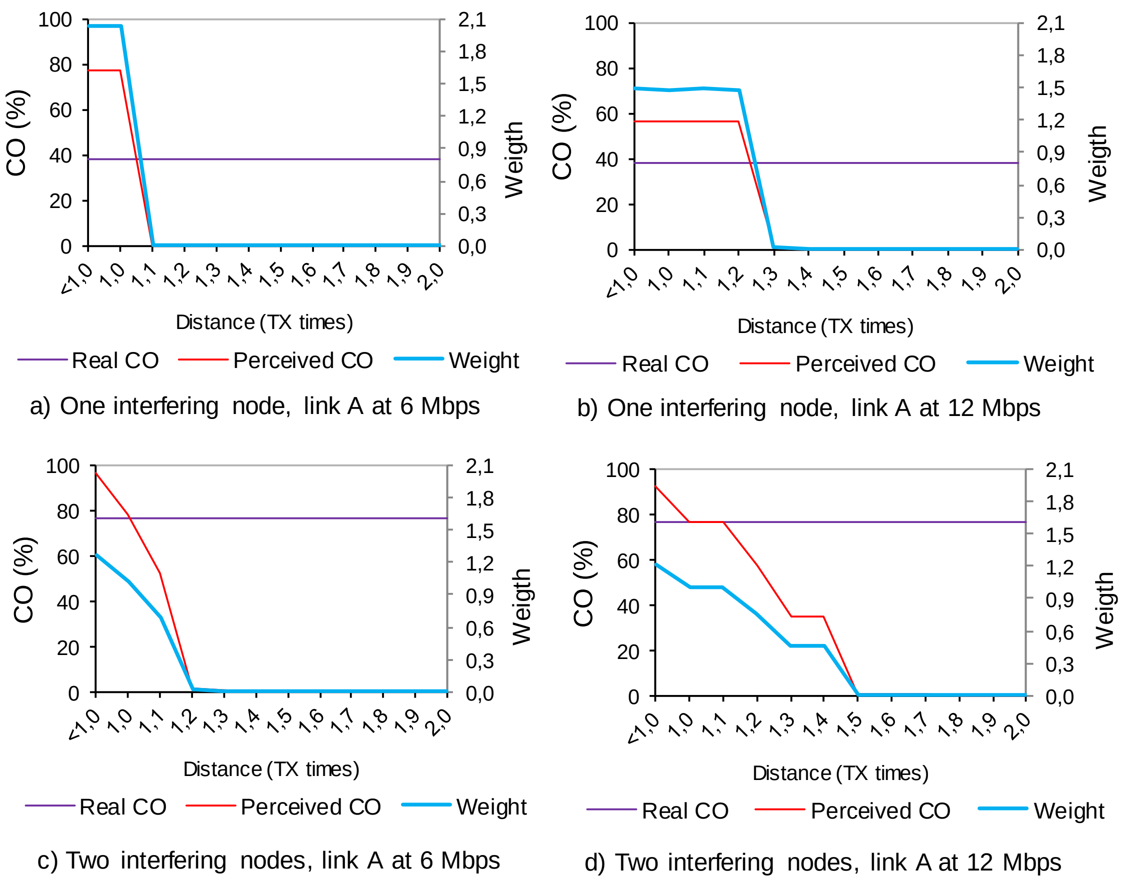


Fig. 3.13: Simulation of different interference scenarios with remote nodes. The distance between receiver and its interferers was varied according to the maximum transmission range at 6 Mbps (TX in the figures). The data rate of the interfering flows was fixed to 2 Mbps.

Finally, in order to discover interferer nodes, a commonly used model at the network layer is based on the interference range model introduced in Section 2.2.3.2, defining the interference range as the n-hop neighborhood of the receiver. Usually, nodes up to the two-hop neighborhood are considered to be interferers [13][17][27][28].

3.3 Multiple channels and radios

The usage of multiple channels and radios has the objective of minimizing some of the aforementioned issues of multi-hop routing in the presence of contention and interference; simultaneous transmissions using orthogonal channels can exist without leading to backoff waits, collisions and retransmissions. Fig. 3.14 shows an example on how the goodput and the average delay of a MIWN improves with the number of available interfaces and orthogonal channels.

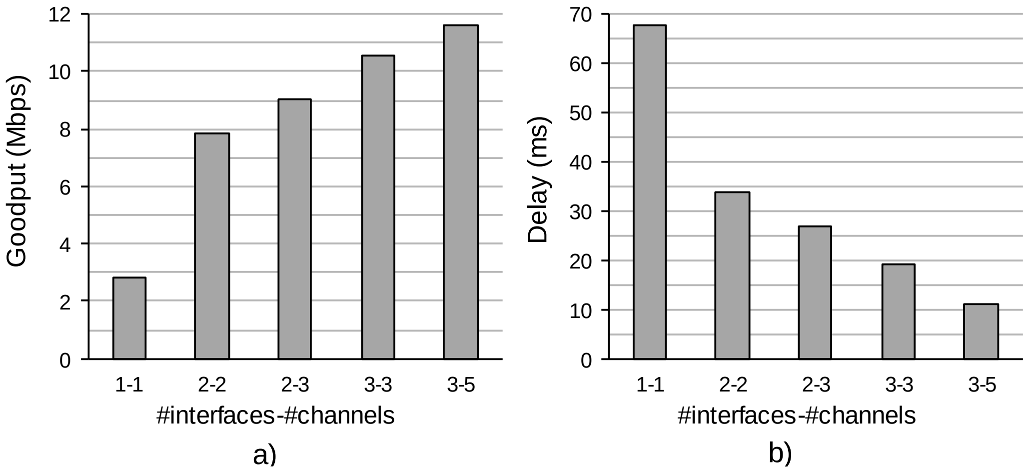


Fig. 3.14: Goodput and average delay of a simulated multi-hop network with a varying number of interfaces and orthogonal channels. The network consisted of a regular grid of 64 nodes with a fixed link bit rate of 12 Mbps. 8 data flows of 1500 kbps were initiated and routed using AODV and ETT metric. Channel assignment was random.

In the case of intra-flow interference, using different channels along a path permits to reduce the throughput decrease with the number of hops. Fig. 3.15 shows the obtained throughput decrease factor of different simulations according to the length of the chain and the channel distribution for a case of two radios and two orthogonal channels. In the figure, the results shown in red denote the worst case, which is the single-radio or single-channel scenario, while the best cases are marked in green. Results show that increasing the channel diversity of a path also increases its maximum available throughput. Also, they show that in long paths it is preferable to reuse a channel in two consecutive hops, leading to contention or half-duplex behavior, than alternate channels in each hop and incur on collisions due to hidden nodes. These two aspects, which also affect the level of inter-flow interference, should be considered in routing procedures [17][20].

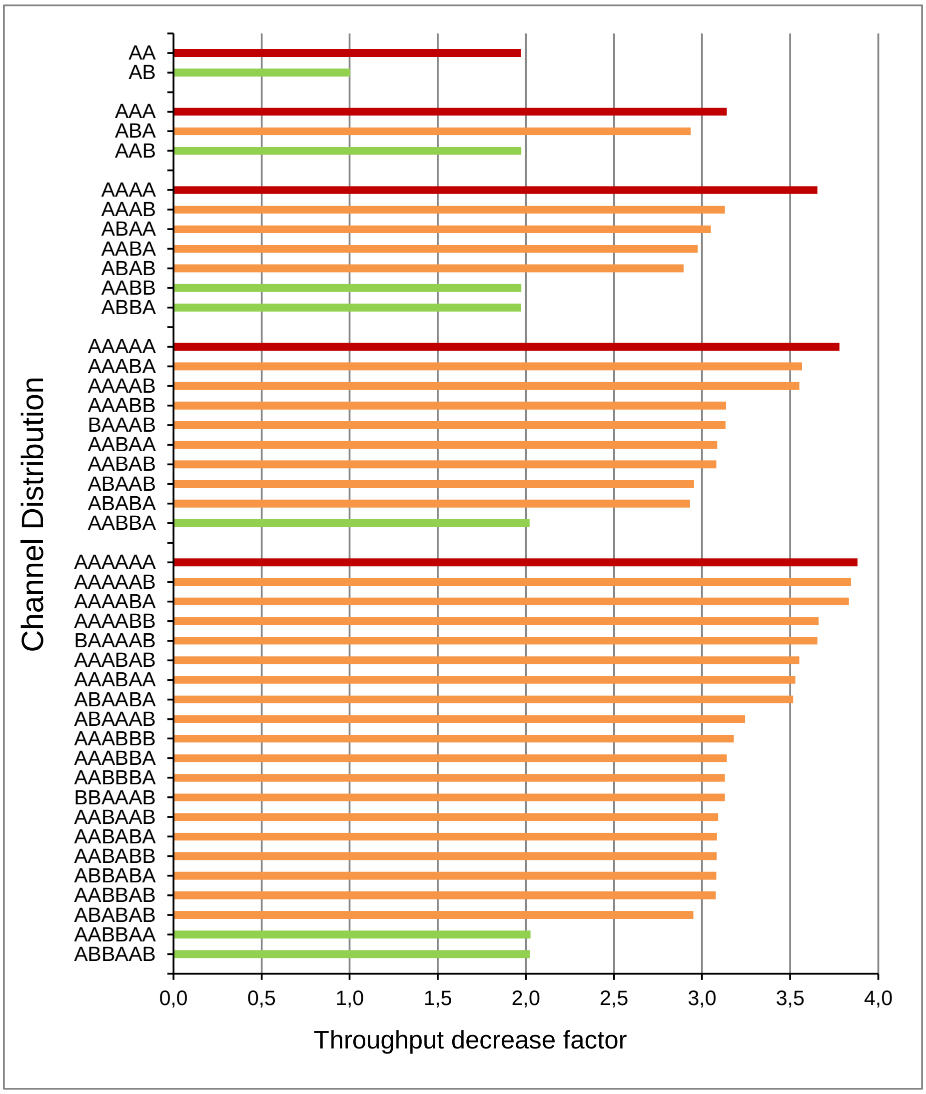


Fig. 3.15: Decrease of the saturation throughput of a simulated chain of nodes according to the number of hops (from 2 up to 6) and the channel distribution. Each node had two radios and two orthogonal channels, A and B, were available.

Although the benefits of multi-radio routing are obvious, its application to real deployments should deal with the hardware limitations of nowadays wireless NICs. Different state-of-the-art studies prove that cross-channel interference between theoretically non-overlapping channels can occur if the transmitter is close to the receiver (about 30-40 centimeters) radios [96][97]. This is the usual case of multi-radio nodes. This phenomenon is known as the near-far effect and can be mitigated by increasing the attenuation of the interfering signal at the receiver; i.e. using better filters or increasing the distance between antennas.

On the other hand, there are some solutions which exploit the utilization of overlapping channels to obtain a higher number of channel alternatives and provide a more efficient utilization of the available spectrum [27][28][98]. Depending on channel separation and the distance between interferers, two overlapping transmissions can occur suffering only a slightly performance degradation [98].

Anyway, in both overlapping and non-overlapping cases, a proper estimation of the interference level in multi-radio networks should consider physical parameters. Since this is complex to obtain and model at the routing level, most state-of-the-art solutions assume that nodes assigned to different orthogonal channels do not interfere each other [27][28].

The channel to be used by a transmission is determined by a Channel Assignment Algorithm. Since channel distribution directly affects the topology of the network and the availability of the routes, there is a trade-off between network connectivity and channel diversity. Higher channel diversity decreases the interference between adjacent nodes, but can lead to network partitioning or the formation of suboptimal routes if channel sharing is too sparse. In conclusion, there is a circular dependency or trade-off between routing/connectivity and channel assignment [28][99][100], as shown in Fig. 3.16.

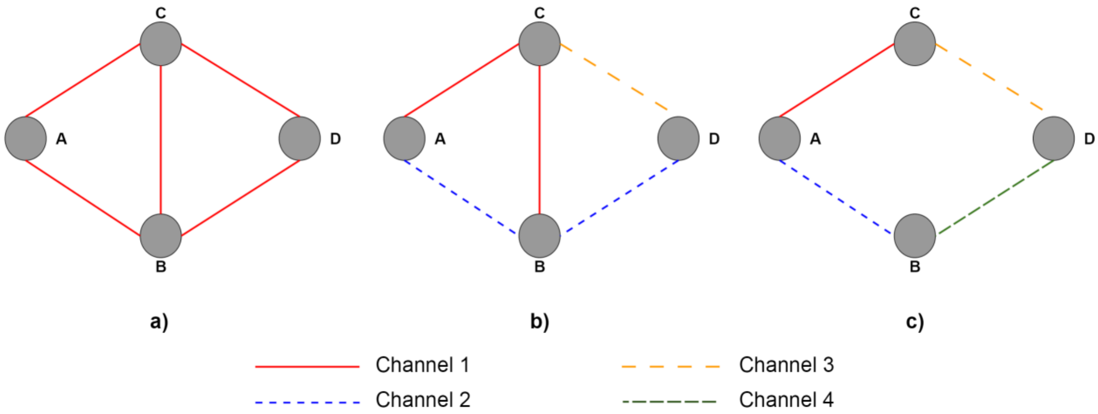


Fig. 3.16: Trade-off between channel diversity and routing/connectivity when using nodes equipped with two radios. In (a), the single-channel single-radio case shows the connectivity of the network. In (b), three channels are used in order to reduce interference without reducing connectivity. However, different links re-use some of the channels. In (c), channel-diversity is maximized by using four channels. However, nodes B and C are yet not connected and a communication between them has to traverse an intermediate node.

Due to the dependency of network topology on the channel assignment, the following problems can affect traffic performance on multi-radio multi-hop networks [27]:

- **Network partition and link breaks**: Channel assignment can cause some paths to be unavailable during route creation. Also, if channel reassignment occurs, active routes can become broken due to the disconnection of previously connected neighbors.
- **Broadcast**: Most routing protocols broadcast signaling messages during route creation and maintenance procedures. Thus, mechanisms should be implemented in order to

assure that broadcast messages can be received by neighbors assigned to different channels.

- **Deafness**: In dynamic assignments, it should be assured that receivers are in the same channel as transmitters when starting data or RTS transmissions. Also, carrier sensing can fail if the interferer was situated in another channel during preamble transmission and then switched to the same channel during data transmission, leading to a hidden node case.

Indeed, these issues are similar to the Communications Gray Zone problem of Rate Adaptation Algorithms described in Section 3.1.2, with the additional difficulty of also losing preambles and broadcast messages. As will be presented in Chapter 6, some proposed CAAs assign a static common channel to one radio of each node in order to avoid these problems [28][99][100][101].

MIWNs can also suffer from the interference of external IEEE 802.11 networks using the same channels or of other technologies using the same ISM band, like Bluetooth, 802.15.4, Zigbee or radars [27][28]. However, the external interference level is complex to quantify since it requires a dedicated interface in monitor mode and, even in this case, only the interference of other IEEE 802.11 networks can be detected [101]. Thus, most CAAs of the state-of-the-art do not consider this source of interference in its designs [27][28].

Finally, channel assignment strategies should also consider that actual wireless interfaces and drivers are not optimized to perform frequent channel switching [26][102]. If not triggered by the user, they are limited to scan operations, where switching delay is not important. Depending on the wireless driver, different studies obtain channel switching delays of the order of milliseconds or hundreds of microseconds [102]. This overhead or switching cost causes a waste of channel time and limits the application of very dynamic channel assignment algorithms (e.g. in a per-packet basis).

3.4 Conclusions

As analyzed in the previous sections, some of the typical problems of wireless communications, like channel variability or interference, become more complex to deal with in MIWNs because of the lack of a centralized management and the impact of multi-hop communications. However, multi-hop routing brings also an opportunity to alleviate these problems, for instance discovering alternate paths that traverse less congested zones or faster links. Thus, enhanced routing protocols can significantly improve the performance of traffic flows traversing MIWNs.

Due to the well-known inefficiency of the classic routing procedure based on the number of hops, the utilization of link quality-aware mechanisms is nowadays very accepted [17][20][37][51][52]. Thus, as will be presented in Chapter 4, most state-of-the-art routing metrics use as start point an estimation of the error [59] and bit rate of the link [43]. Challenges on this topic include estimation methodologies and its integration with other routing procedures, like path maintenance.

Contention and interference-awareness is also commonly applied in route creation [17][51][52] and channel assignment [26][27][100] mechanisms. As analyzed in this chapter, interference and contention levels depend on several physical and MAC phenomena, thus the definition of a proper wireless interference model applicable at the routing layer is required [13][52][71]. Also, although load-awareness in multi-hop networks is very challenging since it can compromise the stability of the network [37], it should be applied in order to properly model contention and interference in terms of channel occupancy. Finally, a proper interference model should also take into account the different impact of contending nodes, hidden nodes and remote interferers on the perceived CO [13][24][52][89][92].

Regarding multi-radio multi-channel solutions, they should consider the trade-off between interference reduction and topology preservation [28][99][100]. Indeed, the circular dependency between routing and channel assignment leads to a NP-hard problem when trying to find an optimal channel assignment solution [99]. Finally, practical limitations, like the channel switching delay [102], the real interference level of non-overlapping [96] and partially overlapping channels [98] or the external interference [101], should also be considered.

Next chapters analyze the state-of-the-art on these topics and present the different contributions of this thesis.

4

Route creation in MIWNs

Route creation basically depends on the combination of a routing protocol and a routing metric. Considerable research effort has been devoted to this procedure, since the routing of flows through appropriate paths can mitigate the performance degradations analyzed in Chapter 3.

The first section of this chapter introduces the basics of path creation in MIWNs, including an overview on AODV and OLSR, since most routing protocol implementations in this area are based on these two protocols. Also, some extensions or enhancements, like multipath routing or QoS provisioning are discussed. Then, next section presents routing metrics requirements and reviews the most relevant proposals of the state-of-the-art. The third section of this chapter describes and analyzes the proposed approach to enhance route creation in MIWNs: the Flow-based Ad-hoc On-demand Distance Vector routing protocol (FB-AODV) and the Weighted Contention and Interference routing Metric (WCIM). Finally, the conclusions of this chapter are presented.

4.1 Routing protocols

Depending on when routes are created, the basic typology of routing protocols considers two main categories: reactive or proactive [16][103]. Reactive routes are created on-demand, according to the destinations of the traffic flows. Usually, the on-demand route discovery mechanism is based on the source flooding the entire network with request messages, which are answered by the destination. This flooding-based algorithm is in fact an adaptation of the Bellman-Ford algorithm for distance-vector routing, where only the routes to the source (request messages) and destination (response messages) are propagated [103]. On the other hand, using proactive protocols, each node obtains a path to every other node of the network regardless of the traffic flows. Nodes transmit periodically their routing information and make use of calculation algorithms like Bellman-Ford or Dijkstra, distance-vector or link-state routing, respectively, to compute the optimal paths [103].

Once the algorithm decides the optimal path, which requires the definition of a routing metric as will be introduced in next sections, nodes should forward the packets to the required destination. According to their packet forwarding scheme, two additional routing protocols categories can be considered: source routing or hop-by-hop routing [103]. Using source routing, the whole path is transported in the packet header; i.e., intermediate nodes only need to forward packets based on the information of the IP headers. Although this scheme avoids route loops, it generates an excessive overhead per packet. Thus, its utilization is very uncommon [48]. On the other hand, using hop-by-hop routing the IP headers only carry the destination address and intermediate nodes take forwarding decisions based on their routing tables, which have been created during the path discovery procedure. This scheme, which is the most common in IP networks, limits the overhead per packet, but needs of a careful design of the routing protocols and its metrics in order to avoid route loops and inconsistencies [41][46][47][103].

Next sections describe AODV [41] and OLSR [46], which are the most relevant reactive and proactive protocols, respectively, both based on hop-by-hop routing. Also, some relevant routing protocol extensions and enhancements are presented.

4.1.1 AODV

When a node requires a new route, AODV initiates a route discovery procedure by broadcasting Route Request (RREQ) messages. The routing metric is computed each time a node receives a RREQ message. The node accumulates the metric of the link from which the RREQ was received to the total path metric carried in the RREQ. If the routing metric computed is the minimum discovered so far, it saves the reverse route and continues broadcasting the RREQ. Otherwise, the RREQ is discarded. Upon reception of the RREQ message, the destination sends a Route Reply (RREP) message back to the source node. Optionally, an intermediate node can also reply the source node if having a valid route entry to the demanded destination. Also, in order to discover neighbors and detect broken links, nodes broadcast Hello messages periodically. As will be described in next sections, Hello messages are usually utilized to exchange the information required to compute routing metrics.

The lifetime of a route is updated with each forwarded packet and expires after a defined timeout without traffic. Since its routing algorithm is based on distance-vector and hop-by-hop routing, AODV uses destination sequence numbers in order to avoid route loops; nodes discard RREQ or RREP messages whose sequence numbers are lower than the saved ones for the same destination.

In addition to the paths between the nodes joining the network, AODV can form routes to external networks like the Internet. This can be accomplished by permitting gateway/portal nodes to send RREPs on behalf the required external destinations. Also, some relevant AODV implementations use proactive spanning trees to create and maintain routes to the gateways [104]. This is also the case of the HWMP protocol defined for 802.11s, which, as mentioned in Section 2.1.3.1, is a hybrid modification of AODV [2][42]. Hybrid routing permits to avoid route creation delay and maintain updated paths for commonly needed paths, as is the case of the routes to the Internet.

Actually, the second version of AODV is being discussed by MANET Working Group (internet draft) [49]. Formerly known as Dynamic MANET On-demand (DYMO), this new version basically uses Generalized MANET Packet/Message Format RFC 5444 [105] for the signaling messages and enables the use of generic metrics, although the hop count metric is still considered the default one.

4.1.2 OLSR

OLSR proactive routing is based on the Dijkstra algorithm, where each node should obtain the whole network topology. In order to form and update the routes, the nodes periodically announce their neighbors, together with their associated link metric, by broadcasting Topology Control messages (TC), which are flooded through the network. When receiving a TC message, the node decides if the transmitter is the best next hop to an announced destination according to the accumulated routing.

In order to reduce overhead and optimize flooding, OLSR implements the Multipoint Relay (MPR) strategy. Basically, by using Hello messages, each node obtains a minimum set of one-hop neighbors required to reach all its two-hop neighbors. These nodes are its MPR nodes set. Then, for each node, only its MPRs will retransmit its Topology Control messages (TC).

The second version of OLSR obtained the RFC status in April 2014 (RFC 7181) [50]. As in the case of AODV, the revision basically updates the format of the signaling messages by adopting RFCs 5444 [105], and enhances route selection by enabling the use of a link metric other than hop count. Also, the MANET Neighborhood Discovery Protocol (NHDP) defined in RFC 6130

[106] is used by the MPR algorithm. Finally, signaling framework is simplified by also using TC messages for announcing multiple interfaces and gateways to external networks, instead of the Multiple Interface Declaration (MID) and Host and Network Association (HNA) messages defined by OLSRv1.

4.1.3 Extensions and enhancements

The routing of inelastic flows and the application of QoS mechanisms like resource reservation or admission control is very challenging in MIWNs [53][107][108]. Compared to wired networks or single-hop wireless networks, the inherent characteristics of multi-hop wireless networks complicate the estimation or quantification of the route resources and the impact of new flows on the active ones; the quality of the routes is difficult to predict due to the variability of the wireless channel and the interference caused by multi-hop routing.

Some proposals define QoS frameworks which monitor the active routes and apply different procedures if the QoS requirements are not satisfied, like the reallocation, the cancellation or the reduction of the data rate of best-effort or elastic flows [53][108]. However, most QoS proposals integrate admission control and resource estimation and reservation in the path discovery procedure of the routing protocols [87][107]. For instance, if a flow has a minimum bandwidth requirement, links with insufficient bandwidth will be not considered during path discovery. Also, in case of minimum delay requirement, paths whose accumulated delay exceeds the delay threshold will be discarded. These mechanisms are generally more suited for on-demand routing protocols, since route decisions depend on the incoming communications [107].

Some routing protocols consider the utilization of multiple simultaneous paths between a source and a destination [109]. By using link-disjoint or node-disjoint paths, multipath routing can increase the reliability of communications in case of link degradations or node mobility. Also, load balancing can be applied by distributing the packets of the flows through different paths. However, due to route coupling, using simultaneous paths for each flow can increase interference and contention due to the augment of transmissions and the utilization of additional links [110]. It also adds more complexity to the routing protocols, since most algorithms are destination-based and designed to obtain a single optimal route [41][46][103].

Large networks can compromise the functionality of routing protocols [11][16][18][111]. Signaling overhead increases significantly, while the discovery and maintenance of longer and numerous paths become complex. Thus, some solutions make use of hierarchical routing in order to obtain a scalable solution [16][112]. In hierarchical routing, nodes are organized into groups called zones or clusters, where each group contains at least one cluster head or border node. Nodes can communicate normally within its cluster zone, while communications with nodes in other zones are managed by cluster heads. For instance, the Zone Routing Protocol (ZRP) uses a hybrid routing approach [113]; while the inner routes are maintained proactively, the outer are discovered on-demand by the border nodes. However, the creation and maintenance of the hierarchy can become complex, for instance in case of mobile nodes, and using border nodes for outer communications can lead to bottlenecks, inefficient routes or disconnections.

The Better Approach To Mobile Ad hoc Networking (BATMAN) routing protocol is a link-state routing protocol also intended for large networks [114]. Its aim is to obtain an efficient and low-complexity solution for embedded devices. Instead of computing all the paths to the rest of the nodes as OLSR does, using BATMAN the nodes only decide the neighbor which is the best forwarding option to a specific destination, leading a lower signaling overhead. The neighbor which transmits the highest number of Originator messages (OGs) from a specific source, which are broadcasted periodically and flooded through the entire network, is assumed to form part of the less congested and more reliable route to this source. Although BATMAN is an interesting solution due to its simplicity and lightness, as was mentioned in chapter 3, the routing performance of broadcast and unicast messages may differ due to MAC retransmissions and the utilization of different link rates [77][81]. Therefore, it can lead to the formation of suboptimal paths.

4.2 Routing metrics

During route creation, multiple paths or next-hop alternatives are discovered. In order to quantify their quality or suitability, and select the optimal paths, routings metrics are used. Usually, the routing metric is defined as additive; i.e. its value is increased with each additional link or hop. In fact, one of the most basic routing metrics is the number of hops, which tries to minimize the number of traversed links or nodes between the source and the destination. In MIWNs, the hop-count metric correctly characterizes some of the issues which affect traffic performance: the shorter are the paths, less transmissions are needed, what usually leads to lower delays and higher throughputs [13].

However, the hop count metric uses a binary logic to characterize the links between neighbor nodes; i.e. a value of 1 if the link exists or an infinite value if not. As analyzed in Chapter 3, this logic does not consider the variable quality of the links due to phenomena related with the physical and MAC layers. Thus, recent routing metrics integrate cross-layer information into link characterization [17]. For instance, AODVv2 and OLSRv2 proposals permit the usage of alternative routing metrics instead of the usually inefficient minimum hop routing used by their former versions [49][50]. Also, the 802.11s standard defines a link-quality aware metric and permits other enhancements by means of the extensible path selection framework [2][42].

Two main properties should be considered when designing a routing metric in order to assure the creation of optimal paths: isotonicity and monotonicity [37][103]. A routing metric is isotonic if the relation between the weights of two links or path sections is preserved if appended or prefixed to another link or path section. On the other hand, a routing metric is monotonic if the weight of a link or path section does not decrease with the previous or the following links or path sections. Fig. 4.1 illustrates these two properties.

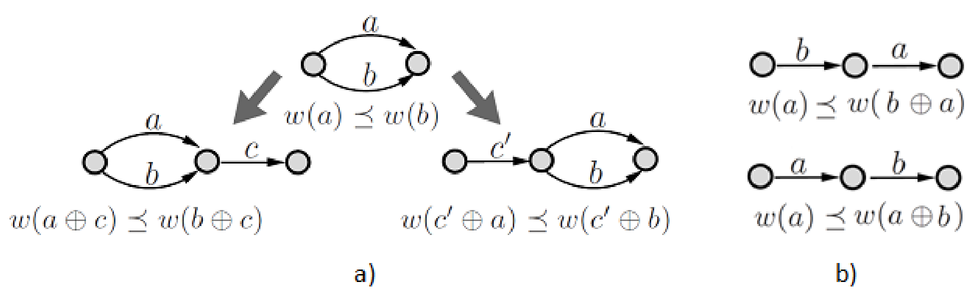


Fig. 4.1: Routing metric properties: (a) Isotonicity and (b) monotonicity. The weight function of a path section or link *a* is denoted as *w(a).*

During route creation, and also during packet forwarding if hop-by-hop routing is being used, intermediate nodes decide the optimal path to a destination according to the routing metric value of the path section between itself and the destination. If isotonicity and/or monotonicity properties are not met, this path section could be suboptimal considering the whole path from the source. This is illustrated in Fig. 4.2.

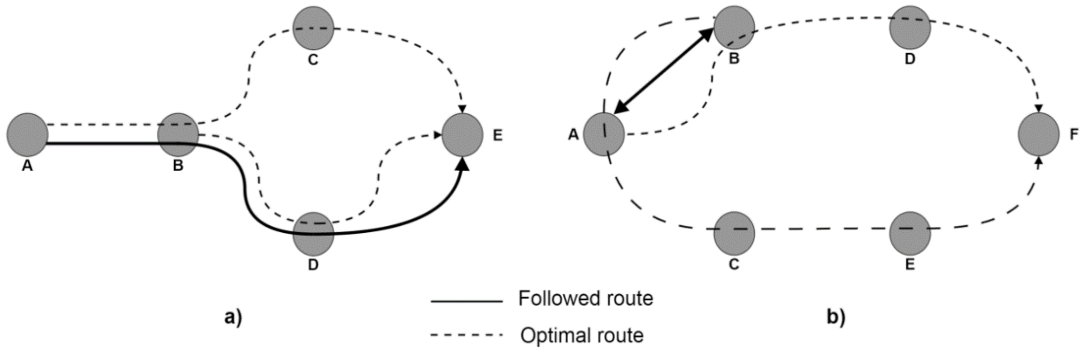


Fig. 4.2: Suboptimal routes and loops due to the lack of isotonicity and/or monotonicity. In (a), the optimal route between node A and node E should traverse nodes B and C. However, the optimal route from node B to node E is through D. Thus, the final route between A and E is A-B-D-E, which is suboptimal for this flow. In (b), the optimal path between node A and F is A-B-D-F. However, the optimal path between B and F is B-A-C-E-F. Thus, if using hop-by-hop routing, both routes have a loop in the link between A and B.

Basically, the design of a routing metric comprehends the selection of one or more parameters which impact traffic performance (e.g. hop count, link bit rate, interference level…), the implementation of an estimation methodology and the definition of an algorithm which gives different weights to the links according to these parameters [103]. Some state-of-the-art solutions consider the usage of multiple link metrics in order to obtain the optimal path according to different independent parameters [115]. However, considering two or more routing metrics or QoS constraints in route creation leads to a NP-complete problem and increases significantly the complexity of the algorithms [87][115]

Next subsections present significant state-of-the-art routing metrics according to its load-awareness.

4.2.1 Load-unaware routing metrics

The Expected Transmission Count (ETX) [59] metric was one of the first attempts to increase performance in WMNs as an alternative to the hop count metric (also denoted as HOPS from this point forward). This metric estimates the expected number of transmission attempts for a packet through a link. A node only needs to compute the packet error probability in transmission and reception, denoted in Equation (4.1) as d_i and d_j, respectively, to obtain the link cost, denoted by ETX_{ij}. Both link directions are considered, since successful frame transmission requires the reception of an ACK frame in 802.11 CSMA/CA. Then, final metric of a path p is the sum of the ETX values of all the links ij forming the path.

$$ETX(p) = \sum_{\forall ij \in p} ETX_{ij} = \sum_{\forall ij \in p} \left[\frac{1}{d_i \times d_j} \right] \qquad (4.1)$$

ETX has been widely adopted due to its simplicity and good performance in front of the hop count metric [59][116]. As was introduced in Section 3.1.1, its major drawbacks are related to the link error estimation mechanism based on monitoring periodically broadcasted Hello messages: the error rate of data packets can differ significantly [81] and variability-awareness depends on the periodicity of the probe messages [79]. The following proposals aim to improve to performance of ETX:

- The Modified ETX (mETX) and the Effective Number of Transmissions (ENT) routing metrics enhance ETX performance in high variable channels [79]. They characterize the bit error probability on a link as a stationary stochastic process and use its mean and variance to represent slow and rapid variations, respectively. Both metrics introduce extra complexity to the link quality estimation since they require to process packets at the bit level.
- The Minimum Loss Metric (ML) uses a multiplicative approach to obtain the ETX metric of a path instead of the additive one [117]. Authors of ML argue that utilization of additive ETX favors shorter paths with higher Packet Loss Rates (PLRs) over longer paths with smaller PLRs, since it is based on minimizing the number of transmissions instead of maximizing the transmission probability. Thus, it leads to a lower number of received packets. However, due to its multiplicative nature, ML does not scale with the number of hops, thus underestimating intra-flow interference. For instance, it cannot differentiate paths composed of two perfect links from paths composed of three perfect links.

The Expected Transmission Time metric (ETT) improves the ETX metric, as it aims to take into account the link bandwidth, thus favoring fast links with low error rates [43]. In order to achieve this goal, ETT_{ij} estimates the time required for the transmission of a packet through the link between nodes i and j. ETT_{ij} builds on the basis of ETX_{ij}, the transmission bit rate of the link, LR_{ij} and the size of a probe packet, S, as shown in Equation (4.2). As introduced in Section 3.1.2, the usual link bit rate estimation mechanisms is based on pairs of probe packets [43][83][84], where S is the size of the second packet.

$$ETT(p) = \sum_{\forall ij \in p} ETT_{ij} = \sum_{\forall ij \in p} \left[ETX_{ij} \times \frac{S}{LR_{ij}} \right] \tag{4.2}$$

The Airtime Link Metric (ALM), a routing metric defined in the IEEE 802.11s draft standard [2], estimates the channel following principles similar to those of ETT. ALM estimates the channel time required for packet transmission through a link. Equation (4.3) shows the metric definition, where O denotes the physical and MAC layer overheads, S is the size of the probe frame, LR_{ij} is the transmission bit rate and e_f is the frame error rate for the probe frame.

$$ALM(p) = \sum_{\forall ij \in p} ALM_{ij} = \sum_{\forall ij \in p} \left[(O + \frac{S}{LR_{ij}}) \times \frac{1}{1 - e_f} \right] \tag{4.3}$$

Like the ALM, the Medium Time Metric (MTM) is defined as an estimation of the medium transmission time of a packet through a path [118]. Also, a vector extension to MTM has been proposed, where different packet sizes are defined to calculate various metric values [119]. Consequently, different traffic types can be classified according to their packet lengths and routed via different paths if necessary.

The above introduced routing metrics improve the simple hop count metric by using link quality information. However, such metrics can also concentrate traffic on the highest quality links, which can produce congestion. Although also being load-unaware, the following routing metrics consider intra-flow and inter-flow interference in order to route flows through links with a lower probability of becoming congested.

The Weighted Cumulative ETT (WCETT) routing metric extends ETT by considering intra-flow interference in multi-channel networks, thus aiming to minimize the reuse of channels along a route [43]. Assuming a total of K available channels, the parameter X_c is the sum of the ETT metrics of all links ij of the path p using channel c, as defined in Equation (4.4). Then, the WCETT metric adds the maximum Xc value of the path to the ETT metric, as shown in Equation (4.5).

$$X_c = \sum_{\forall ij \in p \; using \; channel \; c} ETT_{ij} \tag{4.4}$$

$$WCETT(p) = (1 - \beta) \times \sum_{\forall ij \in p} ETT_{ij} + \beta \times \max_{c \in K} X_c \tag{4.5}$$

WCETT is defined as a tradeoff between delay and throughput, weighted by the tunable parameter β; the first term gives an estimation of the delay of the path, while the second term represents the impact of bottleneck hops (i.e. hops using the same channel) on the throughput [43]. However, WCETT does not consider the impact of inter-flow interference on the performance of the flows. Also, as was shown in Fig. 3.15 of Section 3.3, the real level of intra-flow interference depends on the distance between the links reusing the same channel (e.g. two remote links using the same channel can transmit without interference).

The Metric of Interference and Channel-switching (MIC) considers both inter-flow and intra-flow interference [37]. The Interference-aware Resource Usage (IRU) component scales the ETT metric of a link by the number of its one-hop neighbors N_{ij}, as shown in Equation (4.6). On the other hand, as defined in Equation (4.8), the value of the Channel Switching Cost (CSC) component of a link depends on the channel of the previous hop: w_1 if the channels are different or w_2 if they are equal, where $0 \leq w1 \leq w2$. Finally, the MIC metric of a path is the sum of both components, as shown in Equation (4.8).

$$IRU_{ij} = ETT_{ij} \times N_{ij} \tag{4.6}$$

$$CSC_{ij} = \begin{cases} w_1 & \text{if channel(ij)} \neq \text{channel (hi)} \\ w_2 & \text{if channel(ij)} = \text{channel (hi)} \end{cases} \tag{4.7}$$

$$MIC(p) = \sum_{\forall ij \in p} IRU_{ij} + \sum_{\forall ij \in p} CSC_{ij} \tag{4.8}$$

MIC aims to reduce inter-flow and intra-flow interference by searching for links sharing the channel with few neighbors and by favoring paths with more diversified channel assignments, respectively [37]. However, the IRU component does not consider the channel time consumption of the neighbors (e.g. slower or lossy neighbors consume more channel time). In addition, the alternation of channels can lead to the creation of hidden nodes, which degrades flow performance as was shown in Fig. 3.15 of Section 3.3.

The Exclusive Expected Transmission Time (EETT) metric is defined in a similar way to MIC [120]. However, in this case the cost of a link ij , which is denoted by $EETT_{ij}$ is computed as the sum of the ETT metrics of all the links in the interfering set of link ij, denoted by $IS(ij)$, including link ij itself. Thus, since the ETT metric of a link also determines its channel time consumption, EETT represents the congestion or interference on a specific interfering set with greater accuracy than MIC. However, EETT does not consider intra-flow interference.

$$EETT(p) = \sum_{\forall ij \in p} EETT_{ij} = \sum_{\forall ij \in p} \left[\sum_{\forall l \in IS(ij)} ETT_l \right] \tag{4.9}$$

The Contention-Aware Transmission Time (CATT) [121] and the Interferer Neighbors Count (INX) [122] are two other significant routing metrics of the state-of-the-art with a similar definition to EETT, both scaling the ETT metric of a link by the channel occupancy of its neighbors.

4.2.2 Load-aware routing metrics

Load-unaware metrics assume that all the neighbors of each node continuously contribute to inter-flow interference, which may not accurately reflect network behavior. Indeed, they tend to concentrate traffic on some specific links and may lead to congestion. On the other hand, load-aware metrics can better distribute flows through the network.

The Load-Aware ETT (LAETT) routing metric extends ETT by considering the load of each traversed link [123]. As shown in Equation (4.10), the ETX_{ij} metric of a link ij is scaled by the remaining capacity of nodes i and j, denoted as RC_i and RC_j, respectively, which are obtained by subtracting the transmission rate of the active flows of the node from its total bandwidth. S is the size of a probe packet, while γ_{ij} is a link quality factor that increases with the distance between nodes i and j.

$$LAETT(p) = \sum_{\forall ij \in p} LAETT_{ij} = \sum_{\forall ij \in p} \left[ETX_{ij} \times \frac{S \times 2 \times \gamma_{ij}}{RC_i + RCj} \right] \tag{4.10}$$

Following a similar approach, the WCETT with Load Balancing (WCETT-LB) routing metric defines an additional parameter $L(p)$ in order to capture the load of traversed nodes, as shown in Equation (4.11) [124]. The load of a node i is estimated in terms of its number of active routes, N_i, and the fraction of its average queue length, QL_i, over its transmission rate, b_i.

$$WCETTLB(p) = WCETT(p) + L(p) = WCETT(p) + \sum_{\forall i \in p} \left[\min(ETT) \times N_i + \frac{QL_i}{bi} \right] \tag{4.11}$$

Both LAETT and WCETT-LB routing metrics are intended to balance load between the nodes of the network. However, they do not consider the interference of adjacent nodes, thus leading to an unreal estimation of the available bandwidth. Therefore, next routing metrics combine interference- and load-awareness in order to estimate available bandwidth more accurately.

The metric used in Load-Balanced Ad hoc Routing (LBAR) is shown in Equation (4.12), where the metric of a node i is the sum of the number of active routes A_j of its N_i one hop-neighbors, including itself [92]. However, it assumes that all routes are traversed by flows with identical characteristics, which may not be true in a real network. Also, it does not consider link-quality parameters.

$$LBAR(p) = \sum_{\forall i \in p} LBAR_i = \sum_{\forall i \in p} \left[\sum_{\forall j \in N_i} A_j \right] \tag{4.12}$$

The Load-Aware Routing Metric (LARM) also considers the interference of the one-hop neighbors of the nodes forming the links, but makes use of the average queue size of the nodes in order to measure their load in a more accurate way [125].

$$LARM_{ij} = ETT_{ij} \times \sum_{\forall k \in N_{ij}} Q_k \tag{4.13}$$

where N_{ij} is the set of one-hop neighbors of ij using the same channel and Q_k is the average queue size of node k. LARM considers the quality of the links by using the ETT metric and is channel-aware. However, defining load in terms of queued packets does not consider the impact of the quality of interfering links on the perceived interference (e.g. packets transmitted at low link rates consume more channel time than those transmitted at higher rates). Finally, as was the case of the WCETT metric, the metric of a path is defined as the weighted sum of the accumulated LARM value of all the traversed links and the LARM value of the bottleneck channel in order to capture intra-flow interference.

$$LARM(p) = (1-\beta) \times \sum_{\forall ij \in p} LARM_{ij} + \beta \times \max_{c \in K} \left(\sum_{\forall ij \in p \; using \; channel \; c} LARM_{ij} \right) \tag{4.14}$$

The Interference-Load Aware (ILA) metric [126] considers inter-flow interference by means of the Metric of Traffic Interference (MTI). ILA calculates the cost of a link ij, MTI_{ij}, as follows:

$$MTI_{ij} = \begin{cases} \dfrac{ETT_{ij}}{ETT_{\min}} & if \;\; NI_{ij} = 0 \\ \dfrac{ETT_{ij} \times AIL_{ji}}{ETT_{\min} \times AIL_{\min}} & if \;\; NI_{ij} \neq 0 \end{cases} \tag{4.15}$$

where NI_{ij} is the number of one-hop neighbors of nodes i and j with active flows. If there are interfering nodes, the MTI_{ij} scales the ETT_{ij} by the Average Interference Load (AIL) affecting transmissions from node i to j, denoted by AIL_{ij}. ETT_{min} and AIL_{min} are the smallest values in the network for ETT and AIL, respectively, and are used for scaling purposes. The AIL_{ij} is defined in Equation (4.16), where IL^k denotes the interference load, i.e., the load of the k-th neighbor that causes interference on transmissions between i and j.

$$AIL_{ij} = \frac{\sum_{\forall k \in NI_{ij}} IL_k}{NI_{ij}} \tag{4.16}$$

IL_k is defined as the number of bytes transmitted [126]. As in the LARM case, this definition does not capture the effect of link quality on interference. Finally, the ILA metric of a path is defined as follows:

$$ILA(p) = \sum_{\forall ij \in p} MTI_{ij} + \sum_{\forall ij \in p} CSC_{ij} \tag{4.17}$$

where the CSC parameter captures the intra-flow interference as was defined in Equation (4.7).

The Hidden Node Problem Aware routing metric (HNPA) is an enhancement of the ALM routing metric for 802.11s which aims to avoid the performance degradation caused by hidden nodes[127]. As shown in Equation (4.18), the HNPA metric of a link *ij* is the fraction of its ALM_{ij} metric and an estimation of the packet success ratio:

$$HNPA(p) = \sum_{\forall ij \in p} HNPA_{ij} = \sum_{\forall ij \in p} \frac{ALM_{ij}}{\prod_{k \in HN_{ij}} (1 - TX_k)} \tag{4.18}$$

where TX_k is the transmission time ratio of node k and the HN_{ij} is the set of hidden nodes of node *ij*. The transmission ratio is defined as the fraction of time utilized in the MAC level for packet transmission. Although HNPA is aware of the significant impact of hidden nodes on traffic performance, it does not consider other interference sources like contention nodes or remote interfering nodes.

The Interference Aware Routing (IAR) metric [88] also makes use of MAC-level measurements to estimate link congestion due to the interference from other nodes. The metric of a path is defined by the following Equations:

$$IAR(p) = \sum_{\forall ij \in p} IAR_{ij} = \sum_{\forall ij \in p} \frac{1}{1 - UB_i} \times \frac{S}{LR_{ij}} \tag{4.19}$$

$$UB_i = \frac{T_{Wait} + T_{Collision} + T_{Backoff}}{T_{Wait} + T_{Collision} + T_{Backoff} + T_{Success}} \tag{4.20}$$

where T_{Wait}, $T_{Collision}$, $T_{Backoff}$ and $T_{Success}$ quantify the time spent in the respective states of packet transmission at MAC-level. These time values are obtained via passive measurements (i.e. by using active transmissions in the node) or by active probing, which adds protocol overhead. Thus, in a similar way than the HNPA metric, IAR scales the transmission time of a link by the so-called Unproductive Busyness (UB) ratio, which considers the time loss in MAC states different to the success one.

iAWARE is an interference-aware routing metric defined for a multi-radio routing protocol [128]. The iAWARE routing metric of a link is calculated as follows:

$$iAWARE_{ij} = \frac{ETT_{ij}}{IR_{ij}} \quad (4.21)$$

iAWARE basically weights the ETT metric of link ij by the corresponding Interference Ratio (IR), denoted by IR_{ij}. This parameter is calculated as the minimum value of the ratio between the Signal to Interference and Noise Ratio (SINR) and the Signal to Noise Ratio (SNR), sensed by both nodes forming the link ij. Finally, the iAWARE metric of a path adds the intra-flow component by considering the bottleneck channel in the same way than previous introduced metrics.

$$iAWARE(p) = (1-\beta) \times iAWARE_{ij} + \beta \times \max_{c \in K}\left(\sum_{\forall ij \in p \; using \; channel \; c} iAWARE_{ij} \right) \quad 4.22)$$

SNR and SINR values are obtained from radio interface measurements, thus iAWARE metric is dependent on the hardware used. In addition, computing the SINR of a link in an accurate way is almost infeasible [80]. Finally, since the IR_{ij} parameter is defined as the minimum IR sensed by both nodes forming the link, it only captures contention in sending or interference in receiving (i.e. both phenomena cannot be dealt with simultaneously).

4.3 Proposed approach

As presented in the previous sections, in order to improve the performance of the flows traversing MIWNs networks, considerable research effort has been devoted to enhance the path creation procedure of MANET routing protocols, mostly oriented to the definition of a proper routing metric.

The utilization of link-quality metrics has become a de-facto standard; indeed, as denoted in the previous section, most proposals take as starting point ETX or ETT routing metrics or implement minor variations. Link-quality metrics provide a simple alternative to the hop count permitting the routing protocol to differentiate between good and bad links. In addition, they are intended to be more stable due to its interference- and load-unawareness [37]. Therefore, link-quality routing metrics are usually combined with proactive routing protocols and applied to scenarios oriented to the formation and maintenance of long-term and best-effort paths, as is the case of community networks. However, as pointed out by several studies, in the presence of interfering traffic, the ETX value of a link can suffer of uncontrolled and frequent variations due to collisions, leading to poor performance and even network instability [129][130][131].

Interference-aware but load-unaware routing metrics basically capture the topology of the network: links or nodes with a higher number of potential interferers are more probable to suffer contention and collisions. Also, interference will be more or less probable depending on the link-quality of the interferers due to its impact on channel time consumption. However, this routing strategy is not able to balance the load through the network and tends to concentrate traffic on some specific links, which can lead in fact to congestion and interference [16].

On the other hand, load-aware routing metrics can be used to distribute the load through the different links of the network. As occurs in fixed networks, the own load of traversed nodes can be a sign of congestion. However, due to the wireless medium, the load of interferers should be considered in order to obtain a proper estimation of the channel load or occupancy. In order to estimate interference level, routing metrics made use of different approaches. As analyzed in Chapter 3, the impact of interference on performance depends on the relative position between interferers, transmitters and receivers. However, usually the interference range of a link is modeled as its one-hop neighborhood, while few routing metrics consider the interference of more remote nodes or the detection of hidden nodes. On the other hand, some solutions make use of MAC and physical statistics and measurements to obtain interference estimation. This requires of cross-layer implementations and can limit their practical application to specific NIC drivers.

Multi-radio and multi-channel networks also impact the design of routing metrics and protocols. Multi-radio inter-flow interference can be easily integrated into routing metrics by considering only the interference of links using the same channel or overlapping channels. However, intra-flow interference is more complex to quantify during route creation since the intra-flow level of a link depends on previous and next link selections. In fact, both methods utilized to integrate intra-flow interference into routing metrics, the bottleneck-channel and the Channel Switching Cost, defined in Equations (4.4) and (4.7), respectively, break the isotonicity requirement. Therefore, they can lead to the formation of suboptimal paths and loops [37][103]. While the CSC component can be turned isotonic by using a complex algorithm based on virtual nodes [37], there is no efficient algorithm that can find loop-free minimum paths for the bottleneck-channel component [103]. Nevertheless, both methods are inapplicable to practical solutions [16].

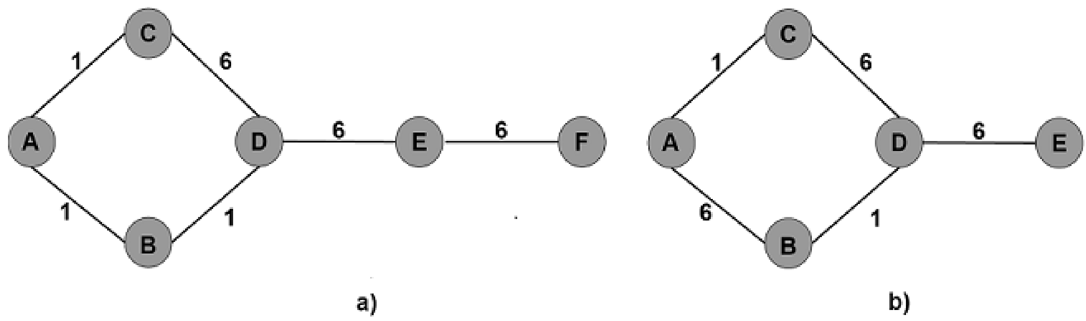


Fig. 4.3: Formation of suboptimal paths caused by (a) bottleneck-channel and (b) CSC intra-flow interference components. In a), according to the bottleneck-channel method, the best path between nodes A and F is ABDEF, since it has a better distribution of the channels 1 and 6 through the entire path. However, node D will decide that its best path to node A is ACD, thus finally leading to formation of the suboptimal path ACDEF. In b), according to the CSC method, both sections ACD and ABD are equivalent and either can be selected by node D as the optimal path to A. However, the optimal route between nodes A and E should be ABDE.

The definition of a routing metric which enhances the performance of the traffics flows traversing MIWNs is one of the contributions of this thesis [52]. From the analysis of the state-of-the-art reviewed in the previous section and the conclusions presented in Chapter 3, the following requirements are considered:

- **Link-quality awareness**: The routing metric should include mechanisms to obtain information about link characteristics, such as error rate and transmission bit rate. These two parameters are fundamental to determine the throughput and delay of a specific link. But they also affect the interference over adjacent links, since the channel consumption of slower or lossy links (i.e. links which require more retransmissions) is higher.
- **Load and interference-awareness**: Due to interference, a wireless link can suffer of lower transmission attempts or a higher number of packet retransmissions or losses. In addition, the occupancy of the shared wireless medium is proportional to the load of the nodes. Also, the interference model should consider the different impact on performance of contending, hidden and remote nodes.
- **Channel-awareness:** The interference model should be aware of the channels being used by interfering links. Intra-flow interference components should not be included into the routing metric due to its lack of isotonicity. However, additional mechanisms should be considered in order to minimize the impact of intra-flow interference.
- **Traffic differentiation**: Depending on traffic characteristics, a link or a path can be more or less adequate for its routing. For instance, short packets are more affected by the MAC layer overhead relative to each transmission, while larger packets are more sensitive to the bit rate of the links [52]. Thus, patch creation should consider the type of flow to be routed.

Some of the introduced routing metric requirements, like load-awareness and traffic differentiation, directly affect the path creation procedure of the required routing protocol. Thus, next section introduces an enhanced version of the AODV routing protocol, the Flow-based AODV (FB-AODV). Then, a new routing metric called the Weighted Contention and Interference routing Metric (WCIM) will be presented in Section 4.3.2.

4.3.1 Flow-based Ad-hoc On-demand Distance Vector routing protocol

4.3.1.1 Design and implementation

Due to its dependence on traffic flows, load-aware routing metrics can lead to network instability when new routes cause the modification of active ones [37]. In particular, proactive routing protocols like OLSR are more probable to suffer of route oscillations or ripple effect during path creation due to its constant update of routes [132]. Nevertheless, due to its hop-by-hop and destination-based routing nature, also reactive protocols like AODV can suffer of uncontrolled path alterations [37][41]; new flows can cause the modification of active routes if an intermediate node discovers a better route to a common destination (e.g. in the case of routes to the Internet through a common gateway).

In general, destination-based routing is appropriate for load-unaware routing metrics, since the best route to a specific destination should be the best one for all the flows. However, when using load-aware routing metrics, it can lead to the formation of suboptimal paths and complicate load-balancing strategies. On the other hand, a flow-based approach can mitigate these limitations and permit a better control of the active routes. Fig. 4.4 illustrates how flow-based routing can enhance load-balancing.

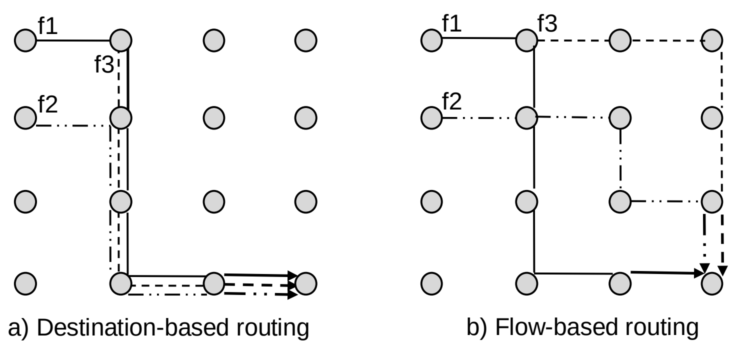


Fig. 4.4: Example of destination- vs flow-based routing. f1, f2 and f3 are three ordered flows with the same destination. In a), all flows share the same path segment from the first common intermediate hop to the destination. Thus, load-balancing is not possible. In b), flow-based routing permits a better flow-distribution in the network, thereby reducing the interference and contention suffered by each flow.

In multi-radio deployments, load-balancing and flow-based routing can also reduce the importance of intra-flow interference awareness during path creation. Intra-flow interference arises when a path becomes saturated by its own traffic. This is more probable to occur in destination-based approaches, since the paths can be used by several flows in an uncontrolled way leading to a high aggregate traffic. However, applying flow granularity during route creation, each path is only traversed by a specific flow and its suitability to route a new flow can be captured by the inter-flow interference component. This is an interesting feature, since, as was introduced in the previous section, the methods to capture intra-flow interference during route creation are inapplicable.

Although there is not a strict definition of what constitutes a traffic flow, some assumptions can be made. First, data from different sources should be considered as independent flows despite having a common destination. This is applied for instance in source-routing solutions [48]. Secondly, following a traffic differentiation approach, the Type of Service (ToS) field of the IP header can be considered in order to distinguish between types of traffic. This way, for instance different routes can be discovered and maintained for Voice over IP (VoIP), video streaming or best-effort traffics, among others.

Flow-based AODV is an enhancement of AODV that permits to route packets on the basis of the destination address, the source address and the Type of Service (ToS) field used by the packets of each flow. The implementation of FB-AODV is based on the following requirements or modifications:

- Sources initiate a new route discovery phase if there is no active route entry for an IP packet according to its destination and ToS.
- Only destinations can answer to RREQ messages, since intermediate nodes cannot have a valid route for a new flow.
- In order to apply hop-by-hop routing instead of source-routing, each intermediate node should maintain different route entries (i.e. different next hops) for each active flow.

In Linux-based systems, as is the case of most MIWNs nodes, flow-based routing can be accomplished by using the Linux Routing Policy DataBase (RPDB), which allows the creation of multiple routing rules and tables according to different IP parameters [133]. Fig. 4.5 illustrates the RPDB of a node which implements FB-AODV.

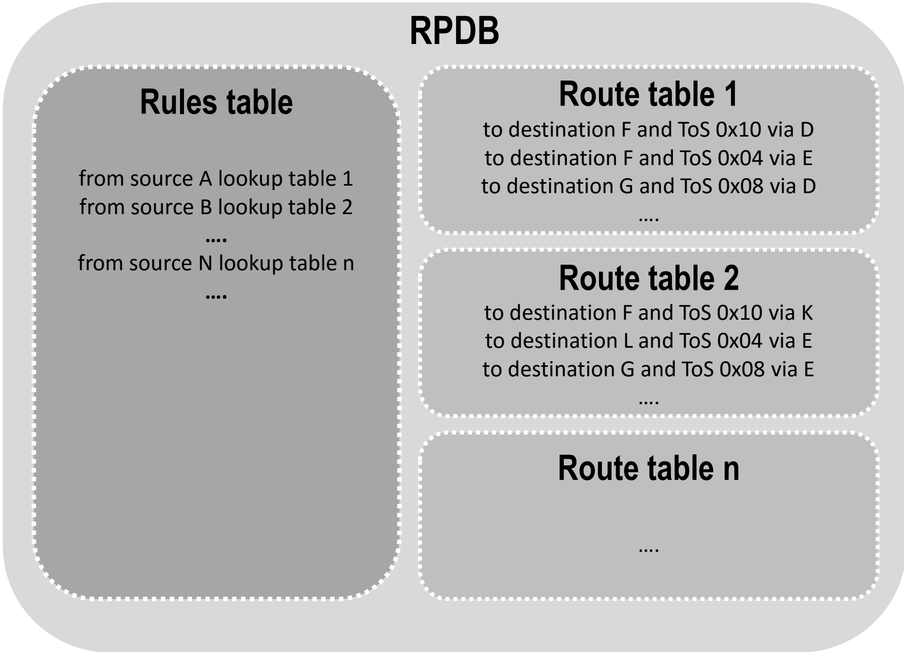
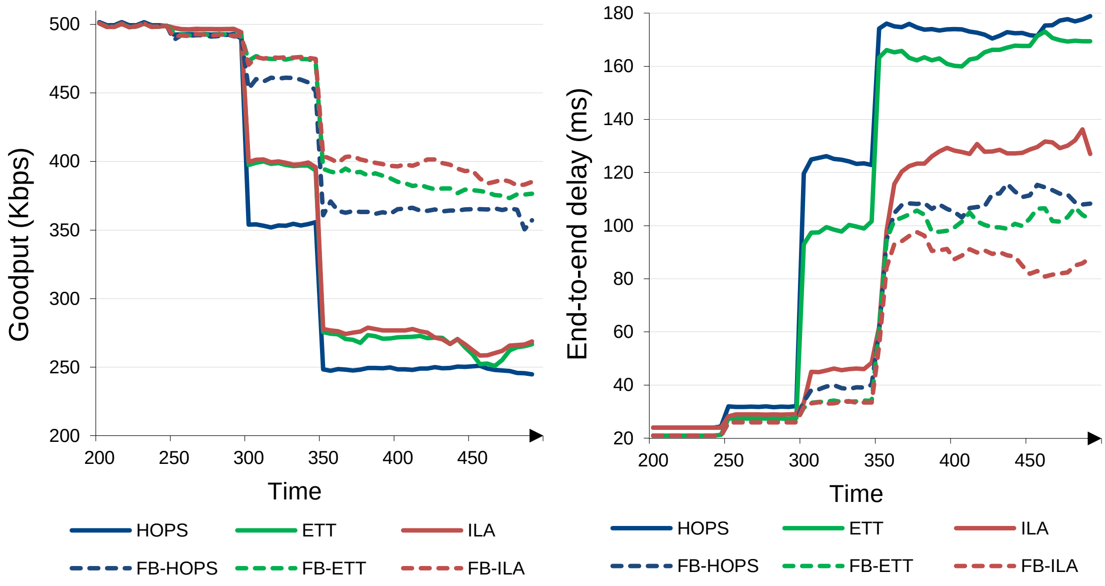


Fig. 4.5: RPDB usage in order to implement FB-AODV

The code of FB-AODV for Linux-based platforms is publicly available under GPL license [134] and has been successfully ported to Android-based mobile phones [62][63].

4.3.1.2 Performance analysis

Fig. 4.6 compares the performance of destination-based and flow-based routing for different state-of-the-art routing metrics. Results are based on a simulated grid scenario which comprehends 64 stationary single-radio nodes, as detailed in Section 2.2.3.3 (Fig. 2.14 and Table 2.9). Four flows are initiated between nodes 1 and 64 (the upper left and bottom right end nodes of the network, respectively), which are separated by a minimum of 14 hops. In the case of the classic AODV routing procedure based on destinations, the first flow creates a path which is followed by all the later flows. In the case of FB-AODV, different ToS are used in order to allow each flow to search for a particular route. The first flow starts at the second 200 of the simulation, and every 50 seconds a new flow starts. The duration of the simulations is 500 seconds. Packets have a size of 1472 bytes and are sent with a constant rate of 500 kbps. Results are obtained as the average values from 100 simulations for each routing option. Fig. 4.6 shows the average goodput and end-to-end delay per active flow for classic AODV and FB-AODV for the three routing metrics considered, HOPS, ETT and ILA, which are aware of the hop-count, the link-quality and the load, respectively.



a) Goodput per flow: AODV vs FB-AODV   b) Delay per flow: AODV vs FB-AODV

Fig. 4.6: Comparison of AODV vs FB-AODV in a single-radio scenario: Goodput (a) and End-to-end delay (b)

As shown in Fig. 4.6, using classic AODV, the activation of the third and fourth flows (at seconds 300 and 350) significantly degrades the goodput and the delay per flow due to severe congestion and link breaks. However, using FB-AODV (see the corresponding results labeled FB-) the first three flows lead to a minor degradation, while the fourth causes less degradation than classic AODV. Note that even when using FB-AODV, the fourth flow leads to significant degradation, since there is an unavoidable bottleneck in the destination neighborhood. Nevertheless, FB-AODV improves classic AODV goodput by up to 45%, while delay is reduced by up to 65%. Also, the number of link failures of the network, which in this stationary scenario are caused by the high levels of traffic interference, is reduced by up to 55%.

The performance improvement of FB-AODV for ILA, which is a load-aware metric, was expected, since FB-AODV allows load-balancing in the network. However, results show that FB-AODV benefits load-unaware metrics like ETT or HOPS to a similar degree. Since the ETT metric is aware of the link error rate, some links that become congested by the first flows are avoided in the route creation of the later ones. This result is consistent with aforementioned studies which analyze the variation of ETX/ETT metric values due to collisions caused by traffic interference [129][130][131]. On the other hand, the HOPS metric leads to load-balancing by chance: since in this scenario there are many possible routes with the same minimum number of hops, the probability of discovering different routes for each flow is high. Also, during route creation procedure, RREQ messages traversing congested zones are more likely to be lost or to arrive later.

Fig 37 shows the benefits of FB-AODV in a multi-radio scenario. As the previous one, the scenario consists on a stationary grid of 64 nodes. However, in this case four flows of 1 Mbps are initiated between nodes 24 and 31, which are separated by eight hops, and the number of interfaces and orthogonal channels is increased. The Channel Assignment Algorithm is the Common Channel Set (CCS); i.e. each interface is assigned to a fixed channel and all nodes share the same set of channels. First, as occurred in the previous scenario, results show that in the single-radio case FB-AODV outperforms AODV for both analyzed routing metrics, although both being load-unaware.

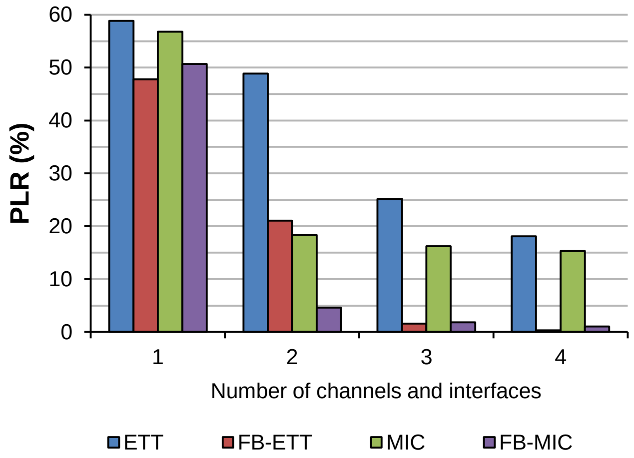


Fig. 4.7: Packet Loss Rate of AODV and FB-AODV in a multi-radio scenario

In multi-radio cases, MIC obtains better performance than ETT since it is aware of channel distribution in order to minimize intra-flow interference (by using the CSC parameter defined in Equation 4.8). However, using FB-AODV, the performance of FB-ETT is similar (2 channels) or even better (3 and 4 channels) than the performance of MIC. This fact confirms that using FB-AODV intra-flow interference awareness is less significant since destination-based routes are discomposed in different flow-based routes, which are then seen as inter-flow interference. Thus, FB-AODV also benefits MIC, since it increases the chance of discovering alternate routes which use less interfered links or channels.

In conclusion, results demonstrate the benefits of a flow-based routing approach, not only in the case of load-aware routing metrics, which was the main objective of this enhancement, but also for load-unaware ones.

4.3.2 Weighted Contention and Interference routing Metric

4.3.2.1 Design and implementation

The objective of the Weighted Contention and Interference routing Metric (WCIM) is to select paths according to: i) the flow characteristics, ii) the quality of the WMN links, iii) the contention in transmission and iv) the interference in reception. WCIM aims to include all of these factors in an accurate yet simple way, taking into account the conclusions of the performance analysis described in Chapter 3.

The parameter describing the load of a node must increase with the sending rate of the active flows of that node. In addition, as introduced in previous sections, in order to weight the channel occupancy, the capabilities of the link being used by the flow must be considered. Traffic routed through a slow link captures the channel for a long time in each transmission attempt. Likewise, links with a high error ratio lead to a high number of retransmissions and channel consumption. Therefore, CF^{ij}_k is defined as the percentage of channel occupied by the k-th flow when routed by node i to next-hop j as follows:

$$CF^{ij}{}_k = \frac{FR_k}{BW_{ij,k}} \tag{4.23}$$

where FR_k defines the sending rate of the k-th flow and $BW_{ij,k}$ denotes the bandwidth of link ij for the k-th flow. The bandwidth of a link is computed as shown in Equation (4.24):

$$BW_{ij,k} = \frac{LR_{ij}}{\alpha_{ij,k} \times ETX_{ij}} \tag{4.24}$$

where the nominal link bit rate LR_{ij} (e.g. 6 Mbps, 12 Mbps, etc.) is divided by the ETX metric of the link [59], ETX_{ij}, and by the parameter $\alpha_{ij,k}$. This coefficient reflects the efficiency of the nominal link bit rate LR_{ij} in relation to the average packet size P_k (in bytes) of the k-th flow, as shown in Equation (4.25)

$$a_{ij,k} = \frac{O + (P_k + O_h) \times 8 / LR_{ij}}{P_k \times 8 / LR_{ij}} \tag{4.25}$$

where O_h is the MAC header in bytes and O denotes the rest of the MAC and PHY layers overhead (i.e. the preamble transmission, DIFS, SIFS, ACK transmission, etc.) in time units. Other routing metrics like ALM (see Equation (4.3)) [2] or MTM [118][119] use an equivalent methodology in order to estimate the expected transmission time of a packet.

In short, Equation (4.23) provides the portion of actual link bandwidth or channel time consumed by the *k*-th flow of node *i*. Next, the percentage of channel occupied by node *i*, CN^i, is defined as the sum of the channel occupancy of all its NF^i active flows, as shown in Equation (4.26). Thus, this parameter provides the total portion of channel time consumed by node *i*.

$$CN^i = \sum_{\substack{k=1 \\ j \in N_1^i}}^{NF^i} CF^{ij}{}_k \quad (4.26)$$

Once defined the channel occupancy of a node, next step is to use this parameter in order to estimate the contention and interference level of a link. As analyzed in Section 3.2.2, contending nodes can be modeled as the one-hop neighborhood of the transmitter; Hello messages are broadcasted at the minimum transmission bit rate as is the case of the preambles used by the PD mechanism of 802.11 in order to sense the medium [2][36]. Using this model, the Contention Level, CL_i, of a node *i* is defined as follows:

$$CL_i = CN^i + \sum_{\forall m \in N^i{}_1} CN^m \quad (4.27)$$

where CN^i is the portion of channel time consumed by node *i* (i.e. the transmitter) as defined in Equation (4.26) and the summation includes the portion of channel time consumed by the one-hop neighbors, denoted by $N^i{}_1$, of node *i*. Hence, CL_j gives the contention level in the carrier sensing range or one-hop neighborhood of node *i*, where a value of 0 represents a free transmission channel and a value of 1 (or greater) represents a totally occupied transmission channel.

Interference in reception is difficult to model at the network layer, since it depends on several physical parameters and phenomena. As reviewed in Section 4.2, state-of-the-art routing metrics usually approximate the interference range as the one-hop or two-hop neighborhood of the receiver. WCIM is based on this approximation, but, according to the conclusions of Section 3.2.3, different weights are given to the channel occupancy of the interfering nodes according to their relative position regarding the sender and the receiver.

Thus, the Interference Level, IL_{ij}, of a link *ij* is defined as follows:

$$IL_{ij} = \sum_{\forall m \in (N^j{}_1 \setminus N^i{}_1)} 2 \times CN^m + \sum_{\forall m \in (N^j{}_2 \setminus N^i{}_1)} \frac{1}{2} \times CN^m \quad (4.28)$$

The first summation considers the interference caused by the hidden nodes for the transmitter *i*, that is, the one-hop neighbors of the receiver *j* which are not one-hop neighbors of the transmitter *i*. Due to packet collisions and retransmissions, the interfered link perceives an inflated channel occupancy with respect to the real channel usage of hidden nodes. According to the results shown in Section 3.2.3, an inflation factor of around 2 seems adequate to model the significant impact on performance of hidden nodes.

The second summation takes into account the interference of the two-hop neighbors of the receiver *j* which are not one-hop neighbors of the transmitter *i*. The interference caused by two-hop neighbors strongly depends on the distance and the number of interfering nodes. As pointed out in Section 3.2.3, while a two-hop neighbor that is very close to the receiver can impact the channel occupancy in a way similar to a hidden node, further nodes may have no impact at all on performance. Intuitively, in most situations the impact on performance of these nodes would be lower than the impact of hidden nodes and contending nodes in transmission. Hence, as shown in the second summation, the channel load of two-hop neighbors is weighted by one half[1].

Then, a node *j* computes the WCIM metric of the *k*-th flow traversing link *ij*, denoted by $WCIM_{ij,k}$, as follows:

$$WCIM_{ij,k} = \frac{P_k}{BW_{ij,k} \times (1 - CL_i - IL_{ij})} \tag{4.29}$$

where P_k is the average packet size of the *k*-th flow of link *ij*, $BW_{ij,k}$ is the bandwidth of the link *ij* for the *k*-th flow, CL_i represents the contention level in transmission for node *i* and IL_{ij} is the interference level in reception for link *ij*. Both CL_{ij} and IL_{ij} are defined as a percentage of channel time and their sum should not exceed 1. The denominator of $WCIM_{ij,k,}$ represents the available bandwidth of link *ij* for the *k*-th flow of that link. Thus, $WCIM_{ij,k,}$ can be regarded as an estimation of the delay for transmitting a packet of size P_k through link *ij*.

Fig. 4.8 illustrates an example of the nodes that contend with the transmitter *i*, the nodes that interfere the receiver *j*, and the weights assigned to each node to calculate the contention and interference levels of the link *ij*. In the case of multi-radio environments, the metric only considers

[1] During the realization of this thesis other values were analyzed (e.g. 0, 0.25, 0.75 and 1) in order to weight the load of two-hop interferers, obtaining in most cases the best results for the 0.5 case. Nevertheless, it can be considered a tunable parameter dependent on the network topology.

the contention and interference levels of the nodes which are transmitting in the same channel as the link *ij*.

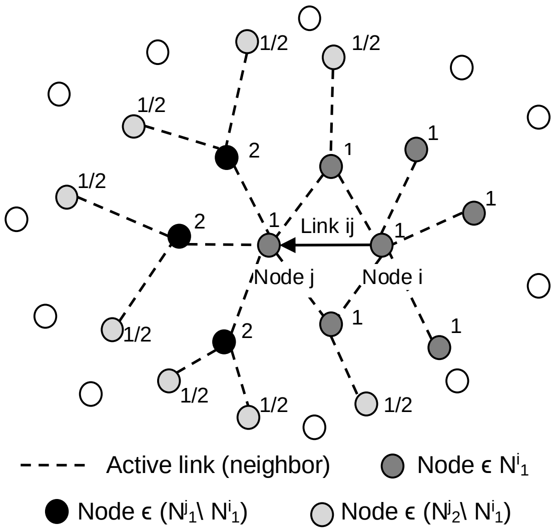


Fig. 4.8: Example of WCIMs channel occupancy algorithm. The one hop neighbors of the transmitter i are weighted by 1, the hidden nodes of link ij by 2 and two-hop neighbors of the receiver j by ½.

Finally, the metric of a path *p* for a flow *k*, denoted by *WCIM(p, k)*, is defined as the sum of all the link costs of the path.

$$WCIM(p,k) = \sum_{\forall ij \in p} WCIM_{ij,k} \tag{4.30}$$

Finally, the following points discuss different requirements and characteristics of WCIM:

- WCIM should be integrated with a flow-based routing protocol as FB-AODV to assure an optimal computation and maintenance of paths and an efficient load-balancing.
- WCIM is isotonic and monotonic. Intra-flow interference was not considered in its design in order to avoid its associated problems. Nevertheless, as pointed out in previous sections, flow-based routing reduces the importance of intra-flow interference awareness during route creation.
- In order to obtain a valid metric as defined by Equation (4.29), the sum of the contention and interference levels of a link should be lower than 1.The contrary implies that the channel is overloaded and, thus, the node should avoid being part of a new route. In such a case, two different routing strategies can be followed. First, the node can discard the RREQ message due to insufficient resources, performing similar to the admission control mechanisms used for QoS assurance in MIWNs [107]. On the other hand, the node can forward the RREQ but applying a penalty to the routing metric (e.g. giving a value

several orders of magnitude over the usual one) in order to discourage the selection of this route.

- The sending rate FR_k and packet size P_k of a flow can be obtained, for instance, by encoding them in the ToS field of the flow (e.g. the average rate and packet size defined by the application type) or by passively scanning the transmitted packets at the routing protocol (using the fact that route lifetimes should be updated with each forwarded packet).
- Each node periodically collects information about the quality of the links to its neighbors in order to compute the bandwidth of link as per Equation (4.24). By default, the loss rate of the links, ETX, is computed using the Hello-based estimation usually proposed for ETX metric implementations [59]. On the other hand, the nominal link bit rate, LR, is obtained by using the packet-pair technique proposed for the ETT metric computation [43]. Nevertheless, other estimation procedures, like passive scanning or the utilization PHY/MAC statistics, can be used if available.
- The computation of ETX as defined in [59] requires each node to add extra information in the Hello messages (i.e. IP address and loss rate estimation of each neighbor). Hence, using this information, a node can easily obtain the one- and two-hop neighbors of a link ij in N^i_1, $N^j_{1/}$ N^i_1 and $N^j_{2/}$ N^i_1 and reproduce the WCIM interference model as shown in Fig. 4.8. In addition, WCIM requires the load of the nodes and its neighbors to be included in Hello messages.

4.3.2.2 Performance analysis

In other to analyze the benefits of WCIM routing metric and compare it with other representative metrics presented in Section 4.2, two main analyses are performed. First, the capacity of routing metrics to estimate the performance or quality of the routes is evaluated; finding the best route according to a set of performance parameters requires that the routing metrics give values to routes based on the expected performance of such routes. Secondly, the performance of different scenarios according to the routing metric being used is studied.

The basic simulation scenario is based on the grid of 64 nodes detailed in Section 2.2.3.3 (see Fig. 2.14 and Table 2.9). The link bit rate of the nodes is randomly fixed at 6 Mbps or 12 Mbps. The main performance metrics utilized are the Packet Loss Rate (PLR), the goodput (i.e. number of bytes correctly received at the destination per time unit) and the average end-to-end delay of the flows. Simulated traffic is generally UDP, Constant Bit Rate and unidirectional. Since using UDP the sources of the flows simply send data packets in a constant rate, regardless of the network state, it permits a better analysis of routing metric performance without the impact of higher layer mechanisms, as is the case of the congestion control of TCP. Also, as mentioned in previous chapters, the usage of TCP in multi-hop networks can be problematic [75] [76]. In any case, a TCP scenario is analyzed in Section 4.3.2.2.2.

4.3.2.2.1 WCIM as performance estimator

Routing metrics are designed in order to characterize phenomena which affect traffic performance. The way routing metric values vary with performance variations determines the capacity of the routing metrics to find the optimal route for a specific flow. This section analyzes whether HOPS, ETT, ILA and WCIM metrics reflect end-to-end delay, which is the reference performance parameter for these metrics.

Three types of CBR UDP flows with random source and destination are defined to be routed: *f1* (sending rate of 500 kbps, packet size of 1472 bytes), *f2* (200 kbps, 972 bytes) and *f3* (50 kbps, 172 bytes). The evaluation is carried out under three different initial load and interference conditions depending on the number of flows (zero, one or two flows) routed in the network. Then, another flow, which is the flow under analysis, is started and routed. For this flow and for each simulation, a pair of values for each considered routing metric is obtained: the routing metric value, which is computed during the route discovery phase, and its average end-to-end delay. The duration of the flow under analysis is 200 seconds and 250 different simulations for each type of flow (i.e. *f1*, *f2* and *f3*) are analyzed. The following figures plot this pair of values for each simulation. For a better comparison of the relationship between routing metric and end-to-end delay values, the pairs are ordered in the horizontal axis by the routing metric value (from minimum to maximum value).

Fig. 4.9 shows the results obtained for the HOPS metric. It can be easily seen that the number of hops of a path has an inaccurate relationship with its end-to-end delay. For instance, a route of 5 hops leads to very different delays depending on the bit rate of the links or the interference of other flows, or even to higher delays than a route of 8 hops. In conclusion, the hop count routing metric cannot find optimal paths in a reliable way. Results for *f2* and *f3* were similar.

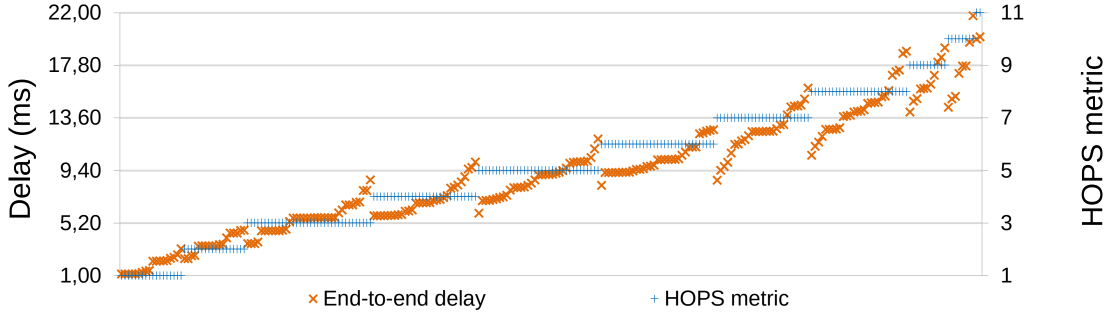


Fig. 4.9: Comparison of HOPS metric and end-to-end delay variations for the flow *f1*

Fig. 4.10 shows the same analysis for ETT metric. The performance of ETT metric as a delay estimator is better than the HOPS metric, due to its link-awareness. For instance, it can correctly characterize that a hop at 12 Mbps is usually faster than a hop at 6Mbps. However, since ETT does not consider the load and interference of the links, there are some cases where routes with the same or similar ETT metric lead to very different end-to-end delays.

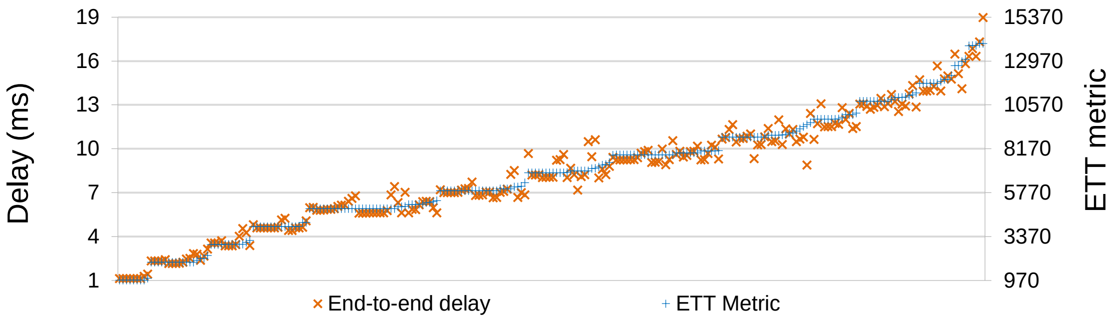


Fig. 4.10: Comparison of ETT metric and end-to-end delay variations for the flow *f1*

In addition, the ETT metric does not consider the influence of IEEE 802.11 physical and MAC overhead on performance, which is more significant in fast links than in slow ones. This is especially significant in the case of flows using small packet sizes, as is the case of *f3*, which is illustrated in Fig. 4.11.

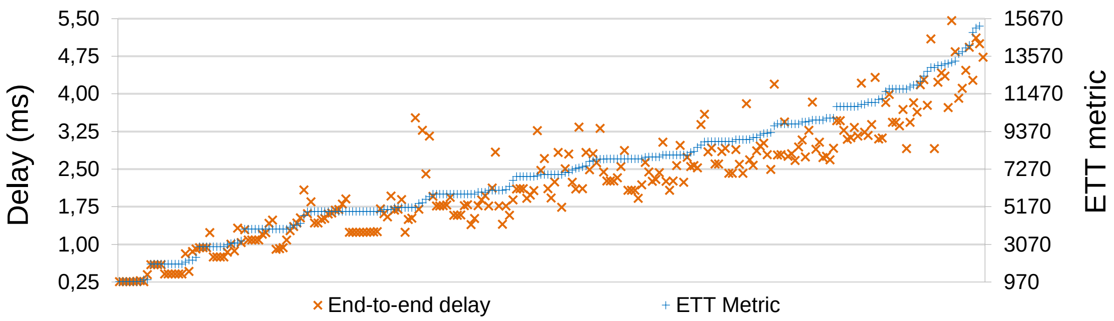


Fig. 4.11: Comparison of ETT metric and end-to-end delay variations for the flow *f3*

As shown in Fig. 4.12, the ILA metric behaves as a poor performance estimator. Two main regions can be seen in Fig. 4.12. The results on the left side of the figure correspond to routes free of interference. In such cases, ILA algorithm is equivalent to the ETT metric. In this region ILA accurately reflects the variations of the end-to-end delay, since in the absence of interference the end-to-end delay basically depends on link rates. However, results on the right side of Fig. 4.12 correspond to routes that include interfered links. For such routes, ILA is unable to reflect the real impact of interference on the performance of the routes and the metric values and end-to-end delay variations become completely disassociated. The main cause of this poor performance is the definition of the ILA metric itself. Since AIL_{ij}/AIL_{min} is always greater than 1, the MTI_{ij} parameter defined in Equation (4.15) grows very fast with interference.

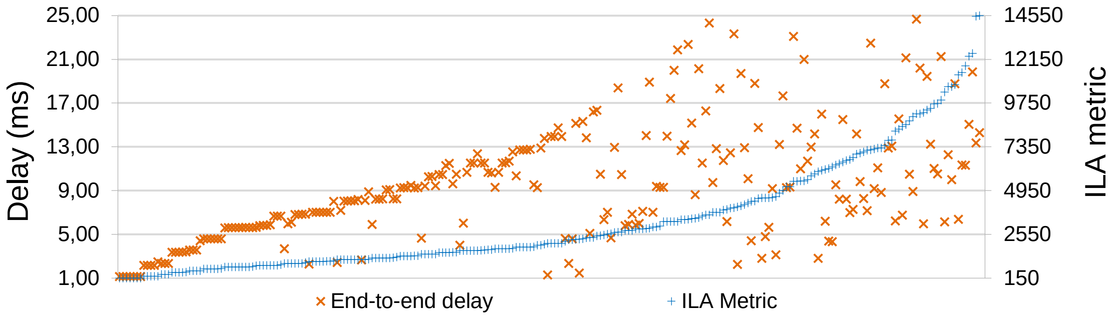


Fig. 4.12: Comparison of ILA metric and end-to-end delay variations for the flow *f1*

Finally, Fig. 4.13 shows the results of this analysis for the WCIM case. Since it considers in a more accurate way the different phenomena which affect the performance of the flows, WCIM clearly outperforms the other metrics. There are still some specific situations in which routes with a similar WCIM metric yield a different performance. The reasons for this behavior include inaccuracies in modeling interference or estimating ETX.

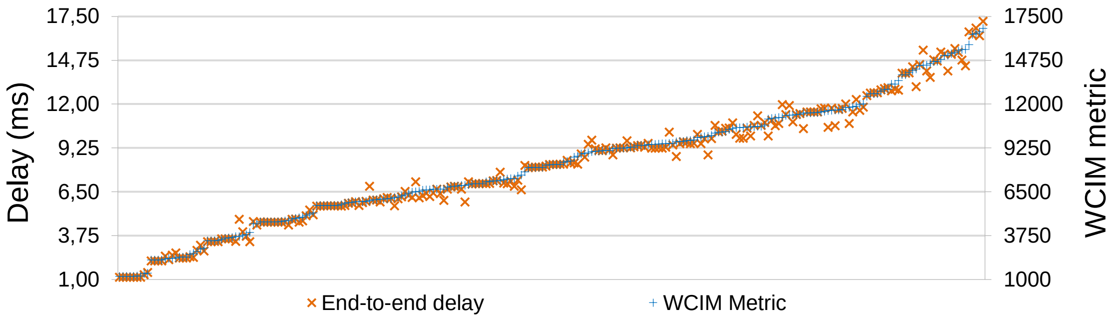


Fig. 4.13: Comparison of WCIM metric and end-to-end delay variations for the flow *f1*

As shown in Fig. 4.14, compared to ETT, WCIM also obtains better results for flows using small packets, since, in addition to interference, PHY and MAC overheads are considered.

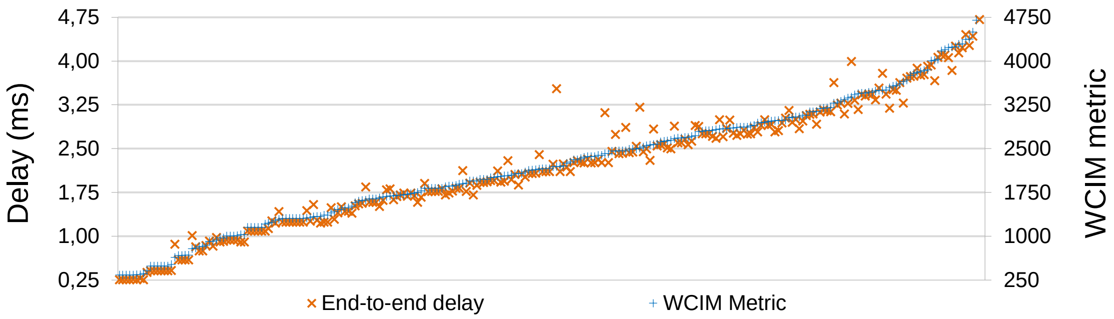


Fig. 4.14: Comparison of WCIM metric and end-to-end delay variations for the flow *f3*

Table 4.1 shows the normalized standard deviation of the ratio between the end-to-end delay and the routing metric value for each type of flow. This parameter is a measure of the ability of each routing metric to predict the performance of the routes in terms of delay (ideally, the ratio between end-to-end delay and routing metric value should be constant, and hence its standard deviation should be zero). The results obtained corroborate the previous analysis and show how WCIM has greater reliability as an end-to-end delay estimator than the rest of routing metrics considered.

Routing Metric	f1(large packets)	f2 (medium packets)	f3 (short packets)
HOPS	18%	20%	28%
ETT	7%	8%	19%
ILA	54%	61%	76%
WCIM	5%	5%	9%

Table 4.1: Standard deviation of delay/metric ratio (expressed as a percentage of the average)

For long packets, except in cases of heavy congestion or interference, the main factors affecting delay are the link bit rates and the number of hops of a path. Thus, ETT results are in average similar to those for WCIM. However, in the case of short packets, the link transmission times are small. Thus, interference, congestion, and also link efficiency, affect the total end-to-end delay more significantly. Since WCIM considers all these parameters, it significantly outperforms ETT results for short-packet flows.

In conclusion, assuming that the path cost using WCIM routing metric expresses the end-to-end delay for the packets of a flow in microseconds, WCIM can be considered as a reliable estimator of the average end-to-end delay for that flow through a given path. This is an interesting feature, for instance in order to route flows with delay requirements. As will be seen in next section, this feature benefits the capacity of WCIM to discover optimal paths and to improve the performance of the flows.

4.3.2.2.2 WCIM performance

This section presents an analysis of the performance of HOPS, ETT, MIC, ILA and WCIM routing metrics in seven different scenarios. Three basic types of CBR UDP flows are defined: *fl* (sending rate of 75 kbps, packet size of 1472 bytes), *fm* (50 kbps, 972 bytes) and *fs* (10 kbps, 172 bytes). Depending on the load configuration, the sending rate of the flows is multiplied. The objective of using different types of flows instead of a unique type, which is more common in MIWNs literature, is to take into account simultaneous flows with different characteristics in order to reflect better the variety of flows which may be present in a real network, and also to consider the impact of load and interference according to the different types of flows (either the interfering or the interfered ones).

For each scenario, the performance under different loads is analyzed in terms of the PLR and the average end-to-end delay during the time interval in which all the flows are active. Results are the average of 100 simulations changing the different seeds of the simulator. Table 4.2 summarizes the main simulation parameters and characteristics of the seven scenarios.

	Scenario 1	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**	**Scenario 6**	**Scenario 7**
Node location	Grid	Grid	Grid	Grid	Random	Random	Grid
Multi-radio	No	No	No	No	No	No	Yes
Number of flows	6	6	6	15	6	15	6
Sources	Random	Random	Random	Random	Random	Random	Random
Destinations	Random	Fixed: GW64	Fixed: GW28	Random	Random	Random	Random
Flow duration	200 s	200 s	200 s	300 s	200 s	300 s	200 s
Simulation time	450 s	450 s	450 s	550 s	450 s	550 s	450 s
Analyzed interval	250 s - 400 s	250 s - 400 s	250 s – 400 s	250 s – 400 s	250 s – 400 s	250 s – 400 s	250 s - 400 s
Load configurations	10	8	6	5	10	5	1
Minimum load	270 kbps	270 kbps	270 kbps	675 kbps	270 kbps	675 kbps	---
Maximum load	2700 kbps	2160 kbps	1620 kbps	3375 kbps	2700 kbps	3375 kbps	2700 kbps

Table 4.2: WCIM performance evaluation: Simulated scenarios

The 95% confidence interval of each PLR result was computed. These intervals were under 2%-3% in most cases regardless of the routing metric. Thus, for the sake of illustration clarity, confidence intervals of the results are not included in the corresponding figures.

Scenario 1

Scenario 1 consists of six active flows with random source and destination. First, in order to better characterize the route decisions performed by the different routing metrics, a specific simulation of the fifth configuration (offered load of 1350 kbps) is analyzed in detail. Fig. 4.15 illustrates the route selections performed by HOPS, ETT, ILA and WCIM metrics, while PLR and delay results are resumed in Fig. 4.16. Flows are numbered according to their initialization time; *f1* and *f5* are of type *fl*, *f2* and *f4* of type *fm* and f3 and f6 of type *fs*.

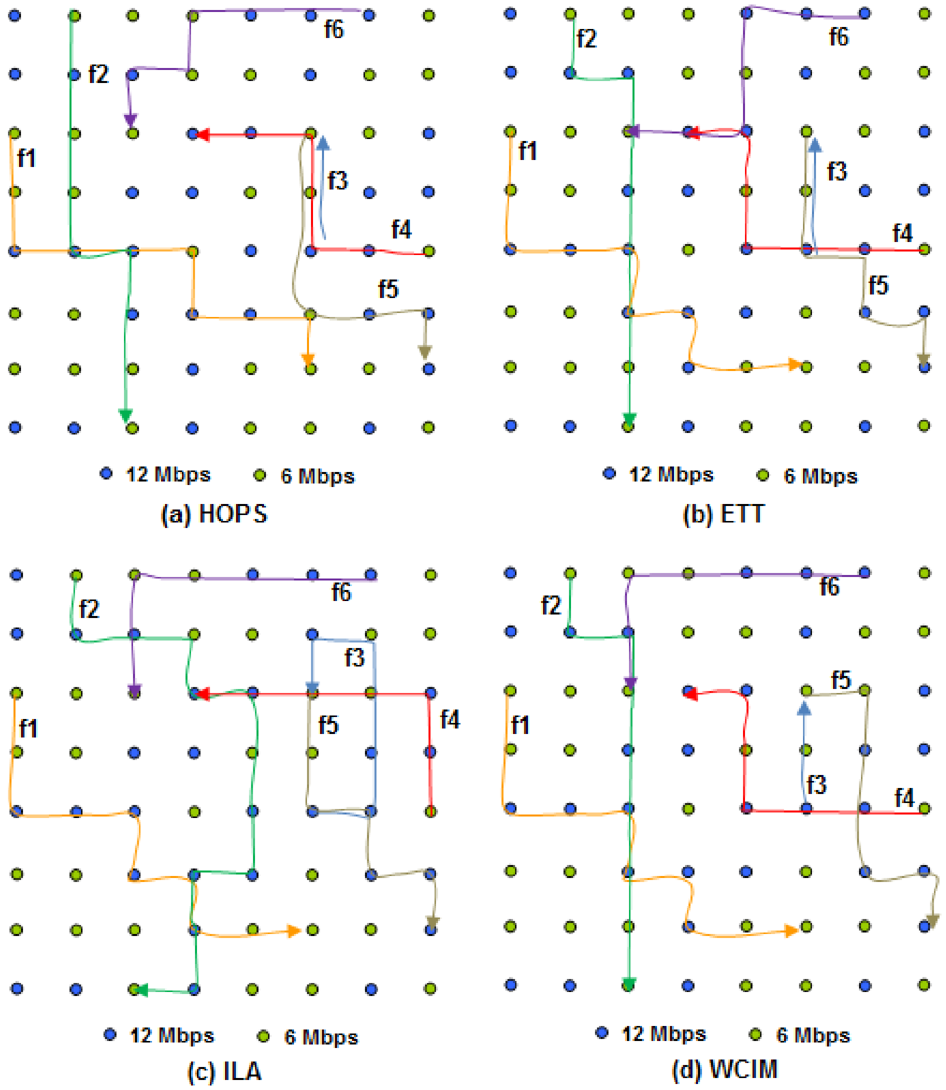


Fig. 4.15: Scenario 1, analysis of path discovery. (a) HOPS, (b) ETT, (c) ILA and (d) WCIM.

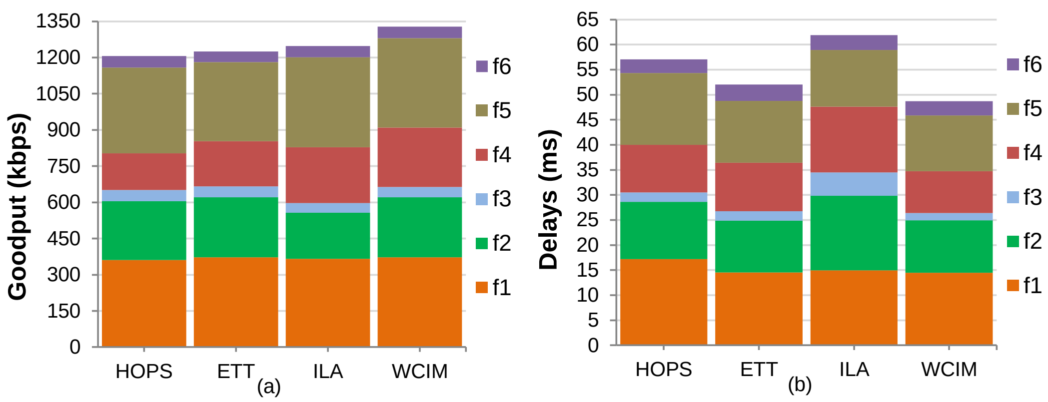


Fig. 4.16: Scenario 1, analysis of a specific simulation. (a) PLR and (b) Delay.

Regarding the paths created for *f1*, the first flow of the simulation, due to its link-quality unawareness, HOPS metric selects a higher number of links at 6 Mbps, thus leading to a higher delay than the rest of the routing metrics. In the case of *f2*, HOPS also uses a slower route than

ETT. On the other hand, ILA tries to avoid the interference of *f1*, leading to a very long route, which in fact degrades its performance. WCIM, on the contrary, determines that the interference of *f1* is not significant and selects the same path as ETT. In fact, note that the first four flows are routed identically by ETT and WCIM metrics, since interference and congestion remain low. Regarding *f3*, ILA again creates an inefficient route trying to avoid the interference of *f2*, while the other metrics select the same path of two hops. Finally, the routing of *f5* and *f6* illustrate the differences between ETT and WCIM; WCIM uses alternative routes which are more distant from *f3* and *f4* in order to avoid interference, leading to better results as pointed out in Fig. 4.16.

Once the different route strategies of the metrics have been analyzed, which are consistent with the Equations presented in Section 4.2, Fig. 4.17 shows the general results for this scenario in terms of PLR and average end-to-end delay (sum of the average delay of all the six flows) according to the load of the different configurations.

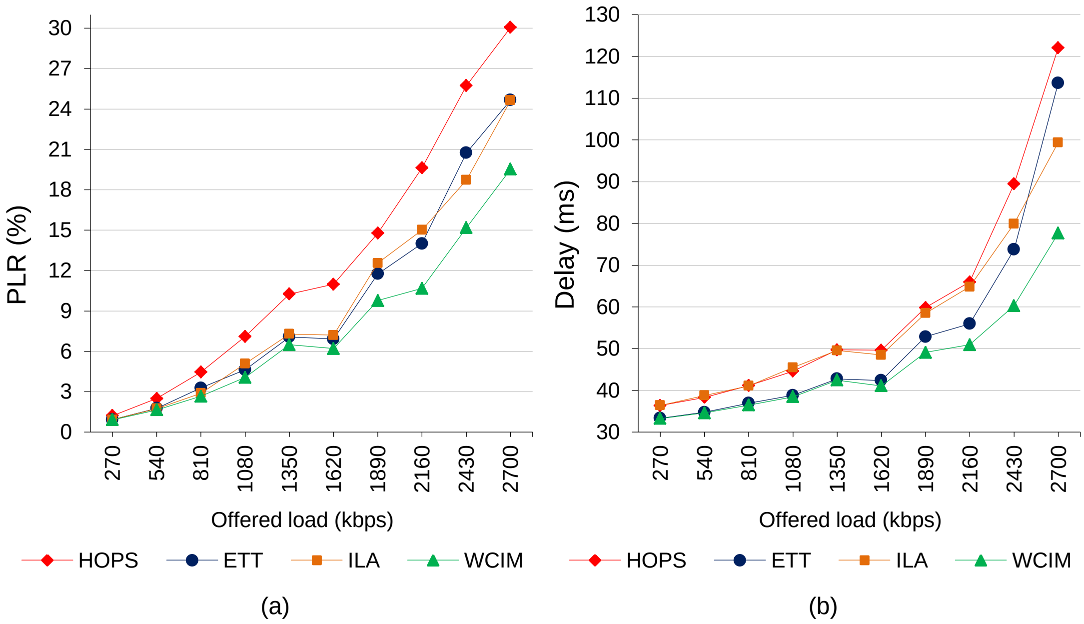


Fig. 4.17: Scenario 1 main results. a) Packet Loss Rate and b) End-to-end delay

As expected, results show that the HOPS metric always gives the worst performance. Under low load conditions, the HOPS metric leads to high delays, since it selects a higher number of links at 6 Mbps than the other metrics. The packet loss rate in these configurations is also high, since these slow links become congested and occupy more channel time, leading to a higher interference level. Thus, HOPS performance degrades significantly with the increase of the load. On the other hand, ETT selects links at 12 Mbps whenever possible, thus obtaining good results with low load conditions both in PLR and delay. However, since ETT is interference- and load-unaware, these faster links also become congested and interfered with the increase of load conditions.

Results show that ILA only outperforms ETT performance under very high load conditions. As mentioned in the previous section, ILA overestimates inter-flow interference leading to longer routes in order to avoid it, as shown in Fig. 4.18a. Thus ILA obtains a similar or better performance per hop than ETT, as illustrated in Fig. 4.18b, but a worse total performance due to its higher number of hops. Indeed, the delay performance of ILA under low load conditions is comparable to that obtained by using HOPS metric.

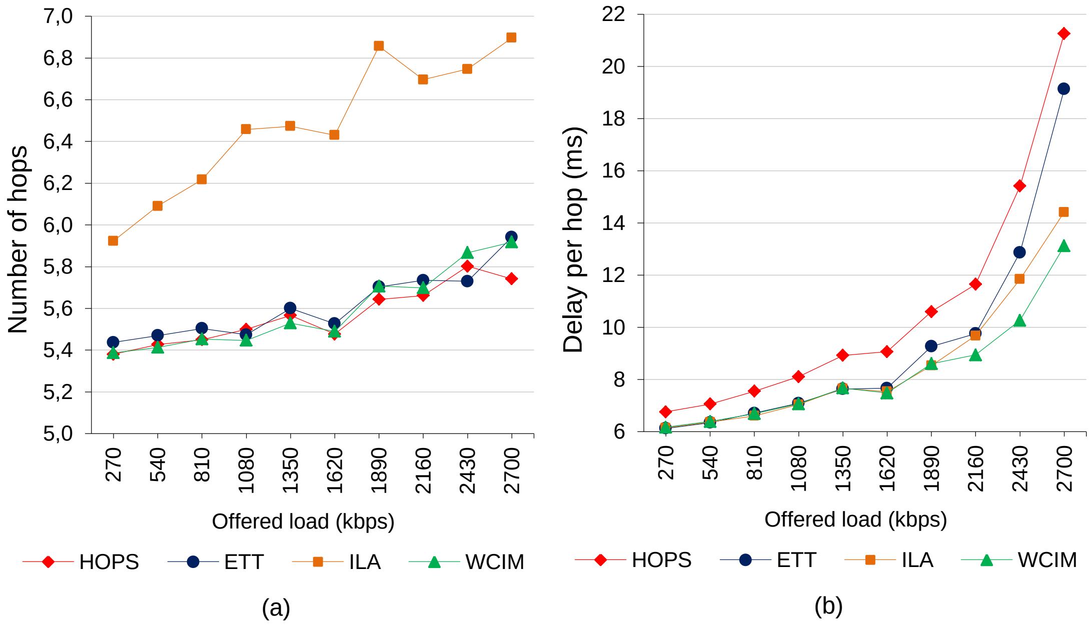


Fig. 4.18: Scenario 1 main results. a) Average number of hops per route and b) end-to-end delay per hop

Finally, Fig. 4.17 shows that the WCIM metric outperforms the rest of metrics in all load conditions, both in PLR and delay. In low load conditions, WCIM's routing strategy is similar to ETT, thus selecting routes through fast links. Under high load, WCIM balances the load in order to avoid highly interfered or congested links. As illustrated in Fig. 4.18, in contrast to ILA, WCIM gives a good performance without increasing the length of the routes. This is a desirable property for WMNs, since shorter routes are in general more robust to link breaks and require fewer transmissions.

Scenario 2

In this second scenario, a network where a node acts as a gateway to the Internet is analyzed. Six active flows with a random source are routed again, but this time with a common fixed destination (the node at the bottom right end of the network, denoted as GW64 in Fig. 2.14). Fig. 4.19 shows the results for this scenario.

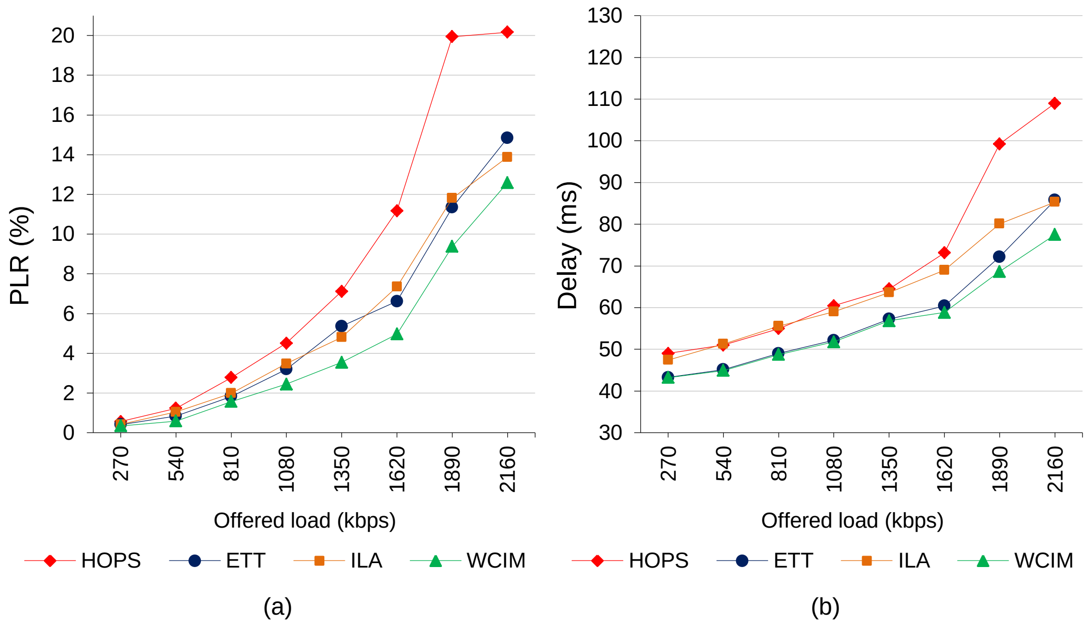


Fig. 4.19: Scenario 2 main results. a) Packet Loss Rate and b) End-to-end delay

The HOPS metric again gives the worst results in both PLR and delay due to its frequent use of slow and congested links. ETT and ILA results have a very similar PLR, even with the use of two very different routing strategies, as explained in the previous section. However, these differences become noticeable when comparing the delay performance, since ILA's longer routes lead to higher delays. As in the previous scenario, under low load conditions, the short and fast routes formed by ETT are more appropriate than the longer routes used by ILA, since link congestion remain low. In addition, in this scenario there is a bottleneck in the neighborhood of the common destination. Thus, ILA's routing strategy is also less effective under high load conditions, since there is no way of avoiding this bottleneck, which is the major source of interference and congestion in the network. Finally, once again, WCIM gives the best performance, improving ETT results by adding load-awareness, but without overestimating the effect of interference as in the case of ILA.

Scenario 3

The third scenario is very similar to the second one, but in this case the gateway is placed in the middle of the grid (GW28 in Fig. 2.14). Thus, the average length of the routes becomes shorter (from an average of 7-8 hops in scenario 2 to an average of 4-5 hops in scenario 3). This fact drastically reduces the number of alternative routes that could be used by metrics like ILA and WCIM in order to apply load- or interference-balancing. Furthermore, congestion in the neighborhood of the destination is increased. Fig. 4.20 summarizes the results for this scenario.

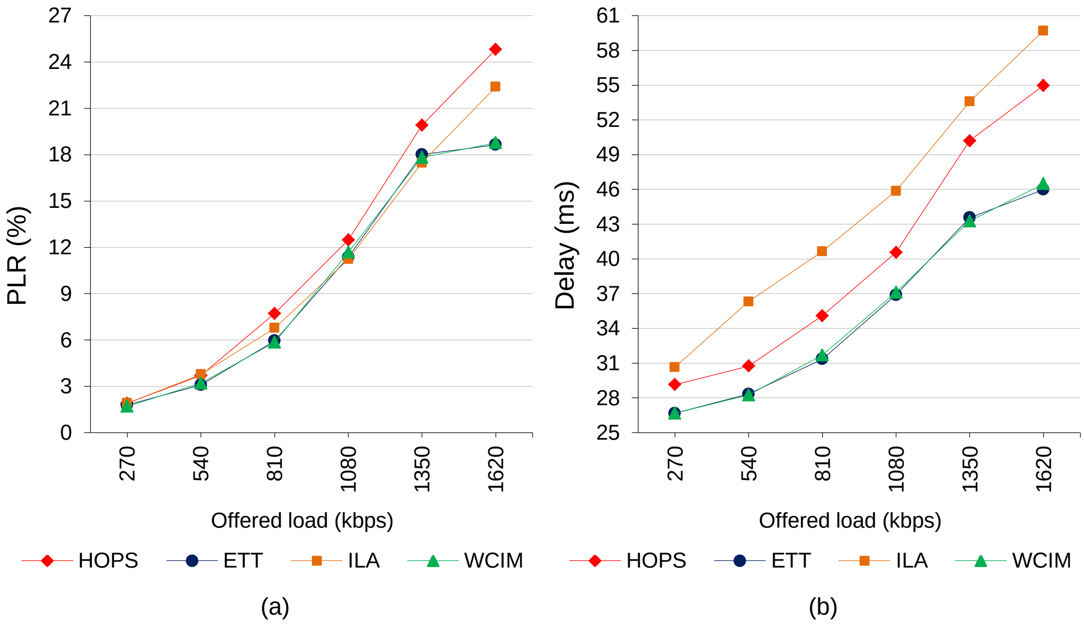


Fig. 4.20: Scenario 3 main results. a) Packet Loss Rate and b) End-to-end delay

As previously remarked, the short length of the routes and the unavoidable interference in the neighborhood of the destination leave little margin for using different routing strategies in order to improve the PLR of the traffic. In some cases, even the HOPS metric yields only a slightly worse PLR performance. On the other hand, the delay performance of the four metrics shows some appreciable differences. ILA performance becomes even worse than HOPS performance, since in this scenario longer routes become totally inefficient. Indeed, the similar performance of ETT and WCIM metrics means that in such a scenario the best routing strategy consists simply in creating routes through the faster links, since interference in the neighborhood of the gateway cannot be avoided.

Scenario 4

As in the first scenario, the fourth scenario is again based on random destinations, but this time analyzing the performance of 15 active flows, i.e. 5 flows of each defined type *fl*, *fm* and *fs*. Since the network quickly becomes congested, only 5 load configurations are analyzed. Fig. 4.21 illustrates the results of this scenario.

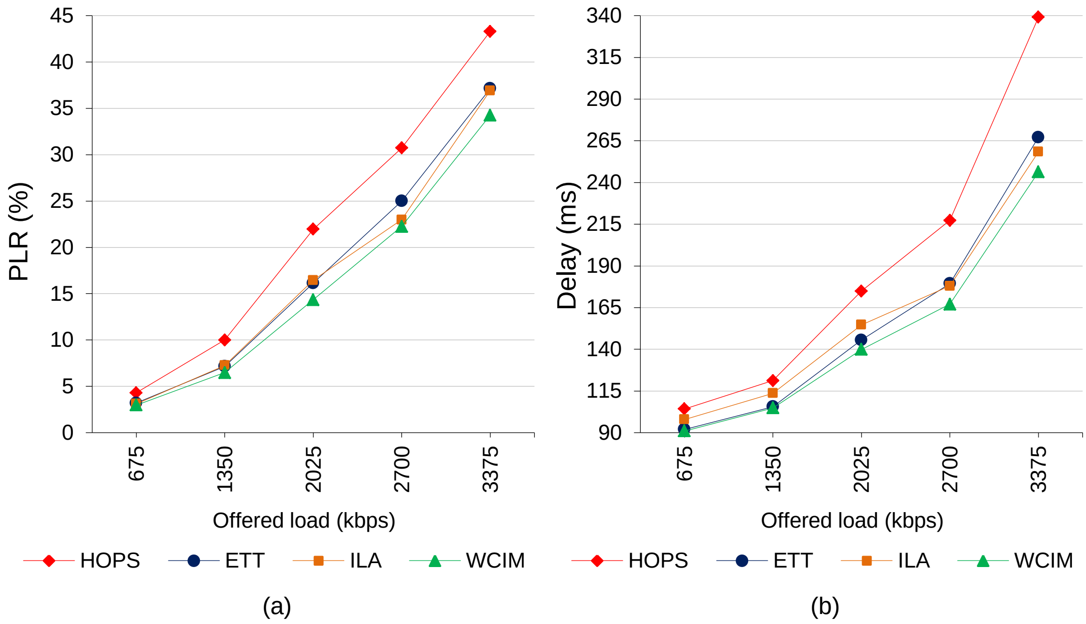


Fig. 4.21: Scenario 4 main results. a) Packet Loss Rate and b) End-to-end delay

Results are similar to those obtained in previous cases. The HOPS metric gives the worst performance, especially under high load conditions, while the other three metrics yield significantly better performance. ETT outperform ILA under low load conditions, mainly in delay measurements. However, ILA gives slightly better results with the increase of load. Indeed, ILA is more efficient than in the previous scenarios, since the characteristics of this scenario (i.e. random destinations and medium to high congestion) favor its routing strategy based on interference avoidance. Finally, WCIM again yields the best performance both in PLR and delay, outperforming the rest of the routing metrics.

Scenario 5

Scenario 5 is based on the same traffic parameters defined in the first scenario (i.e. six random flows and ten load configurations), but in this case the nodes are located in the 980 m x 980 m area using a uniform random distribution. Since the number of neighbors is variable and sometimes scarce, the number of alternative routes that could be used by the different metrics also becomes limited. Thus, network congestion dramatically increases with offered load. The average results for this scenario are illustrated in Fig. 4.22.

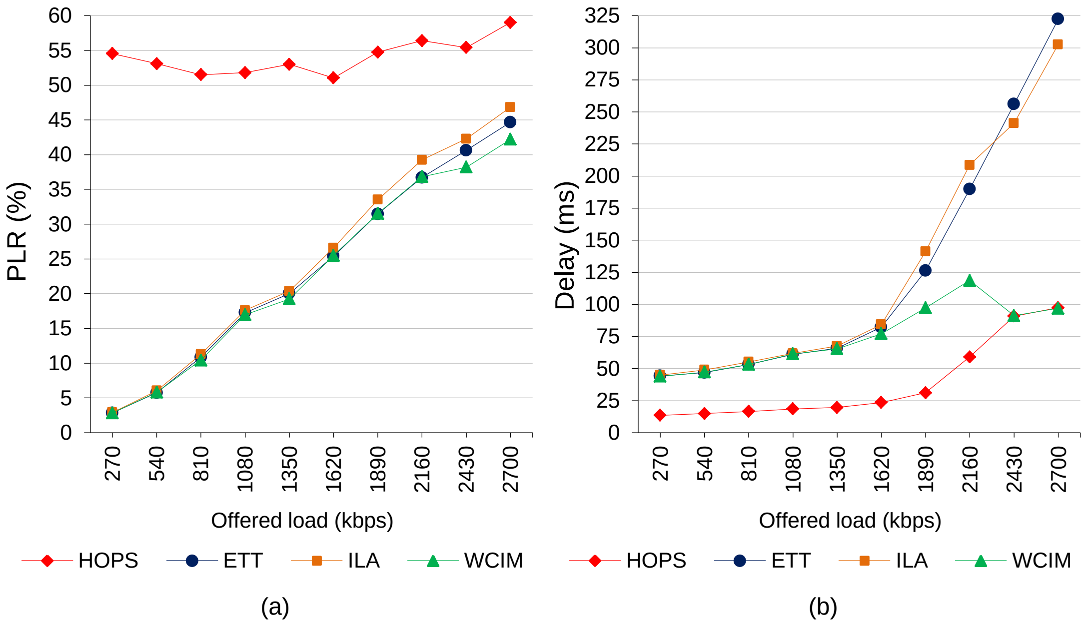


Fig. 4.22: Scenario 5 main results. a) Packet Loss Rate and b) End-to-end delay

Results show that HOPS yields a very different performance compared to the other metrics. Since neighbor discovery is based on HELLO messages, which are broadcast at 6 Mbps, unicast communication between neighbors is not always possible (recall that unicast link rates are randomly fixed at 6 Mbps or 12 Mbps). Thus, the use of HOPS involves some forward routes which are created by the broadcast flooding of RREQ messages; however, the corresponding backward routes cannot be successfully built since RREP messages are unicast. This issue is known as the Communications Gray Zone problem and was introduced in Section 3.1.2. The other metrics do not suffer from this problem, since in order to discover the link rates they implement the packet-pair technique, which is based on periodical unicast signaling between neighbors. Hence, these metrics discard RREQ messages during route discovery if unicast communication with the RREQ sender is not possible. For this reason, HOPS yields a PLR between 50% and 60% of the theoretical offered load throughout all the simulations. On the other hand, the end-to-end delay of HOPS remains low, since the network is less congested (as shown in Fig. 4.23a) due to the routes which cannot be created.

While ETT, ALM and ILA metrics obtain similar results in this scenario, Fig. 4.22b shows that WCIM yields low end-to-end delay with the increase of offered load. As previously explained, this scenario becomes very congested due to the random location of the nodes. This means that in some cases WCIM does not find any feasible route for new flows, that is, there is no route whose nodes have a sum of contention and interference levels smaller than 1 as defined in Equation (4.29). As shown in Fig. 4.23a, with increasing load, this yields a lower percentage of traffic being sent. In consequence, WCIM controls the increase of the PLR of the active flows, as illustrated in Fig. 4.23b.

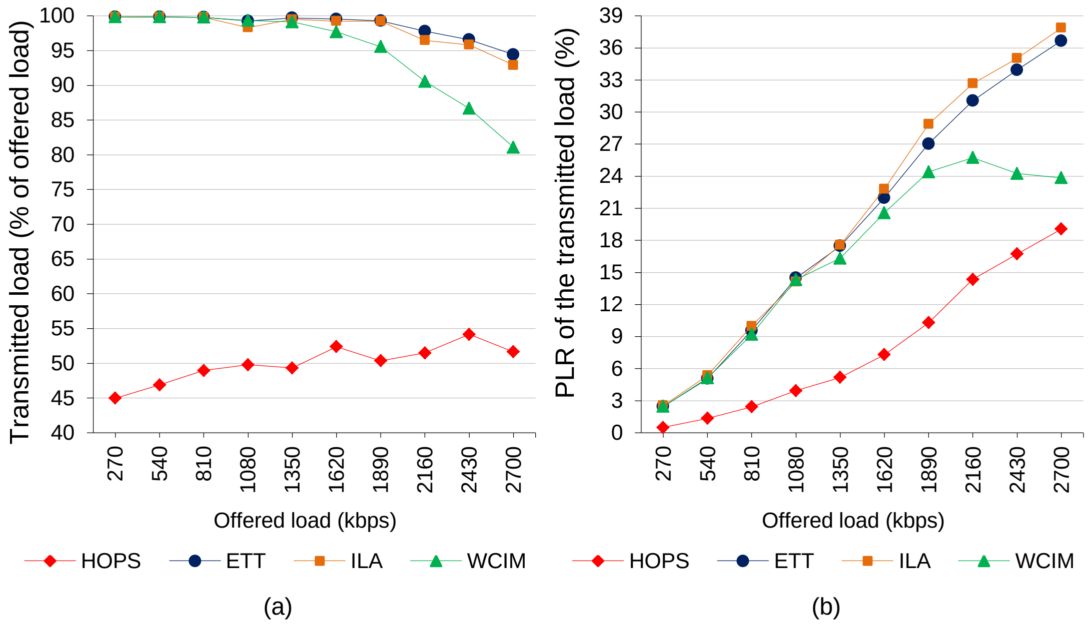


Fig. 4.23: Scenario 5 additional results. a) Transmitted load and b) Packet Loss Rate of transmitted load

In this way, unlike HOPS, the PLR of the total offered load of WCIM remains similar to ETT and ILA, and even outperforms them with load increase, as shown in Fig. 4.22a. In addition, this routing strategy clearly benefits the delay performance, as shown in Fig. 4.22b. This interesting feature of WCIM is similar to the admission control mechanisms used for QoS assurance in WMNs [107]. In Section 4.3.2.2.2 this characteristic of WCIM will be analyzed more in detail.

Scenario 6

Finally, the sixth scenario is also based on a random distribution of the nodes but now with the traffic parameters defined in the fourth scenario (15 random flows and 5 load configurations). Fig. 4.24 summarizes the results obtained.

As in the previous scenario, HOPS and WCIM obtain a differentiated performance as regards the other three metrics. Once again, HOPS transmits less than the 50% of the offered load through the network due to unavailable routes, thus obtaining a high PLR and a low end-to-end delay. On the other hand, while decreasing the sent load due to congestion detection, WCIM yields a similar and even better PLR than the other three metrics as well as a significantly lower end-to-end delay.

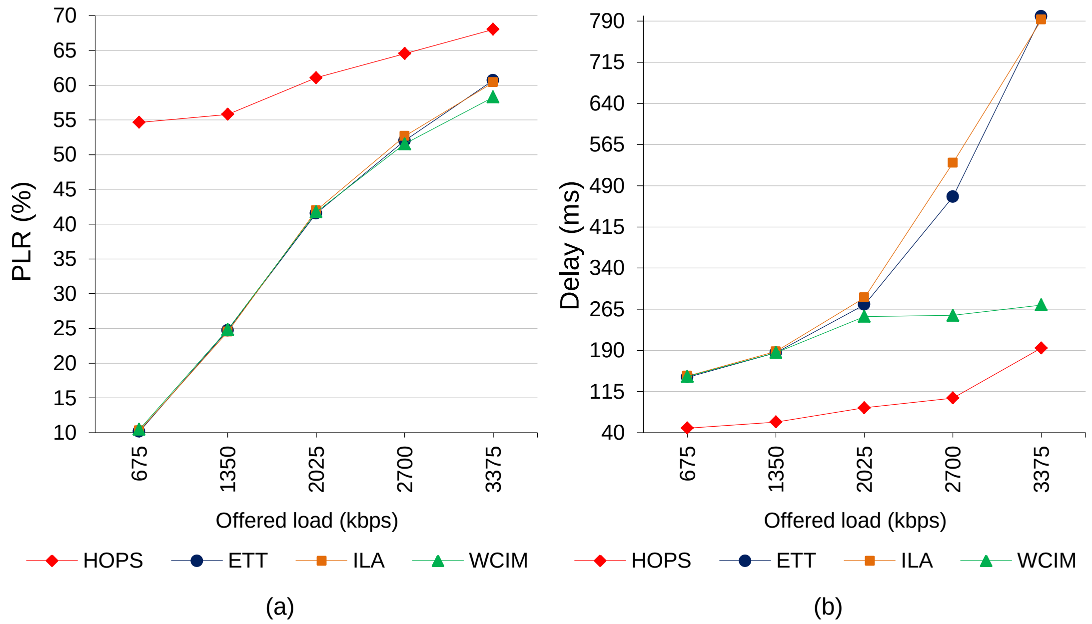


Fig. 4.24: Scenario 6 main results. a) Packet Loss Rate and b) End-to-end delay

Scenario 7

Scenario 7 analyzes the performance of the routings metrics according to different multi-radio configurations. The scenario is based on the same traffic parameters defined in the first scenario (i.e. grid topology and six random flows with random destinations), but in this case only the most loaded configuration is tested. Results are shown in Fig. 4.25. Common Channel Set (CCS) and Random Channel Assignment Algorithms (CAA) are used. CCS assigns to the two radios of each node the same set of orthogonal channels; i.e. all nodes have an interface assigned to channel A and another to channel B. On the other hand, Random CAA randomly assigns a different channel to each interface. In this scenario, the MIC routing metric is analyzed instead of the hop count metric, due to its channel-awareness.

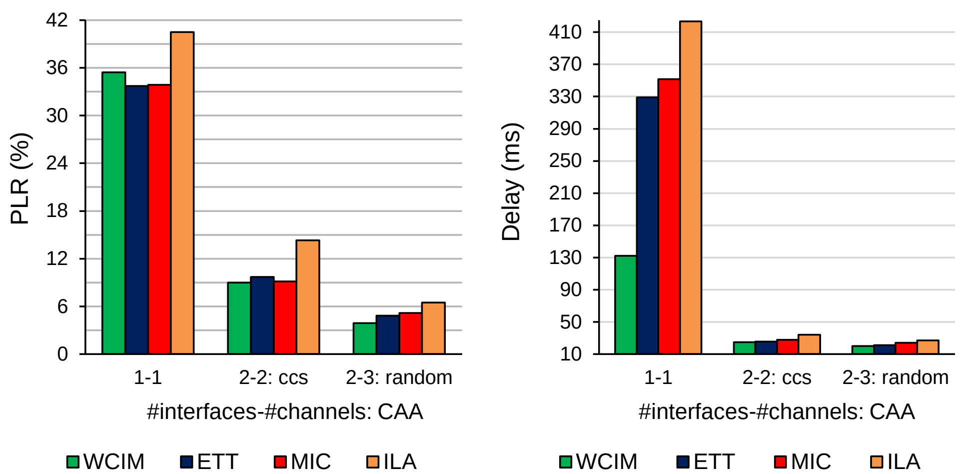


Fig. 4.25: Scenario 7 main results. a) Packet Loss Rate and b) End-to-end delay

For the single-radio single-channel case, results are similar to the analyzed ones in the previous scenarios; ILA leads to worse performance than ETT and MIC due to its utilization of longer and inefficient routes, while WCIM outperforms all metrics.

ETT obtains a very good performance in the CSS case. Since all neighbor nodes are connected through two links, direct paths using fast links can lead to good performance if flows are routed appropriately through orthogonal channels. As pointed out in previous sections, the error rate estimation used by the ETT metric is sensitive to interference, which, in addition to its tendency to use 12 Mbps links (which occupy less channel time), leads to good results in this scenario. On the other hand, using the Random CAA some nodes are connected through a single channel, thus ETT has less probability of using orthogonal channels when selecting the faster paths. Therefore, on the contrary to the load-aware routing metrics, its performance is worse in the Random case.

Although MIC routing metric is aware of the inter-flow and intra-flow interference, its routing strategy is inefficient in this scenario. First, its inter-flow interference algorithm is based on the number of neighbors of a link, which in a grid scenario is not especially useful. Secondly, its intra-flow avoidance is based on the alternation of channels, which can lead to the formation of hidden nodes, as pointed out in Section 3.3.

ILA results are better when using Random CAA due to a higher number of available orthogonal channels. Therefore, there are more chances to find routes using channels which are not interfered by any active flow, leading to shorter routes (average of 6.9 hops in front of the 7.3 of the CSS case).

Finally, WCIM obtains the best results both in CSS and Random CAA cases. In the CSS case, it performs similarly to ETT metric, selecting direct and faster routes and using the two available channels to decrease interference. In the Random case, its better trade-off between link-quality and inter-flow interference awareness permits WCIM to outperform both ETT and ILA routing strategies.

4.3.2.2.3 WCIM performance using TCP

In order to appropriately route TCP traffic, a minor modification of the WCIM routing metric is required. Since the bit rate of TCP is controlled by transport layer mechanisms and it is not constant, the flow rate parameter FR cannot be encoded into the ToS field as for UDP flows (although rate control mechanisms can be applied in the sources in order to limit the sending rate of TCP data). Thus, a mechanism is implemented in order to allow the nodes to passively monitor the transmitted load. Since using AODV route lifetimes should be updated with each forwarded packet [41], flow rate statistics can be easily obtained from the routing layer [54].

Fig. 4.26 shows the results of an 8x8 grid scenario with a varying number of TCP flows. Results are the average of 50 simulations. ETT and WCIM_MON (i.e. WCIM using passive monitoring) are analyzed.

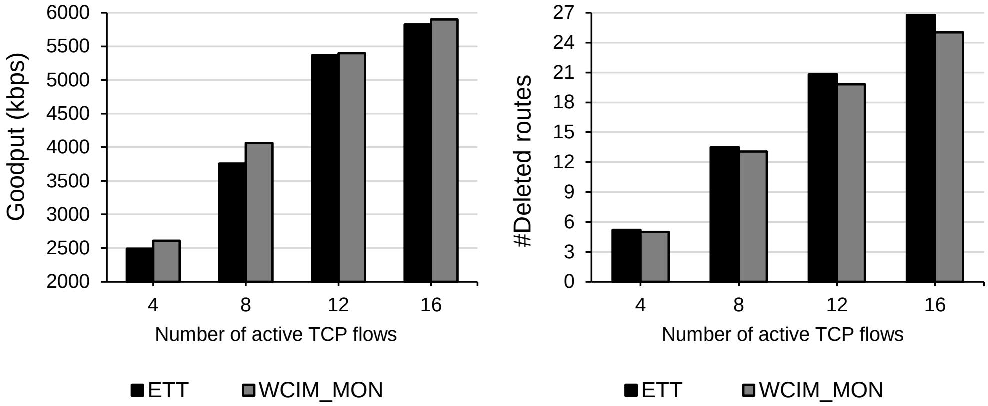


Fig. 4.26: WCIM performance using TCP. a) Goodput and b) number of deleted routes

Results show that in all cases WCIM obtains better results than ETT, especially in the first two, where the congestion is not so high. Indeed, as shown in Fig. 4.26b, TCP traffic easily saturates the network, leading to a higher number of deleted routes even in the less loaded cases. Multi-hop routing mechanisms make use of periodical signaling in order to maintain routes, which are impacted by the high data rates of TCP (e.g. due to collisions or buffer overflow). Ways to avoid this problem could include the limitation of TCP data rates [75] or assuring the delivery of signaling frames by using for instance a common channel isolated from data in multi-radio networks [135]. In any case, results show that WCIM_MON can be used to route TCP traffic at least as well as the ETT metric.

4.4 Conclusions

Contributions of this chapter focus on the impact of route creation strategies on performance of traffic flows traversing MIWNs. Based on the analysis of the most relevant state-of-the-art solutions and the conclusions of Chapter 3 regarding the phenomena which affect the performance of a path, a novel routing proposal is presented.

First, FB-AODV, a flow-based extension for the reactive routing protocol AODV which creates different paths according to the destination, the source and the ToS of the flows, is introduced. In front of the classic destination-based routing, FB-AODV permits to appropriately discover and maintain optimal routes for each flow. Although being designed to allow a proper utilization of load-aware routing metrics, results show that it also benefits other types of routing strategies.

Significantly, in multi-radio networks, FB-AODV reduces the importance of intra-flow interference awareness during path creation, which is the major cause of the non-isotonicity of some routing metrics and can lead to the formation of suboptimal paths and loops.

Then a novel routing metric, WCIM, which combines link- and load-awareness using a weighted model of contention and interference based on IEEE 802.11 physical and MAC layer mechanisms, is presented. By means of simulation, the performance of WCIM in a variety of scenarios is analyzed and compared with that of other representative routing metrics. As expected, the shortest-path Hop Count routing leads to a very poor performance in all cases due to its link-, load- and interference-unawareness. On the other hand, ETT's routing strategy, which is based on the selection of fast links, gives good results especially in scenarios which make load balancing difficult (e.g. multipoint-to-point scenarios). However, ETT suffers significant degradation under high load due to its load- and interference-unawareness. Finally, although being load-aware, ILA gives a poor performance because of overestimating inter-flow interference, thus leading to longer and inefficient routes. ILA results remark the importance of appropriately combining the different phenomena which impact the performance of the flows in order to obtain a proper route creation strategy. In multi-radio scenarios the performance of the MIC routing metric is also analyzed. MIC also leads to inefficient routes due to its unrealistic model of intra- and inter-flow interference.

WCIM outperforms the other considered metrics in almost all cases. Its routing strategy performs well both in low and high load conditions by selecting paths of low interference and congestion, but also a low number of hops using faster links. WCIM can actually be considered as a reliable estimator of the average end-to-end delay, which makes it possible to route flows through the best paths in terms of this performance parameter. Simulations in a random scenario show that with the increase in congestion WCIM operates in a way equivalent to an admission control mechanism, due to the scarceness of resources and available routes. This is an interesting feature for controlling the impact of new routes on the performance of active flows.

Finally, the performance of WCIM when routing TCP flows is also analyzed. A minor modification is introduced in the algorithm in order to properly capture the load of the flows, which can vary in time due to the congestion control mechanisms of TCP. In general, although improving the performance of ETT, WCIM benefits are limited in this scenario due to the high intra-flow interference caused by TCP flows.

The weighted model of interference and contention can be improved by considering more parameters which can affect the relationship between interference and available bandwidth analyzed in Chapter 3. For instance, perceived interference can vary according to the distance between sender and receiver or the robustness of the modulation being used. Indeed, due to capture effect, nodes are capable to receive frames even in hidden node scenarios [94]. Also, as pointed out in Chapter 3, according to the distance to the receiver, the level of interference caused by distant nodes may vary. Future work can make use of additional cross-layer parameters related with physical and MAC layers in order to improve the interference model.

Finally, due to its reactiveness, one of the major drawbacks of AODV is its reaction to dynamic events or scenarios which can degrade the performance of supposedly optimal routes [54][55]. This includes the arrival of new flows or the creation and elimination of links due to mobility, high interference or dynamic channel assignments. Therefore, next chapter discusses route maintenance in MIWNs and introduces an enhancement of the FB-AODV routing protocol which recovers active routes in a preemptive way.

5

Route maintenance in MIWNs

Once the optimal route is created, it should be maintained at least for the duration of the communication. However, uncontrolled phenomena like fading, external interference or node mobility could severely degrade link performance and even cause route disconnections. Route maintenance in MIWNs is usually focused on link break detection in order to recover disconnected routes due to these phenomena.

However, the unpredictable arrival of new flows in the network may cause congestion or interference on the flows being routed, also affecting the quality of the former optimal route. Route recovery methods which consider the impact of inter-flow interference variations have gained less attention from the research community.

This chapter is organized as follows. First section introduces route maintenance in MIWNs and surveys existing route recovery mechanisms for reactive routing protocols. Then, the proposed approach in order to enhance the route recovery of AODV is presented: DEMON, which stands for performance DEgradation MONitoring, allows preemptive route recovery based on passive estimation of link data loss rate. The performance of DEMON is evaluated by means of extensive simulations. Finally, the conclusions of this chapter are discussed.

5.1 Route maintenance in MIWNs

In proactive routing protocols like OLSR, all the paths are periodically updated by means of the periodic information exchange [46]. Therefore, their ability to react to route degradations and disconnections basically depends on signaling periodicity; higher signaling frequency leads to faster recoveries but it increments the overhead in the network [136][137]. On the other hand, in reactive protocols active routes are only updated during the route discovery procedure, which is dependent on active flows [41]. Thus, a new flow to the same destination can update an active route or path section if intermediate nodes are shared. Also, in order to react to route disconnections, reactive protocols implement mechanisms based on detecting link breaks and perform route rediscoveries. Since link break detection is usually based on monitoring the loss of signaling packets between neighbors (i.e. the Hello messages), recovery time is also dependent on the frequency of signaling messages [78]. In conclusion, in both types of routing protocols, by using the default recovery procedure a flow may undergo a large interval of performance degradation until the detection of the link break and the rediscovery of the new route.

However, since in reactive protocols active routes are bound to traffic flows with known sources and destinations, preemptive route maintenance mechanisms can be implemented [54][55]. Preemptive maintenance is basically based on detecting route degradations before disconnection occurs and alerting the sources of the flows in order to start the recovery of an active route. As has been introduced in the previous chapter regarding routing metrics, instead of using a binary logic to detect degradations (i.e. the link exists or not), preemptive mechanisms permit to monitor link quality variations. Thus, an estimation and integration of cross-layer parameters is also needed. Although preemptive maintenance was initially designed to improve routing performance in mobile networks [55], it can also be used to avoid performance degradation caused by other phenomena, as is the case of inter-flow interference.

This section reviews the route maintenance mechanisms used by the AODV routing protocol and the main preemptive route recovery extensions designed for on-demand routing protocols. Indeed, some of the analyzed preemptive solutions can be also applied to other reactive protocols, such as the Dynamic Source Routing protocol (DSR) [48].

5.1.1 Route recovery in AODV

When a link breaks along an active path, the node that detects the link break transmits a Route Error (RERR) message which lists the set of destinations that have become unreachable. Upon reception of the RERR message, the sources affected by the link break start a new route discovery, providing they still have data to transmit to the same destination. If alternative paths exist, the source and destination of a broken route will remain disconnected from the moment of transmission of the RERR until the reception of a new RREP by the source. The duration of this disconnection interval (or route change latency) may be extremely significant, especially in highly loaded, mobile or large networks [78][111]. This problem can be alleviated by means of an option called Local Repair [41][138]: the intermediate node which noticed the link break initiates route recovery by broadcasting RREQ messages with a Time-To-Live (TTL) set to the last known distance to the destination, plus an increment value. In this way, the route is recovered faster and the mechanism prevents the entire network from being flooded again.

For connectivity maintenance purposes, each node can periodically broadcast Hello messages within a one-hop radius. By default, the interval between Hello messages is 1 second and the loss of 3 consecutive Hello messages is understood as a link break [41]. Increasing the frequency of Hello messages or decreasing the number of allowed Hello losses is a simple way to improve the network sensitivity to mobility [78]. However, as was introduced in Section 3.3 regarding the estimation of link errors, the detection of link breaks based on Hello messages is not optimal [77]. Hello packets are short and they are broadcast at the lowest and most robust data rate. Also, there are therefore cases in which Hello packets can be correctly received, while data packets cannot, leading to large periods of unsuccessful data packet transmission (i.e. the Communications Gray Zone problem) [81].

There are other strategies for link failure detection, such as Link Layer Notification and Passive Acknowledgement, based on the absence of link layer ACK messages and the overhearing of forwarded packets, respectively [41]. However, these techniques need link layer feedback, which makes the routing protocol implementation dependent on the link layer mechanisms. Therefore, almost all routing protocol implementations are based on the exchange of Hello messages for connectivity maintenance, which allows a node to carry out one-hop neighborhood discovery and maintenance regardless of the specific link layer used.

5.1.2 Preemptive route recovery

One approach that mitigates the connectivity maintenance limitations of AODV mentioned above is the maintenance of routes using preemptive mechanisms. Preemptive route recovery comprehends the following two components: link quality monitoring and route recovery [55]. Nodes monitor the quality of the links that participate in active routes and decide when the quality is no longer acceptable. In such cases, the node which detects the performance degradation warns the source of the route, which then can start the discovery of a new route, or initiates a local repair process in order to find an alternative route.

5.1.2.1 Link quality monitoring

Most state-of-the-art link quality monitoring solutions for preemptive route recovery define link quality as a function of the received signal strength, in order to detect node mobility and anticipate link breaks. Since this mechanism was first introduced [55], it has also been adopted by subsequent proposals [139][140][141][142][143][144]. When a node receives a packet, the node compares the received power with a defined power threshold. If the received power is smaller than the threshold, the node assumes that the sender has left the region where communication was safe (i.e. now it is located in the so-called preemptive region). Thus, it may soon be unreachable due to mobility (i.e. be located in the out-of-range region). In that case, therefore, the receiver triggers route recovery preventing an incoming link-break and route disconnection. Fig. 5.1 illustrates the different communication regions.

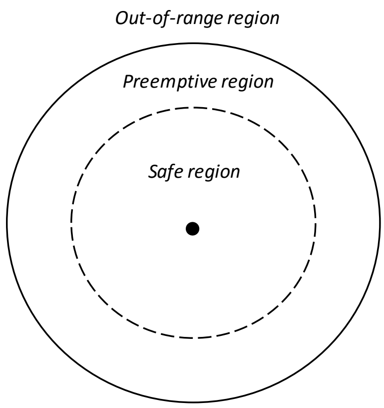


Fig. 5.1: Illustration of the regions involved in the preemptive recovery mechanism based on signal strength. The black dot at the center of the circles represents a receiver that determines whether the received power is below the threshold.

A significant drawback of preemptive solutions based on link quality monitoring is that they need successful packet reception in order to monitor the signal strength of the packets sent by a particular neighbor. Thus, these solutions are not able to detect (and react to) congestion and interference, since such phenomena cause packet drops and corrupt receptions due to collisions (e.g. as in the case of a hidden terminal) and do not affect the received signal power of successfully received packets. Furthermore, these solutions must have access to nodes' PHY layer parameters, which limits their implementation to specific NIC drivers. As aforementioned, a wide majority of routing protocol implementations for MIWNs use connectivity maintenance mechanisms which operate at the network layer, in order to avoid dependence on specific drivers.

Instead of using received signal strength, other preemptive protocols use GPS to obtain the position and speed of the nodes and compute the Link Expiration Time (LET), i.e. the predicted amount of time during which the link will remain active [145]. When the LET of a link falls below a defined threshold, a route recovery procedure is started. This approach requires a GPS receiver on each node and clock synchronization, thus limiting its application in real deployments. In addition, this solution is only aware of link degradation due to mobility.

Another type of preemptive solution is based on the Rate Adaptation Algorithms (RAA) used by some drivers of IEEE 802.11. A transmission rate decrease because of packet losses can be considered as an indicator of mobility [146]. According to the neighbors' data rates and to its own, a node can detect when the distance between itself and the neighbors increases and initiate a route recovery procedure. However, as described in Section 3.1.2, the behavior of the rate adaptation algorithm under congestion and interference could be counterproductive due to uncontrolled rate decrease, which might lead to unnecessary route recoveries [82].

Link break prediction can also be based on packet loss monitoring carried out by potential relay nodes. In a proposed routing protocol of the state-of-the-art [147], relay nodes, which are neighbors of the sender and receiver of the monitored link, overhear packet transmissions. When a relay node notices that a packet has reached its maximum number of retransmissions, it assumes that, due to mobility, the transmitter and the receiver are now out of their coverage ranges. The relay node then warns the transmitter in order to recover the route and proposes itself as an alternative next hop to the receiver. However, in real deployments it is difficult to assure the presence of a relay node for each pair of nodes. In addition, although this mechanism can detect packet losses due to any phenomena, under high load conditions (where collisions and retransmissions are very frequent) it may lead to network instability due to a high amount of route recoveries. Packet overhearing under these conditions could also burden the resources of the nodes. The mechanism has only been evaluated under mobility and very low load conditions [147].

Note that the preemptive solutions introduced in this subsection depend on a threshold in order to determine when the quality of a link is no longer acceptable, and therefore when route recovery should be initiated. The definition of the threshold is critical, since a threshold that is too high could lead to a late reaction to link quality degradation, whereas if the threshold is too low it may trigger unnecessary recoveries (e.g., due to temporary wireless channel quality fluctuation). Thus, some protocols use additional mechanisms to assure that the link is really degraded. For example, the nodes that form the degraded link can use a ping-pong procedure [55]: if more than a certain number of pings (i.e. probe packets requiring a reply) are lost, degradation is confirmed and the route recovery is initiated. Another technique is based on comparing the power of the last two received packets in order to estimate the relative speed between the two nodes that form the link

[141]. This estimation is used to update the value of the power threshold. In this way, as relative speed increases, the preemptive region becomes greater.

Finally, all the state-of-art link quality monitoring mechanisms, apart from [145] which uses GPS, are based on the reception of data packets. Therefore, if there are large intervals without data packets (for instance, due to TCP congestion control), link quality estimation could become poor or even unfeasible. In such a case, route recovery should be assumed by the default mechanisms of the routing protocol (i.e. route maintenance based on Hello losses in basic AODV).

5.1.2.2 Route Recovery

Depending on which node aims at repairing a broken route, route recovery techniques can be classified in the following two categories: source-initiated route recovery and local repair-based route recovery.

In source-initiated route recovery works in a similar way to RERR procedure, as illustrated in Fig. 5.2. The node which notices the degradation notifies this fact to the source by using a special control packet. Then, the source initiates a new route discovery for the same flow. In order to avoid the selection of degraded links during route recovery, RREQ messages should carry additional information. For instance, the RREQ messages can transport the minimum allowed link quality threshold [55][143]. Using this information, nodes will discard the RREQ received through a link of a quality lower than the threshold. The main drawbacks of source-initiated route recovery are the related overhead and delay.

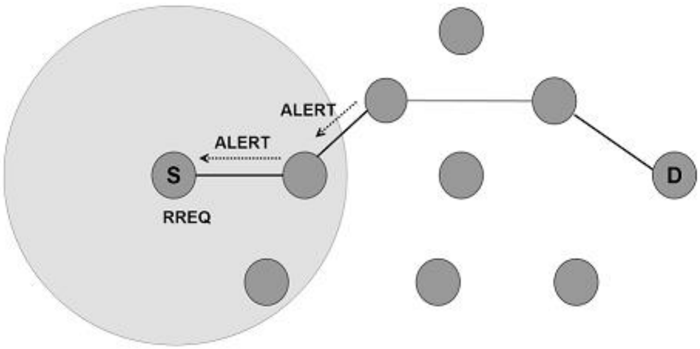


Fig. 5.2: Source-initiated route recovery. The node which detects the degradation (red link) notifies the source S, which initiates a new route discovery to the destination D. The active route is not changed until the new one becomes created.

On the other hand, local repair-based route recovery mechanisms allow intermediate nodes to start the route recovery procedure. The node which notices link degradation may broadcast RREQ messages as per the classical local repair procedure, as illustrated in Fig. 5.3a [144][145][146].

Other proposals use a relay node, which is a neighbor of both nodes forming the degraded link, to maintain the connectivity between the two link ends, as show in Fig. 5.3b [139][142][147].

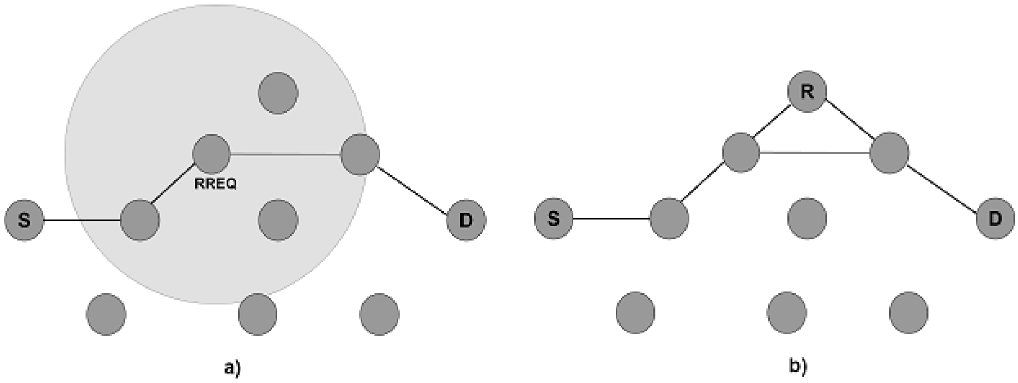


Fig. 5.3: Local repair-based recovery. (a) Route recovery is initiated by the node which detected the degradation. (b) A relay node is used in order to avoid the degraded link.

Local repair-based solutions may fail to find alternative routes in sparse networks. In addition, if performance degradation is due to congestion or interference, route recovery based on using nearby nodes could be inefficient, since it may reproduce the problem that led to performance degradation. In contrast, source-initiated route recovery allows modifying completely the route of the degraded flow once significant performance degradation has been found.

5.2 Proposed approach

In this section the DEMON preemptive routing mechanisms is presented. DEMON stands for performance DEgradation MONitoring and has been implemented as an extension of AODV, although it could be applied to other reactive protocols as DSR. It has been designed in order to satisfy the following requirements obtained from the analysis of the state of the art:

- A preemptive solution should use a comprehensive link quality monitoring mechanism which allows the protocol to take into account not only mobility but further reasons for performance degradation like congestion or interference.
- The link quality monitoring mechanism should be based on information available at the network layer, so that the solution does not depend on the link layer implementation and is not limited to particular network interface card drivers or hardware.
- The route recovery mechanism should be source-initiated in order to allow appropriate flow distribution in the network.

5.2.1 Motivation

This section introduces an example of performance degradation which is not caused by mobility in order to illustrate the purpose of DEMON. As in the previous chapter, a 64-node grid using the basic version of AODV was simulated (see Fig. 5.4). At second 200, a flow *f1* with a data rate of 1 Mbps was initiated and routed through *Initial route*. Then, at second 250, a highly loaded flow of 5 Mbps, called *f2*, was initiated. Note that in such a scenario, regardless of the routing metric in use, *f2* would degrade the performance of *f1,* since no route for *f2* can avoid that its source interferes several nodes traversed by *f1*. Thus, the only solution in order to avoid the interference of *f2* is to allow *f1* to be rerouted. However, basic AODV only performs route recovery after the detection of a link break.

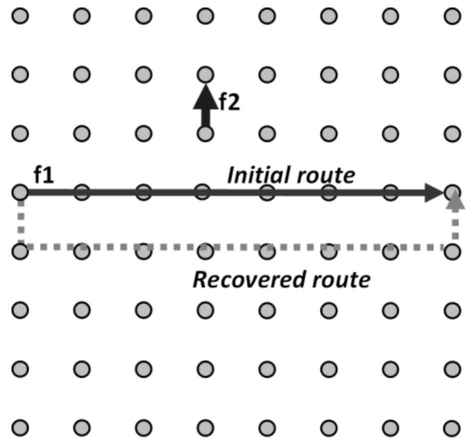


Fig. 5.4: DEMON motivation example scenario

After repeating the experiment 20 times with different seeds, two different types of results were obtained. In the first one, *f1* traversed the *Initial route* during all the simulation time. As shown in Fig. 5.5a, due to the high contention and interference of *f2,* the throughput of *f1* became reduced approximately in one half. In the second one, the *Initial route* was detected as broken by AODV after a long period of performance degradation due to the interference of *f2* and AODV finally recovered *f1* through the *Recovered route* (see Fig. 5.4), which did not suffer the influence of the interfering flow (the WCIM routing metric was used). However, route recovery was only triggered after 3 consecutive Hello message losses, which occurred after roughly one minute of performance degradation, as shown in Fig. 5.5b.

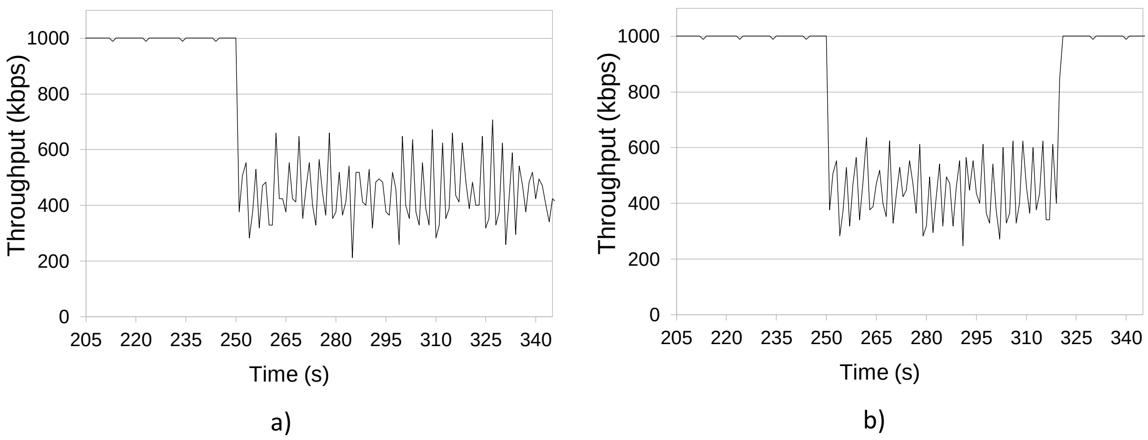


Fig. 5.5: DEMON motivation example results. a) Throughput of *f1* using basic AODV in a simulation whereby route disconnection did not occur. b) Throughput of *f1* using basic AODV in a simulation whereby *Initial Route* became detected as broken and a new route was discovered. In the figures the throughput is averaged each second according to the number of received packets. Thus, since the route rediscovery time is less than one second, the results of case b) do not show a throughput of zero after the route disconnection.

Note that in the presented scenario, where the reason for performance degradation is contention and interference, the preemptive solutions introduced in the previous section, which were based on received signal strength, node position or link data rate, would behave analogously to basic AODV; the interfering flow does not affect the signal strength of successfully received packets, while the position and the link data rate of the nodes are fixed. Therefore, the aim of DEMON is to obtain a preemptive route recovery extension of AODV which is aware of flow performance degradation due to any reason and allows a fast route recovery.

Results of DEMON in this scenario are illustrated in Fig. 5.9. In the following subsections DEMON’s components are described in detail.

5.2.2 Design and implementation

5.2.2.1 Link quality estimation mechanism

In order to detect performance degradation caused by a range of reasons wider than mobility alone, link loss rate is chosen as the criterion for determining link quality. A high loss rate may be a sign not only of mobility, but also of interference or congestion. In addition, due to retransmissions, lossy links also impact negatively on the performance of nearby nodes. For these reasons, the ETX metric of a link [59] is used as the start point of DEMON’s estimation mechanism.

As introduced in Chapter 4, the ETX metric, which estimates the expected number of transmission attempts for a packet through a link, was one of the first means for increasing performance in

MIWNs to be proposed as an alternative to the hop count metric. Since that time, ETX has been widely adopted. In fact, most of subsequent routing metrics that consider the link loss rate have been designed on the basis of ETX [17][37][51][52] and it is the de-facto metric of several popular routing protocol implementations [129].

ETX computation is usually implemented by taking into account the number of Hello messages which have been lost in a given period of time [59]. However, as previously introduced, the estimation of the link error rate based on Hello messages is not optimal [77]. Also, recent studies also show that ETX estimation based on probing messages is not reliable if the links are interfered by active flows [130][131]. Thus, in order to obtain a better estimation of the link performance than the one provided by the ETX metric, DEMON redefines ETX by using passive measurements of actual data traffic instead of Hello messages.

This new link-quality metric is called passive ETX (pETX). The pETX metric of a link *ij*, denoted $pETX_{ij}$, represents the expected number of data packet transmission attempts required for successful data packet delivery in the link *ij*, and is computed as follows:

$$pETX_{ij} = \frac{1}{d_i} \times \frac{1}{d_j} = \frac{NS_{ij}}{NR_{ij}} \times \left(\frac{NR_{ij} + ND_{ij}}{NR_{ij}} \right) \tag{5.1}$$

where:

- d_i and d_j denote the packet error probability in transmission and reception, respectively.
- NS_{ij} is the number of packets that the network layer of *i* has passed to its link layer in order to be transmitted to *j* during a certain interval. Note that since NS_{ij} is computed at the network layer, packets originated from upper layer retransmissions contribute to NS_{ij} as new packets.
- NR_{ij} is the number of non-duplicated packets that the network layer of *j* has received from node *i* during a certain interval. Note that these packets may be forwarded to the next hop (if *j* is an intermediate node) or processed by the upper layers (if *j* is the destination node).
- ND_{ij} is the number of duplicated packets received by the network layer of node *j* from node *i* during a certain interval. Duplicated packets can be detected by comparing the last two received packets from a neighbor. Reception of two consecutive identical packets implies that the link layer of the transmitter has performed a retransmission due to the loss of an ACK. Indeed, by using DEMON, duplicated IP packets can be discarded by intermediate nodes, thus avoiding useless channel time consumption.

Remarkably, nodes compute pETX by using information available at the network layer. While parameters NR_{ij} and ND_{ij} can be monitored by node *j*, this node needs to know the number of packets sent by node *i* during a certain period (which is called *cycle*) in order to calculate NS_{ij}. For this purpose, node *i* includes the number of packets sent since the start of the current cycle in its Hello messages, making it possible for node *j* to compute $pETX_{ij}$. The duration of the cycle is equal to the number of allowed Hello losses of the routing protocol. The frequency of Hello messages is a configurable parameter, which affects the time required to detect performance degradations and will be analyzed in Section 5.2.3.

The parameters NS_{ij}, NR_{ij} and ND_{ij} are recomputed by node *j* upon reception of a Hello message sent by node *i*. In order to provide robustness to the pETX computation even when Hello messages are lost, sequence numbers are included in the Hello messages. Fig. 5.6 shows an example of $pETX_{ij}$ computation, whereby sequence numbers are reset after a cycle of 3 Hellos. Intervals without transmitted packets (during which NS_{ij} is equal to zero) are not included in the pETX computation. Finally, if there is a complete cycle without transmitted packets, the pETX computation of the link is cancelled until data packets are received and can be monitored again.

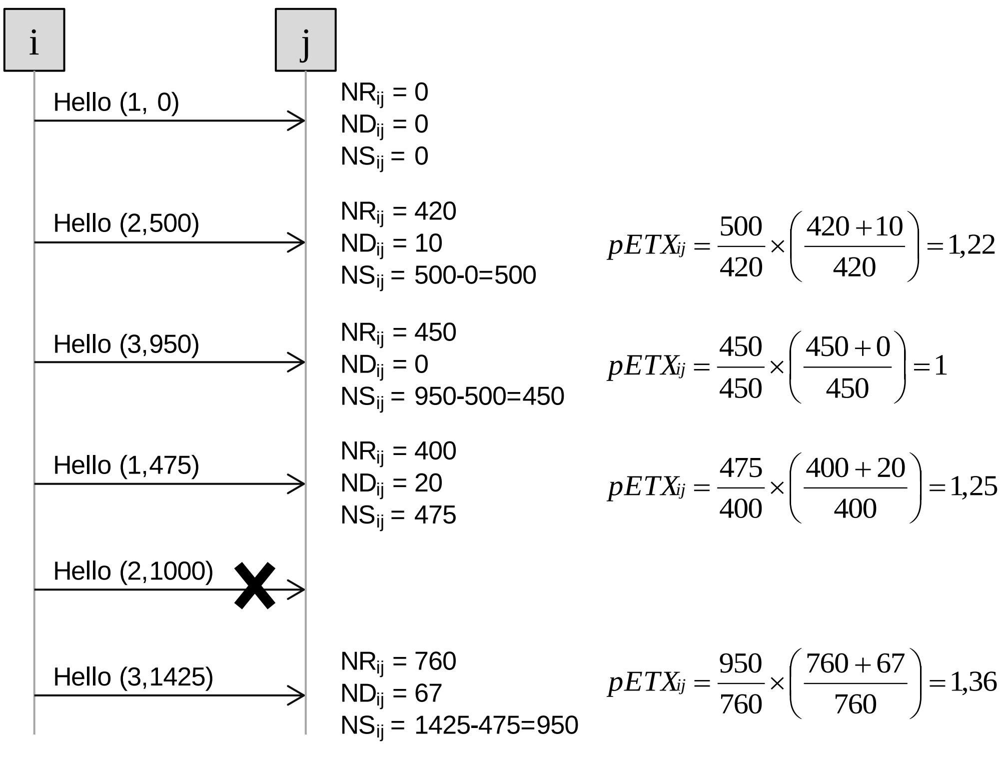


Fig. 5.6: Example of $pETX_{ij}$ computation performed by node *j* with a cycle of 3 Hellos. The notation of the Hello messages is *Hello (sequence number, number of packets transmitted in the current cycle)*. Note that the fifth Hello is lost. However, by means of the sequence number, node *j* knows that the sixth Hello belongs to the same cycle as the one previously received (otherwise, a link break would have occurred), and thus node *j* can correctly compute the pETX metric.

In order to filter out the influence of temporary fluctuations of the radio channel and avoid spurious detection of link quality degradation (which would trigger spurious route recoveries), an Exponentially Weighted Moving Average (EWMA) is applied to pETX, as shown in Equation (5.2). This filter has been called the time averaged filter or Window Mean EWMA (WMEWMA), and has been recommended for link quality estimation since it offers a good trade-off between reaction time and stability [148]. The smoothed pETX of a link *ij* at instant *n*, $spETX_{ij}(n)$, is defined as follows:

$$spETX_{ij}(n) = \alpha \times spETX_{ij}(n-1) - (1-\alpha) \times pETX_{ij}(n) \quad (5.2)$$

where α is a coefficient between 0 and 1 which controls the contribution of a new $pETX_{ij}(n)$ sample to the smoothed $spETX_{ij}(n)$. The latter is updated when a new $pETX_{ij}(n)$ sample is available.

Finally, node *j* computes the Link Success Rate (LSR) of link *ij*, LSR_{ij}, by using Equation (5.3). The LSR of a link is then compared with a link quality threshold to determine whether link performance is sufficient, as explained in the next subsection.

$$LSR_{ij}(n) = 100 \times \frac{1}{spETX_{ij}(n)} \quad (5.3)$$

5.2.2.2 Link quality threshold

As explained in the previous section, in DEMON every node computes the LSR of each link it belongs to. If the LSR of a link *ij* falls below a given threshold, node *j* starts route recovery procedure.

The threshold is a parameter that represents the minimum allowed LSR of a link being traversed by a flow, expressed by a percentage. In order to use a particular threshold in the network, it is necessary to consider the trade-off between sensitivity and stability. If it is not possible to find routes with a high success rate due to congestion, a high threshold may lead to continuous recovery of routes. On the other hand, in the presence of mobility, a low threshold will give rise to a slow reaction to performance degradation. In Section 5.2.3 the performance of different fixed values for the link quality threshold will be analyzed.

In addition to the option of using a fixed threshold for all links and flows in the whole network, a dynamic solution has been designed in which a particular threshold $\delta_{k,ij}$ is used for each flow *k* and traversed link *ij*. After route discovery, the threshold for each flow and link is set to the LSR of the link minus a safety margin, β, as follows:

$$\delta_{k,ij} = LSR_{ij}(t_k) - \beta \tag{5.4}$$

where t_k is the instant when the new route for the flow *k* traversing the link *ij* becomes active, and the margin β is used in order to avoid spurious route recoveries due to small variations of the LSR (which can be caused by the own load of the new flow). β is a percentage between 0% (immediate route recovery) and the LSR of the link (threshold zero, i.e. the route recovery is disabled). Once the threshold is set as per Equation (5.4), if the LSR of the link falls below the threshold, a route recovery is triggered. When a route is recovered, a new threshold is set for the affected flow for each traversed link. The objective of this mechanism is to be aware of the actual state of the network and accordingly set the thresholds to avoid continuous recoveries.

5.2.2.3 Route recovery mechanism

In DEMON, once the LSR of a link *ij* falls below the corresponding threshold, node *j* starts route recovery. The route recovery mechanism comprises two components: i) the selection of a flow that will be recovered, and ii) the transmission of a warning message to the source of the flow, so that the source triggers the AODV route discovery.

Since link quality degradation may not only be due to mobility, it may be counterproductive to re-route all the flows traversing a degraded link. For instance, in case of congestion, re-routing all the affected flows at the same time could reproduce the same problem in another zone of the network and cause instability. In order to avoid this problem, if node *j* notices link degradation, DEMON selects one single flow k^* to be re-routed, by using Equation (5.5):

$$k^* = \arg\max_{k \in K} \{\min\ (d_k(\mathrm{src_k}, j), d_k(j, \mathrm{dst_k}))\} \tag{5.5}$$

where *K* denotes the set of flows that traverse the degraded link, and $d_k(a,b)$ denotes the number of hops between nodes *a* and *b* through the route of flow *k*. The algorithm expressed in Equation (5.5) selects the flow k^* whose minimum distance in hops from node *j* to one of the endpoints of its route is the greatest one among the flows in *K*. As shown in Fig. 5.7, the algorithm attempts to re-route the most appropriate flow at a greater distance from the degraded link.

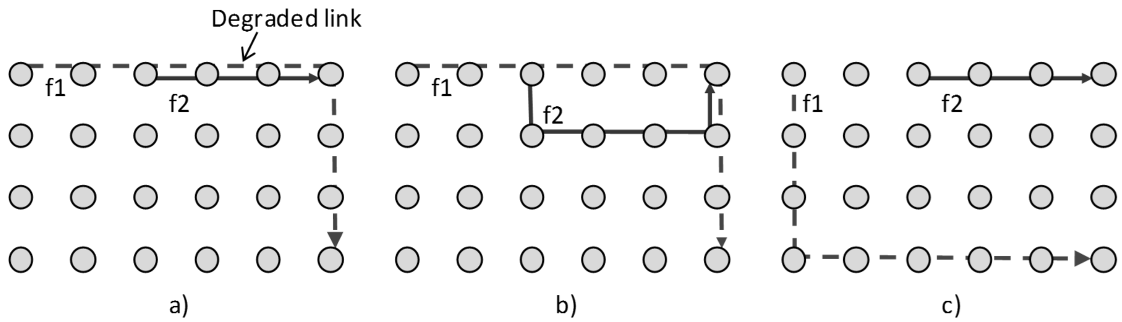


Fig. 5.7: Flow selection and route recovery in case of degradation. a) Initially, flows f1 and f2 are being routed through a link which becomes degraded. b) If the degradation is due to congestion, and f2 is selected for being re-routed, the new route might reproduce the same problem. c) As per the algorithm shown in Equation (5.5), f1 is selected for being re-routed, which leads to a better flow distribution in the network whereby flows affect each other to a significantly smaller extent.

Once the flow is selected, the node warns the source of that flow about the degradation, and then the source carries out a new route discovery to determine a new route for the flow. This way, a new path is created between the source and the destination (which is the same for both the forward and the backward directions).

The route recovery mechanism encounters a performance limitation due to the fact that AODV is destination-based. As introduced in Chapter 4, in AODV, all flows with the same destination that traverse the same common intermediate node are forced to follow the same route between the intermediate node and the destination node. Therefore, using AODV, the recovery of one route could also cause an implicit recovery of other routes to the same destination. This would limit the benefits of the route selection algorithm, since as mentioned above it might reproduce the problems that led to quality degradation in another zone of the network. Therefore, FB-AODV, whose design and benefits were introduced in Chapter 4, is chosen as the basis of DEMON in order to exploit to the full redistribution of the flows in the network after performance degradation [52].

Finally, in order to illustrate the complete DEMON process, Fig. 5.8 shows a flow chart that includes all DEMON components and their sequencing.

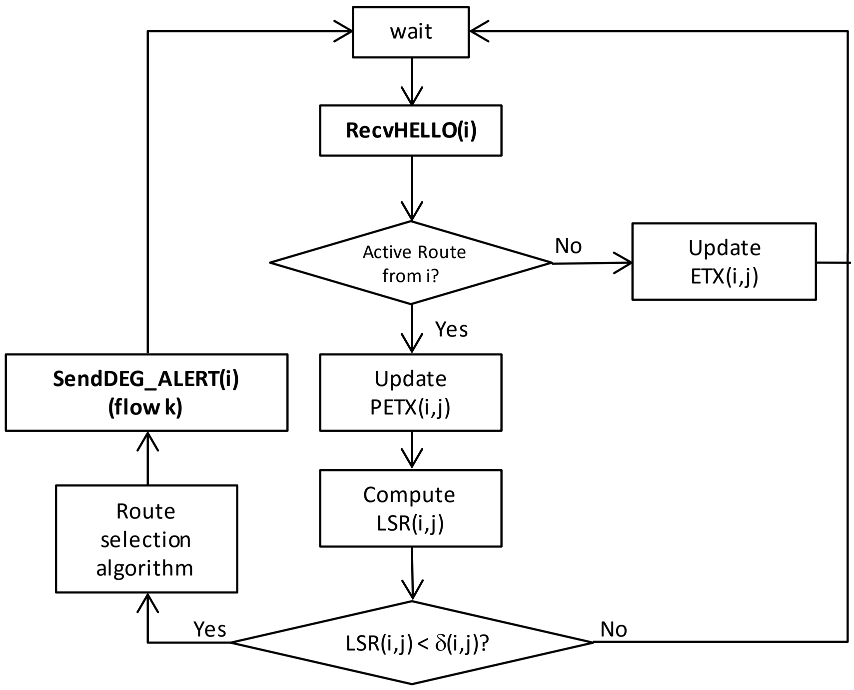


Fig. 5.8: DEMON flow chart of node j and link ij

5.2.2.4 Performance of DEMON in the motivation example scenario

Finally, revisiting the example scenario described in Section 5.2.1, and using DEMON instead of basic AODV, a significant improvement of the performance of the interfered flow is observed, as shown in Fig. 5.9. Since the interference of flow *f2* caused the loss of about the 50% of the packets, the LSR of the degraded link fell very fast under the threshold (in this case, a fixed threshold of 90% was defined). Once a node of the path monitored that degradation had occurred, it warned the source of *f1* which rerouted the flow through *Recovered Route*. As shown in the figure, in this scenario the whole DEMON procedure took around 5 seconds from the beginning of the interference until the flow became rerouted, thus reducing dramatically the duration of the performance degradation period (see Fig. 5.5 for comparison). In the next section DEMON will be extensively analyzed under a wide variety of conditions.

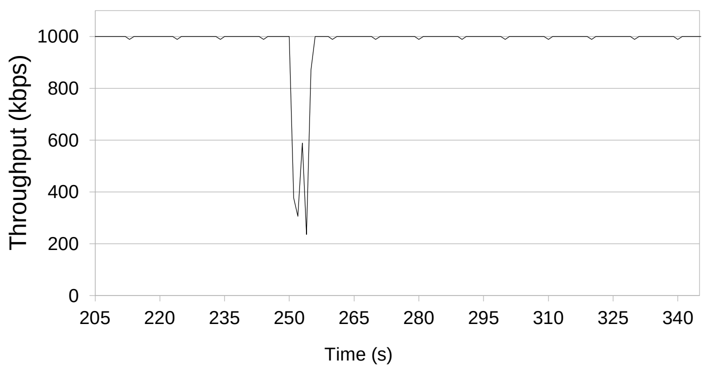


Fig. 5.9: DEMON motivation example results. Throughput of *f1* using DEMON

5.2.3 Performance Analysis

In this section, the performance of DEMON is analyzed by simulation. First, the simulation platform and the main parameters used in the evaluation are introduced. Then, next subsection studies the performance of DEMON when mobility is the main cause of link quality degradations. Subsection 5.2.3.3 analyzes the performance improvement of DEMON under interference in a wide range of scenarios. Finally, the performance of DEMON when data flows use TCP as the transport protocol is studied.

5.2.3.1 Simulation platform and scenario

Evaluation was carried out by simulation, taking as basis the grid scenario of 64 nodes detailed in Section 2.2.3.3 (see Fig. 2.14 and Table 2.9). The link bit rate of the nodes is 12 Mbps. Table 5.1 summarizes the other main parameters of the simulations.

Parameter	Value or Configuration
Simulation Time	460 seconds
Flows initialization	First flow starts at second 100. Then, a new flow starts every 5 seconds.
Flows ending	At second 450
Number of simulations per obtained average result	50
α (EWMA)	0.5
β (LSR)	10%

Table 5.1: Basic simulation parameters of DEMON's performance analysis

For the evaluation, DEMON is implemented as an extension of the FB-AODV. Hereafter, the AODV routing protocol without the DEMON extension will be referred as *default AODV*, while the AODV routing protocol with the DEMON extension will be simply denoted as *DEMON*. With regard to the DEMON link quality threshold, the performances of three fixed thresholds (whose values are set to 90%, 80% and 70%) and of the dynamic (DYN) one are analyzed.

The setting of α and β shown in Table 5.1 is chosen, which offers a reasonable trade-off between avoiding spurious route recovery and fast reaction to degradation. More specifically, low α values (i.e. higher impact of the last link pETX sample on the link pETX estimation) could trigger unnecessary route changes due to temporary link degradations, whereas high α values could excessively delay route recovery. On the other hand, setting the β parameter to very low values (i.e. the adaptive threshold approaches the LSR), could lead to immediate route recovery due to the own load of the recovered flow, whereas high β values will lead rapidly to low threshold values, which can delay the reaction to performance degradation. Nevertheless, both α and β parameters should be fine-tuned for each particular scenario.

Two different routing metrics are used for route discovery (i.e. during route creation and route recovery), WCIM [52] and ETT [43]. This way, the behavior of DEMON when two different route discovery strategies are used can be analyzed. Since WCIM is load- and interference-aware, it will benefit the route recovery phase in case of degradations caused by congestion, leading to new routes at a greater distance from the degraded links. In order to better analyze the impact of DEMON on the performance of the flows, the admission control functionality of WCIM is disabled (see Scenarios 5 and 6 of Section 4.3.2.2.2); instead of discarding links with insufficient resources, a high link metric is set in order to consider them but discourage its selection. On the other hand, although ETT is not load-aware, it offers a notable performance in a variety of scenarios, as analyzed in Chapter 4. Also, since it is one of the most popular routing metrics of the state of the art, it is interesting to evaluate if DEMON can also benefit it.

In the next subsections, goodput (i.e. number of bits correctly received at the destination per time unit) will be used as the main performance indicator. Each result depicted in the figures presented hereinafter illustrates the average value obtained from 50 simulations. The 95% confidence interval of each average result was computed during the simulations. These intervals were below 3% and 5% of the results obtained in stationary and in mobile scenarios, respectively, and do not provide significant conclusions. Thus, for the sake of illustration clarity, they are not included in the corresponding figures.

5.2.3.2 Analysis of DEMON performance with mobility

The scenario analyzed in this subsection consists of six active UDP, Constant Bit Rate (CBR) flows, each with randomly selected source and destination. Starting from a random location, nodes move according to the random waypoint model (RWP). In this model, each node remains static during a random pause interval, and then it selects a random destination point in the simulation area and moves towards the destination at a random speed. Each time the node reaches its destination, the process is repeated. In the scenario considered in this subsection, the speed and the pause time of each node are determined using a uniform random distribution within the intervals [0, v_{max}] m/s and [0, 20] s, respectively. The total traffic load in the network is 1620 kbps.

The evaluation starts by analyzing the impact of two critical parameters of the Hello message-based connectivity maintenance mechanism on the performance of the flows in MIWNs, for different node speeds. The results are used to determine the settings for these parameters in the next subsection. The parameters under consideration are the frequency of Hello messages and the number of allowed Hello losses. In default AODV, these parameters determine the maximum Hello wait time, i.e. the time interval that a node will wait for a Hello message from a neighbor before deciding that the corresponding link has become broken [41]. In addition, in DEMON, since Hello messages are needed to compute the pETX metric of the links, their frequency determines the time required to detect performance degradation. Thus, adequate tuning of these parameters is critical for achieving good network performance, especially in mobile scenarios.

Fig. 5.10 show the results obtained when using default AODV with ETT and WCIM metrics for route discovery, which are very similar. When mobility increases, performance improves by means of using low allowed Hello losses and low Hello interval (which determine a low Hello wait time). On the other hand, under low mobility conditions, the best results are obtained when Hello wait times are high for all the routing metrics and mechanisms. This is because when mobility is low, link breaks are mainly caused by congestion or interference between active flows. In these conditions, Hello packets, which are neither acknowledged nor retransmitted at the link layer, are more likely to be unsuccessfully delivered than data packets. According to the results, despite the Hello packet losses, it is better to continue using a link of moderate quality for data exchange than declaring the link as broken and incurring the overhead of finding a new route, which may suffer the same problems as those of the old route.

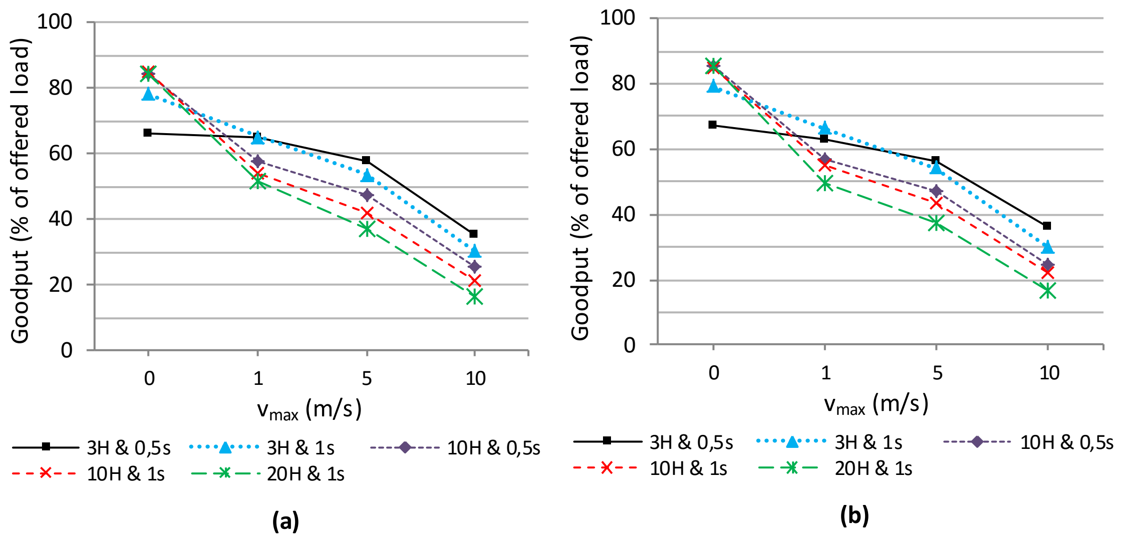


Fig. 5.10: Study of Hello message connectivity maintenance parameters using default AODV. a) Goodput obtained by using the ETT metric for route discovery; b) Goodput obtained by using the WCIM metric for route discovery. The notation "xH & ys" denotes an allowed loss of x Hellos and a time between Hello messages of y seconds.

The AODV specification defines by default a time between Hello messages of 1 second and an allowed loss of 3 consecutive Hellos [41]. These settings yield good results in the considered scenario. Note that setting the allowed Hello loss to a value smaller than 3 might lead to spurious link break detections, given the variable link quality that is characteristic of wireless links.

Fig. 5.11 shows the goodput obtained by using DEMON. Since all the different thresholds led to similar results in this scenario, figures show the average of the results obtained by using all of the different thresholds (i.e. 90, 80, 70 and dynamic). As speed increases, performance is more sensitive to the frequency of Hello messages than to the number of allowed Hello messages lost. Since link quality monitoring uses Hello messages for exchanging message transmission count information between neighbors, a higher frequency of these messages allows a faster reaction to performance degradation. For example, in high mobility cases, a faster reaction is necessary in order to recover routes before a link break occurs. Similarly to default AODV, under low mobility conditions, better results are obtained when Hello wait times are high.

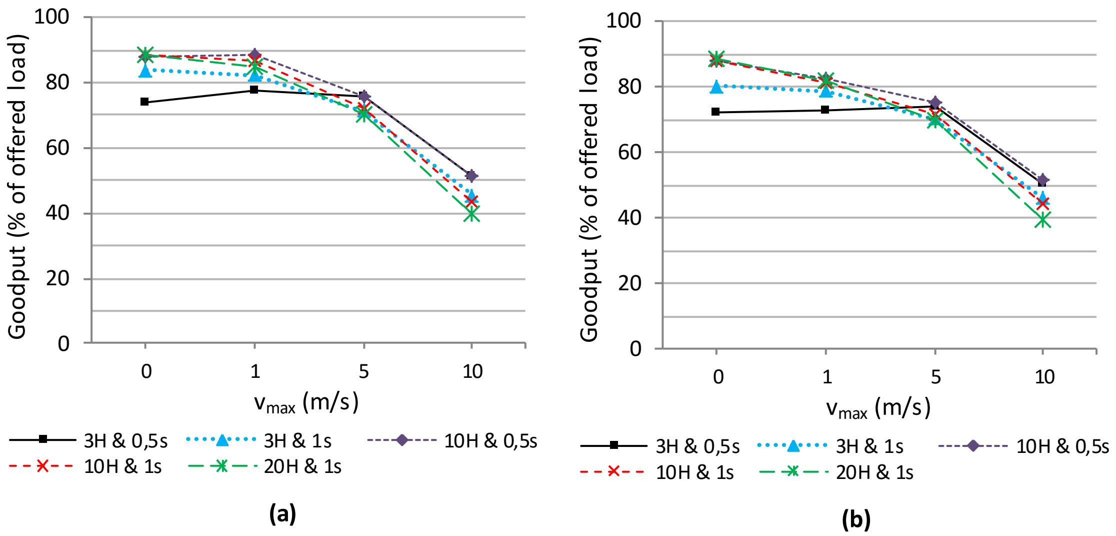


Fig. 5.11: Study of Hello message connectivity maintenance parameters using DEMON. a) Goodput obtained by using the ETT metric for route discovery. b) Goodput obtained by using the WCIM metric for route discovery. The notation "xH & ys" denotes an allowed loss of x Hellos and a time between Hello messages of y seconds.

As shown in Fig. 5.12, in average DEMON achieves up to 80%-90% goodput increase with respect to default AODV, when both use ETT or WCIM.

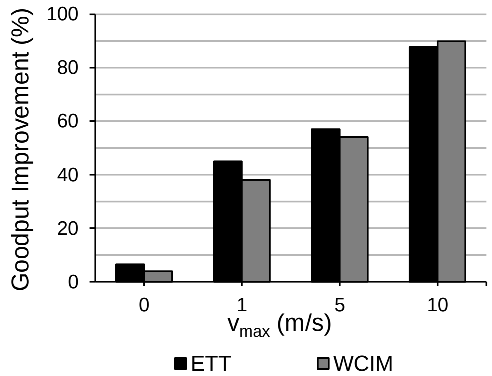


Fig. 5.12: Performance degradation caused by mobility. Goodput improvement obtained using the DEMON extension.

Finally, Table 5.2 shows a qualitative comparison of the evaluation results for the state-of-the-art preemptive proposals. In general, topology and mobility conditions used in the evaluation of state-of-the-art proposals are comparable to those of this scenario, although some works analyze other conditions such as higher mobility or lower load. As shown in Table 5.2, improvements in state-of-the-art preemptive solutions with regard to the basic versions of the corresponding routing protocols is similar to or lower than the one obtained by DEMON.

Solution	**Number of nodes**	**Mobility**	**Load configuration**	**Goodput gain of preemption**
H-AODV [139]	80	RWP Max. speed: 10 m/s Min. pause time: 7 s	CBR: 40 flows of 16 kbps and 30 s of duration. Simulation time of 300 s	10% - 25%
CPDSR [140]	50	RWP Max. speed: 30 m/s Min. pause time: 1 s	TCP: 50 FTP connections. Simulation time of 200 s	20% - 30%
LAW [141]	50	RWP Max. speed: 20 m/s Min. pause time: 0 s	TCP: 50 FTP connections. Simulation time of 500 s	20% - 30%
AODV-PSR [142]	50	RWP Max. speed: 20 m/s Min. pause time: 0 s	CBR: 40 flows of 12 kbps. Simulation time of 900 s	10% - 15 %
RELREC [147]	200	RWP Max. speed: 10 m/s Min. pause time: 20 s	CBR: 2 flows of variable load: 8 kbps – 64 kbps. Simulation time of 5000 s	0% - 5%
AODVLP [144]	50	RWP Max. speed: 30 m/s Min. pause time: 10 s	CBR (50 flows of 2 kbps) and TCP (50 connections) Simulation time of 900 s	0% - 15%

Table 5.2: Comparison of the improvement and evaluation details of state-of-the-art preemptive solutions. The works [55], [145], [146] and [143] do not include an evaluation of the solutions proposed therein in terms of goodput.

5.2.3.3 Analysis of DEMON performance under interference

Next, the performance of DEMON is analyzed in six scenarios where the main cause of performance degradation is the interference caused by the increasing load of the active UDP, CBR flows. Each scenario has particular conditions in terms of offered load, number of flows, spatial node distribution, link rates, node mobility and use of single- or multi-radio nodes. Table 5.3 summarizes the main characteristics of the six scenarios.

	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6
Type of Scenario	Stationary grid	Stationary grid with a gateway	High mobility	Low mobility	Stationary random distribution	Stationary multi-radio grid
Node location	Grid	Grid	Random	Grid	Random	Grid
Number of flows	32	32	6	6	6	32
Sources	Random	Random	Random	Random	Random	Random
Destinations	Random	One, fixed	Random	Random	Random	Random
Minimum offered load (Mbps)	1.60	1.60	0.54	1.62	0.54	1.60
Maximum offered load (Mbps)	4.00	4.00	3.24	3.24	2.16	6.40
Link rate (Mbps)	12	12	12	12	12	6
Multi-radio	No	No	No	No	No	Yes
Mobility	No	No	Yes	Yes	No	No

Table 5.3: Simulation study scenarios.

Based on the results of Section 5.2.3.2, in all scenarios an allowed Hello loss of 10 and an interval of 1 second were set for both default AODV and DEMON in all scenarios, except for Scenario 3. In this latter scenario, where node mobility is high, an allowed Hello loss of 3 was set for default AODV, since it provides better performance, while the allowed Hello loss of 10 was still used in DEMON.

As previously analyzed, state-of-the-art preemptive solutions are insensitive to performance degradation due to reasons other than mobility, such as interference or congestion. Therefore, in scenarios without mobility (i.e. scenarios 1, 2, 5 and 6) it can be assumed that these solutions would obtain results similar to those of default AODV.

5.2.3.3.1 *Scenario 1: stationary grid*

In the first scenario, 64 nodes are stationary located in a regular grid topology, with a distance between consecutive nodes in the same row or column of 140 meters. 32 flows are present in this scenario, each with randomly chosen source and destination.

Fig. 5.13 shows the results for this scenario in terms of goodput. In this scenario, performance degradation is caused by congestion and interference between active flows. In low load conditions, the improvement of DEMON is minor, since flows suffer hardly any performance degradation. Under high load, congestion and interference degrade the quality of links. In this case, DEMON clearly outperforms default AODV by properly reallocating flows in the network.

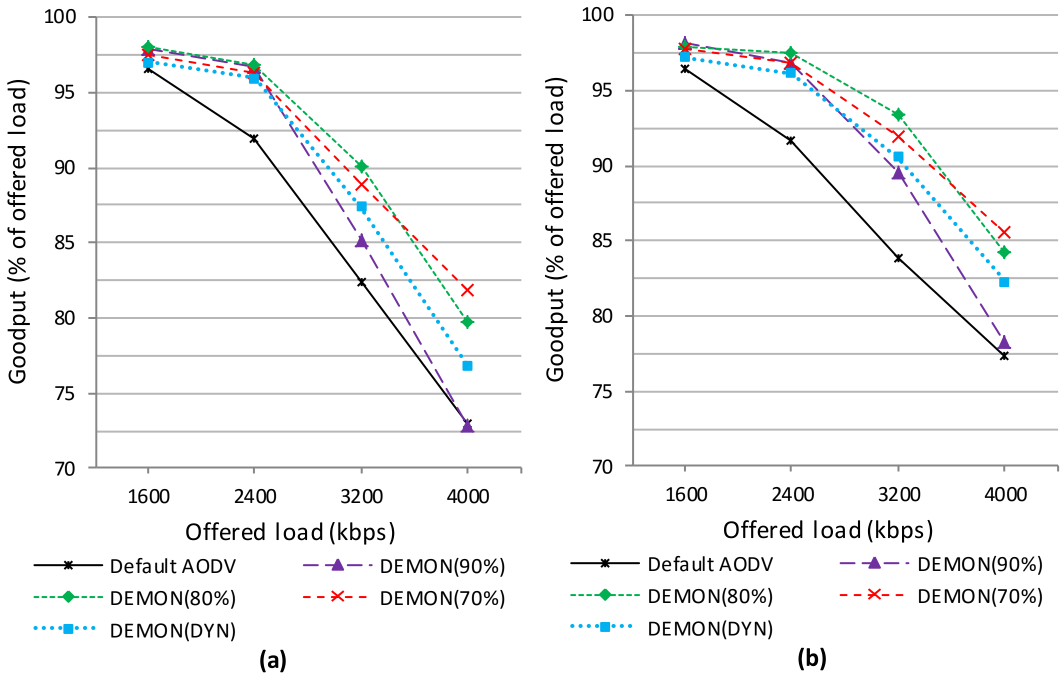


Fig. 5.13: Scenario 1 results: goodput. a) ETT metric for route discovery. b) WCIM metric for route discovery. DEMON(*X*) denotes the use of DEMON, where *X* is a percentage or 'DYN' if a fixed or the dynamic threshold is used, respectively.

The highest fixed threshold (i.e. 90%) obtains good results under low load conditions. However, as load increases, performance of this threshold decreases, and even becomes similar to that of default AODV. As shown in Fig. 5.14, when using this threshold, the number of route recoveries per flow significantly increases with the offered load. This is due to the fact that, because of congestion and interference, the number of links with an LSR below 90% increases significantly; hence the threshold of 90% becomes unsuitable under high loads. On the other hand, the lower fixed thresholds yield a better performance, since they lead to a smaller amount of route recoveries.

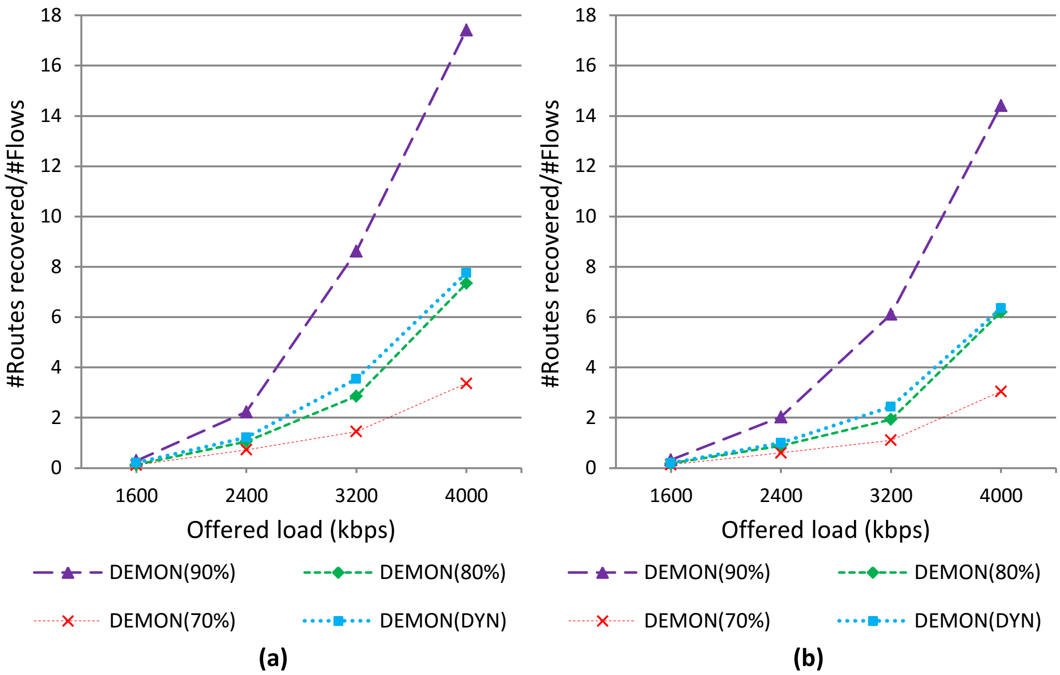


Fig. 5.14 Scenario 1 results: route recoveries per flow. a) ETT metric for route discovery. b) WCIM metric for route discovery

Under moderate to high load, the dynamic threshold performs better than the highest fixed threshold, but worse than the lower ones. Because the dynamic threshold is set on the basis of link quality at the instant of route discovery, it underperforms, since link qualities in this scenario are highly variable due to the presence of a high number of flows. Nevertheless, the dynamic threshold achieves the objective of avoiding the high number of route recoveries that occur with the highest threshold.

Note that as shown in Fig. 5.14, the use of the DEMON extension and ETT as the routing metric leads generally to a higher number of route recoveries than DEMON with WCIM. Since the WCIM routing metric is load-aware, it takes into account interference and congestion, which provides a better route selection than ETT, for both route discovery and route recovery. Indeed, in some cases, flows recovered by the ETT metric became routed again through the same degraded route. For this reason, in this scenario and also in the following ones, DEMON achieves usually better performance using WCIM than with ETT.

Fig. 5.15 shows the average packet end-to-end delay for this scenario. As observed in the goodput results, in this scenario the DEMON extension also outperforms basic AODV in almost all considered cases. Again, the highest fixed threshold obtains the best results under low load conditions but performance of this threshold degrades as interference increases. In contrast, the rest of evaluated thresholds perform similarly and better than the highest fixed threshold under high load. According to the results depicted in Fig. 5.15, it can be concluded that contention and interference affect significantly the packet end-to-end delay.

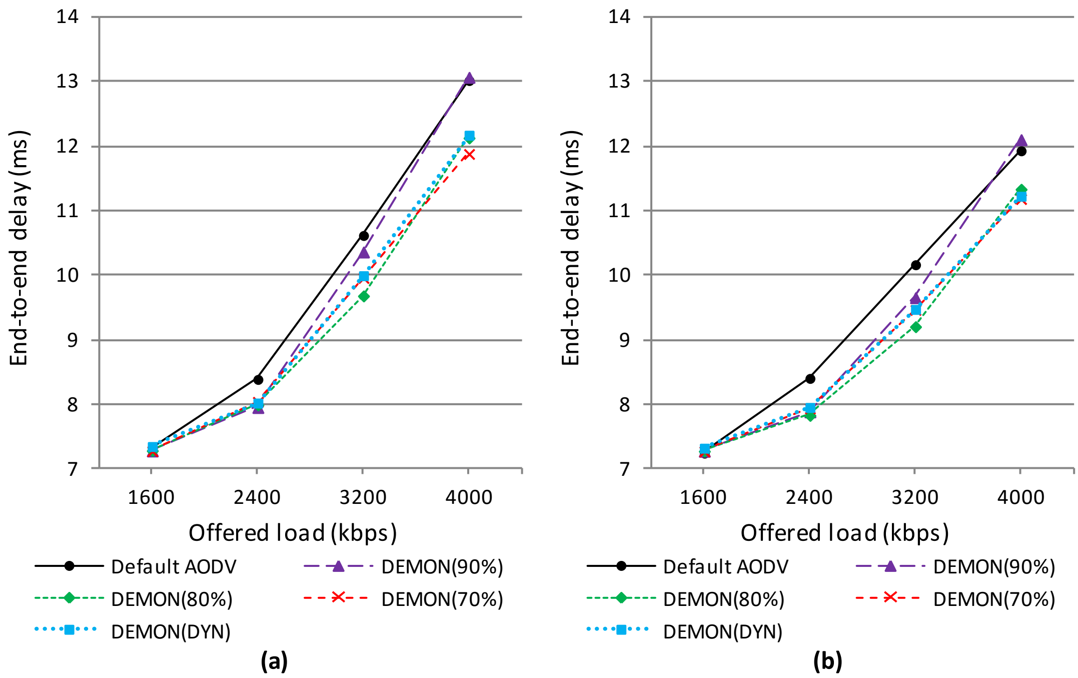


Fig. 5.15 Scenario 1 results: average packet end-to-end delay. a) ETT metric for route discovery. b) WCIM metric for route discovery

DEMON rerouting strategy improves performance in terms of delay, even though it generally leads to longer routes in order to avoid congestion. In general, in this scenario and in the following ones, end-to-end delay performance of both basic AODV and DEMON is almost complementary to their goodput performance (i.e. when a configuration provides high goodput, it provides also low delay, and vice versa). Therefore, for the sake of avoiding redundancy, henceforth the analysis of DEMON is focused on the basis of goodput results.

5.2.3.3.2 Scenario 2: stationary grid with a gateway

The second scenario analyzes a network in which a node acts as a gateway (e.g. offers connectivity to the Internet). 32 flows with a randomly selected source are again present in the network, but in this scenario the destination is the same for all these flows (the destination is the node at the bottom right end of the regular 8x8 grid). The remaining scenario characteristics are the same as those in the first scenario.

Fig. 5.16 shows the results for this scenario. Once again, DEMON clearly outperforms default AODV.

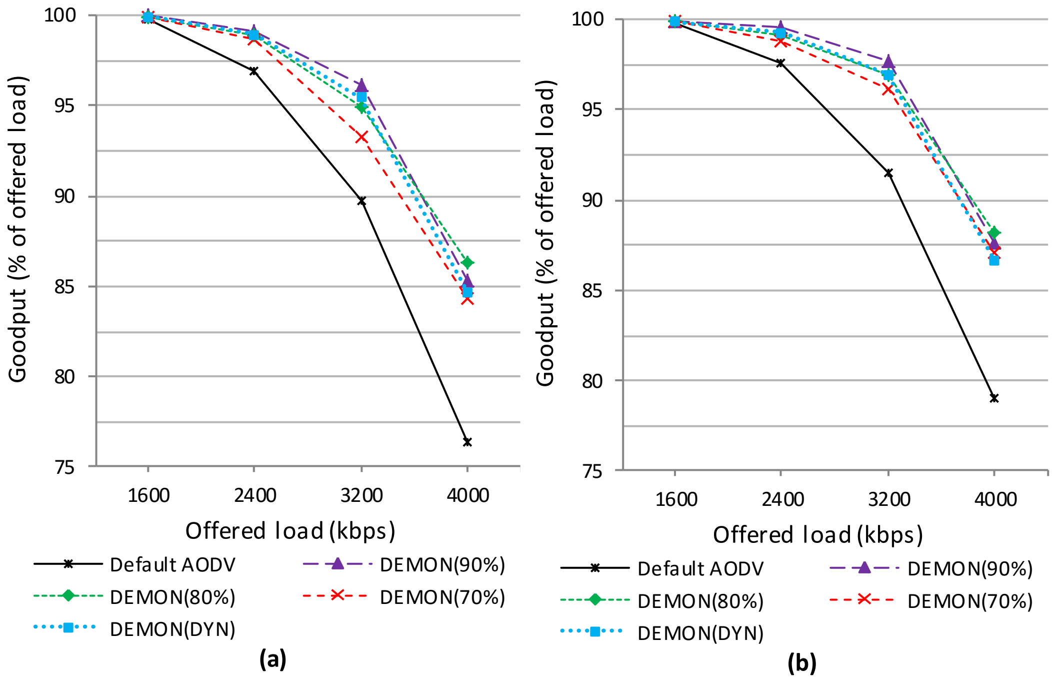


Fig. 5.16 Scenario 2 results: goodput. a) ETT metric for route discovery. b) WCIM metric for route discovery

In this scenario, the difference between the performances provided by using the different thresholds is minor. The reason of these results is that congestion is lower than in the previous scenario due to sparser routes (an average of 8 to 9 hops), leading to a lower number of route recoveries as shown in Fig. 5.17. Indeed, the 70% threshold obtains, in general, slightly worse results due to its more conservative behavior.

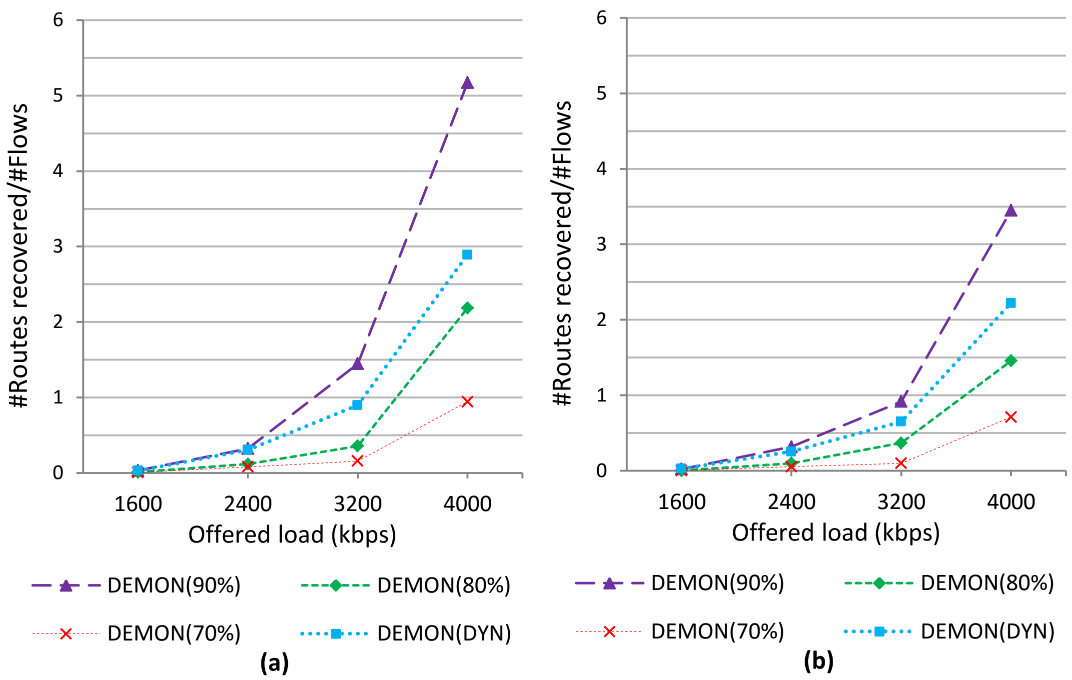


Fig. 5.17: Scenario 2 results: route recoveries per flow. a) ETT metric for route discovery. b) WCIM metric for route discovery

5.2.3.3.3 Scenario 3: high mobility

In this scenario, nodes are initially placed in a randomly chosen location, and then move according to the random waypoint model (RWP). The speed and the pause time of each node are determined using a uniform random distribution within the intervals [0, 5] m/s and [0, 20] s, respectively. There are 6 flows with random source and destination.

As shown in Fig. 5.18, DEMON clearly outperforms default AODV, achieving from 30% up to 90% of increase in goodput, depending on the offered load, for both ETT and WCIM routing metrics. As the load increases, the goodput gain of DEMON compared with default AODV decreases; this is because default AODV suffers from long disconnections due to route change latency. Thus a smaller amount of data traffic is transmitted, and the degree of congestion is low regardless of the load offered to the network. In contrast, DEMON allows a greater fraction of data traffic to be transmitted, but the goodput, expressed as a percentage of offered load, decreases as load increases due to congestion plus mobility.

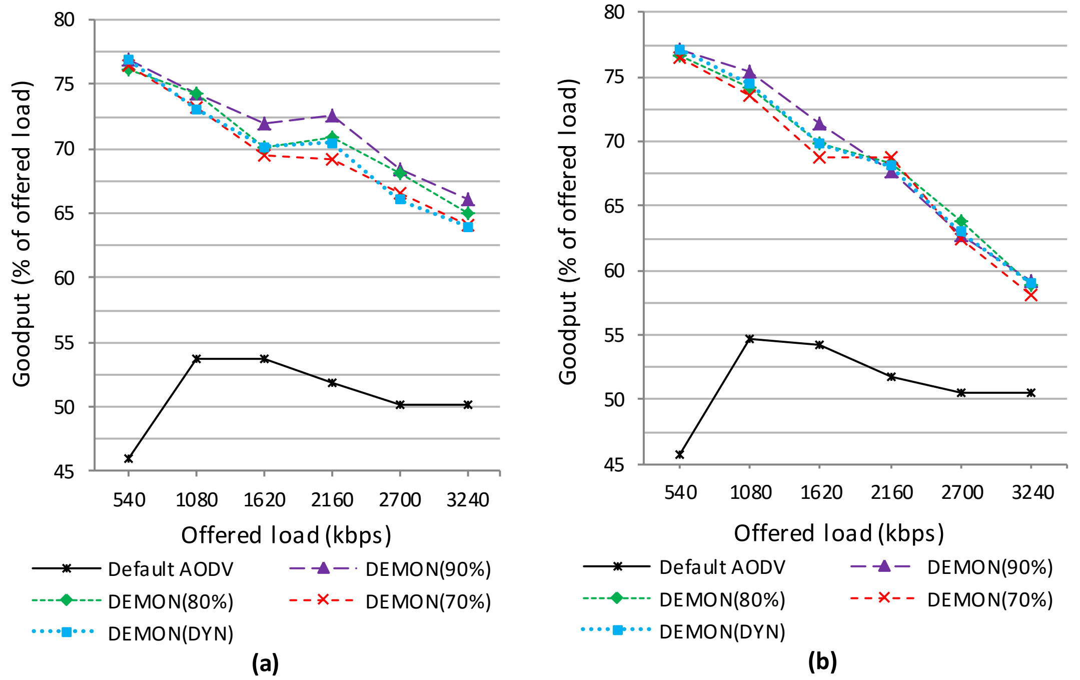


Fig. 5.18 Scenario 3 results: goodput. a) ETT metric for route discovery. b) WCIM metric for route discovery

On the other hand, Fig. 5.18 shows that the different thresholds used in DEMON lead to similar goodput results, especially when the WCIM metric is used. In the case of the ETT metric, the fixed threshold of 90% offers a slightly better performance than the other thresholds. This phenomenon occurs because in this scenario link performance degradation is mainly caused by mobility, and therefore a high threshold provides a fast reaction to link breaks.

Note that in this scenario ETT combined with DEMON obtains with increasing load better results than WCIM. In such a dynamic scenario, the WCIM model presented in Fig. 4.8 is difficult to stabilize due to the high variation of one- and two-hop neighbors, especially with high load which causes the loss of signaling messages. On the other hand, ETT only depends on link-quality, which in this case is the main issue affecting the performance of the routes.

5.2.3.3.4 Scenario 4: low mobility

In the fourth scenario, the nodes are first located in the same grid used in Scenario 1. However, after initialization, the nodes select a random direction and move linearly in that direction. The speed is determined by using a uniform random distribution within the interval [0, 0.1] m/s. Under the low speed conditions of this scenario, the number of link breaks is low. Note that the unicast transmission rate of the nodes is fixed at 12 Mbps, while neighbor discovery is based on Hello messages, which are broadcasted at 6 Mbps. Compared to the previous scenario, low mobility causes some nodes to remain for a longer time in the zone where links are unable to transmit data packets successfully, but are considered active links by default AODV, since Hello messages are not lost (i.e. the Communization Gray Zone problem presented in 3.1.2). The number of flows in the scenario is 6, each with randomly selected source and destination.

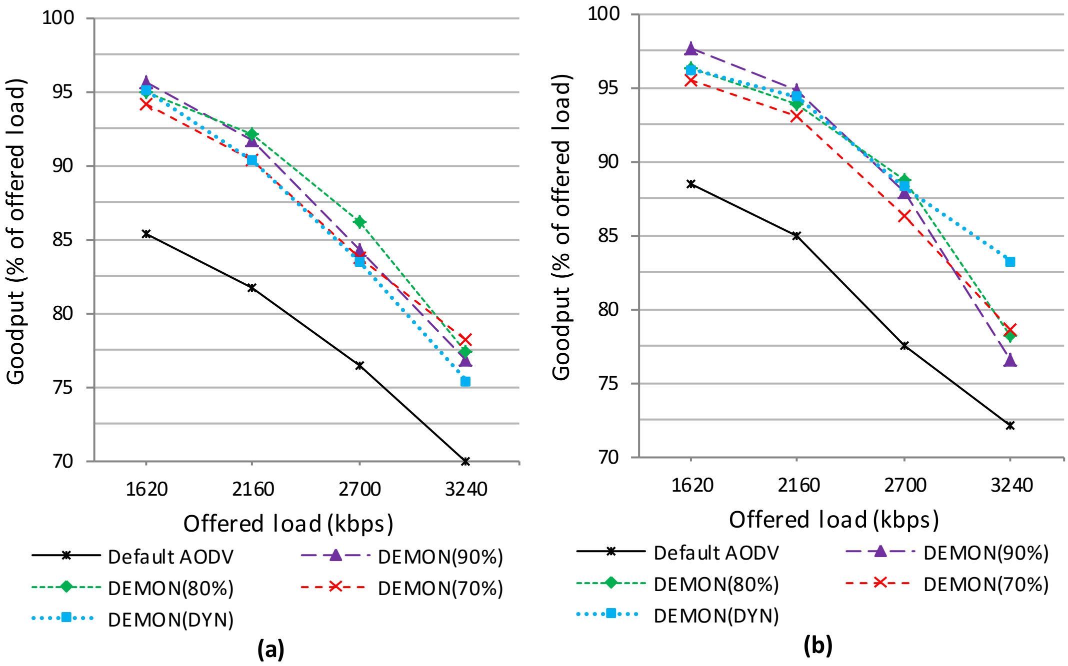


Fig. 5.19: Scenario 4 results: goodput. a) ETT metric for route discovery. b) WCIM metric for route discovery

As shown in Fig. 5.19, the gray zone problem causes significant performance degradation of default AODV, even under low offered load. In contrast, since DEMON detects link performance degradation based on the link data loss rate, it is able to detect when a link becomes degraded and recover the corresponding routes. In this scenario, due to the lower mobility, WCIM can apply load- and interference-awareness in a more proper way, thus leading in general to better results than ETT.

With regard to the link quality thresholds tested for DEMON, in contrast to previous scenarios, under high load the dynamic threshold obtains the best results using WCIM. This is due to that fact that in this scenario network conditions are less variable than in the previous ones because of the smaller number of flows and the lower mobility. Link qualities are therefore more stable, and the dynamic thresholds, which are set during route discovery, are consistent with the network conditions for long time intervals. Nevertheless, the dynamic threshold underperforms when ETT is used. As introduced in previous scenarios, when using ETT, DEMON leads to a high number of rediscoveries due to its load-unawareness. This problem restricts the benefits of the dynamic threshold when the ETT metric is used, since the dynamic threshold depends on the quality of the new route.

5.2.3.3.5 Scenario 5: stationary random node spatial distribution

The fifth scenario has the same characteristics as the previous one, except for the fact that nodes are statically located in the simulation area using a uniform random distribution. Since in this scenario the number of neighbors of a node is variable and sometimes scarce, the number of alternative routes that can be used is also limited. Thus, network congestion dramatically increases with the offered load. For this reason, the range of offered loads is smaller than the one evaluated in previous scenarios. Fig. 5.20 illustrates the obtained results.

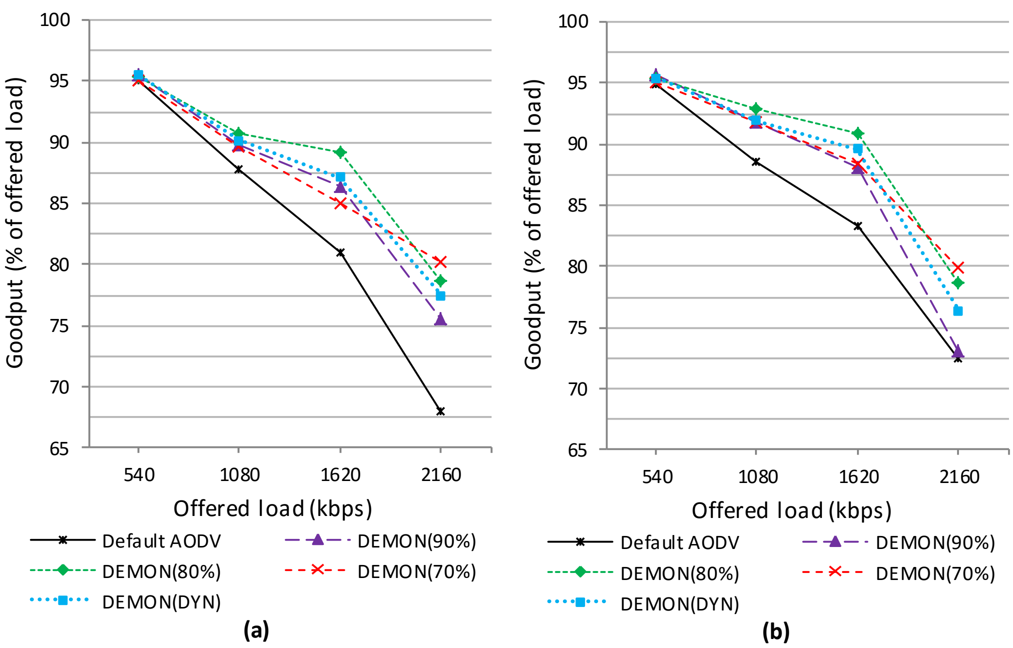


Fig. 5.20: Scenario 5 results: goodput. a) ETT metric for route discovery. b) WCIM metric for route discovery

Once again DEMON outperforms default AODV. Since network congestion is high, the fixed threshold of 80% gives better results than the 90% threshold, which gives rise to a large number of route recoveries even under low load conditions. Furthermore, in this case, the dynamic threshold yields moderate to good performance. On the other hand, for the highest load tested, the best threshold is the 70% one, since the LSR of several links is below 80% due to congestion.

Fig. 5.20 shows that WCIM performs poorly using the 90% threshold when the offered load is high. In general, as has been introduced in the previous scenarios, WCIM obtains worse results under high dynamic conditions. This is the case of mobility, but also when the number of route recoveries is large, as occurs generally with the 90% threshold under high load conditions. In such cases, the inter-flow interference caused by adjacent routes is more complex to consider, since the lifetime of the routes is short.

Finally, Fig. 5.21 illustrates the percentage of duplicated packets (from the total number of received packets) which were received at the destination when using default AODV. As mentioned in Section 5.2.2.1, during pETX computation, DEMON can detect and discard duplicated IP packets at intermediate nodes. This way, as shown in Fig. 5.21, in this scenario a notable amount of useless traffic can be avoided from being transmitted. In the other analyzed scenarios, the percentage of duplicated packets in the worst cases was between 2% and 3%.

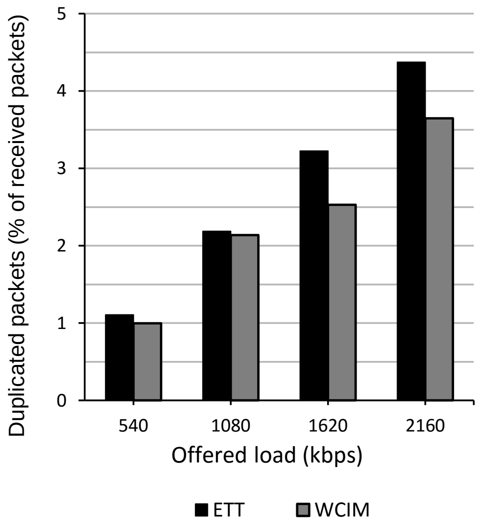


Fig. 5.21 Scenario 5 results: duplicated packets received at the destination by using default AODV.

5.2.3.3.6 Scenario 6: stationary multi-radio grid

The sixth scenario simulates a multi-radio network. Each node has two radio interfaces and randomly chooses two channels from three available orthogonal channels. In this way, due to the pigeonhole principle, it is assured that each pair of neighbors shares at least one common channel. The data rate of all the links is fixed to 6 Mbps to increase congestion. As in the first Scenario, there are 32 flows with random source and destination, and the nodes are stationary and located in a grid topology. The results obtained in this scenario are plotted in Fig. 5.22.

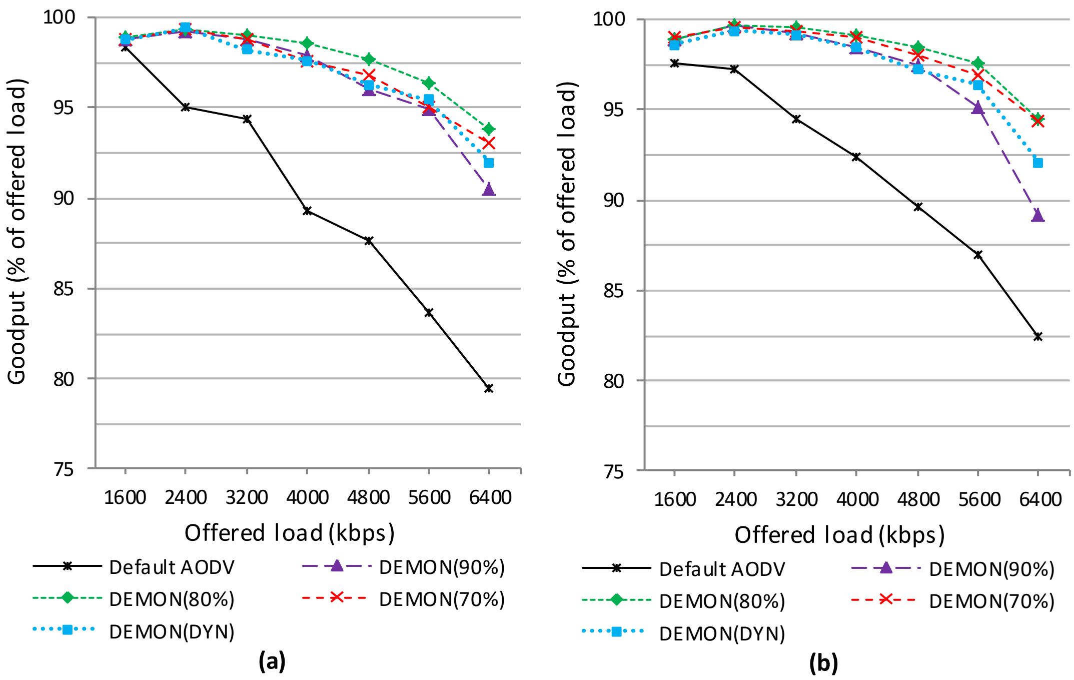


Fig. 5.22 Scenario 6 results: goodput. a) ETT metric for route discovery. b) WCIM metric for route discovery

Results show that DEMON again provides considerably higher goodput than default AODV. Compared with Scenario 1, the offered load can be increased significantly without leading to congestion or inter-flow interference. Due to the use of two different radios (with orthogonal channels) by each node, route recovery has more alternative routes for avoiding interference and congestion than in single-radio scenarios. As in previous scenarios, the different thresholds lead to a similar performance in low load conditions, while in high load conditions the low fixed thresholds give better results since they are better suited to the actual LSR of the links and lead to a lower number of route recoveries.

5.2.3.4 Analysis of DEMON performance with TCP

In the previous scenarios the behavior of DEMON using UDP as the transport protocol was analyzed, where the sources of the flows simply sent data packets in a constant rate, regardless of the network state. TCP, on the other hand, implements different mechanisms in order to adapt the data rate to its view of the congestion state of the network. In this section the performance of DEMON when TCP is used as the transport protocol of the data flows is studied.

Two scenarios are considered. In the first one, an 8x8 static grid with a varying number of TCP flows is simulated, where congestion and interference is the main cause of performance degradation. In the second one, 64 nodes are initially placed in a randomly chosen location, and then move according to the random waypoint model (RWP). In this latter scenario, the number of TCP flows is fixed to four, while the maximum speed of the nodes is varied. WCIM results are based on the passive monitoring extension presented in Section 4.3.2.2.2. Goodput results are illustrated on figures Fig. 5.23 and Fig. 5.25.

Regarding the first scenario, Fig. 5.23 shows that DEMON using ETT improves the performance of the TCP flows, while WCIM results are very similar in all analyzed cases. As discussed in Chapter 4, the benefits of WCIM when routing TCP flows in high congested scenarios are limited.

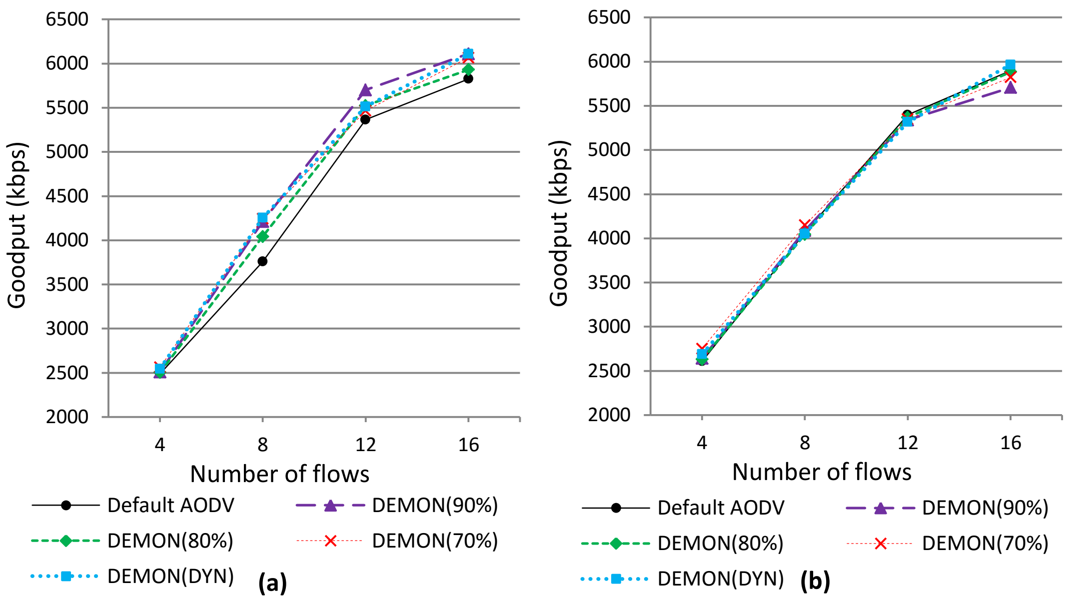


Fig. 5.23: TCP analysis, goodput results of scenario 1. a) ETT metric for route discovery. b) WCIM metric for route discovery

As shown in Fig. 5.24, the number of recovered routes is high even in the first case. Indeed, in this scenario the dynamic threshold leads to the lower number route recoveries. This is a sign of the bad performance of the recovered routes (lower than the 70%), which is mainly caused by the congestion of the own route due to TCP, as shows the fact that the number of recovered routes does not increase, and even decreases, with the number of active flows.

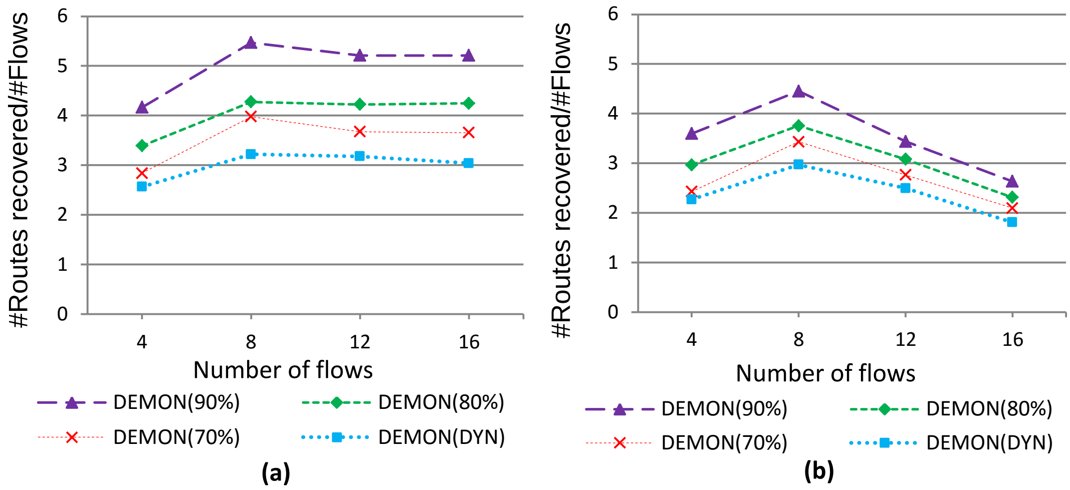


Fig. 5.24: TCP analysis, route recoveries of scenario 1. a) ETT metric for route discovery. b) WCIM metric for route discovery

In the mobility case, Fig. 5.25 illustrates that, for both routing metrics, DEMON benefits the performance of TCP flows. It is remarkable that the performance of the network became improved with the increase of mobility. Since results were obtained from 5 different node distributions, in the stationary scenario some of them were especially detrimental for the flows (i.e. inadequate location of the nodes). On the other hand, low speed improved the connectivity between the nodes and increased the number of available routes, thus leading to a higher goodput. Nevertheless, the scenario is still useful in order to analyze DEMON when routing TCP flows under mobility.

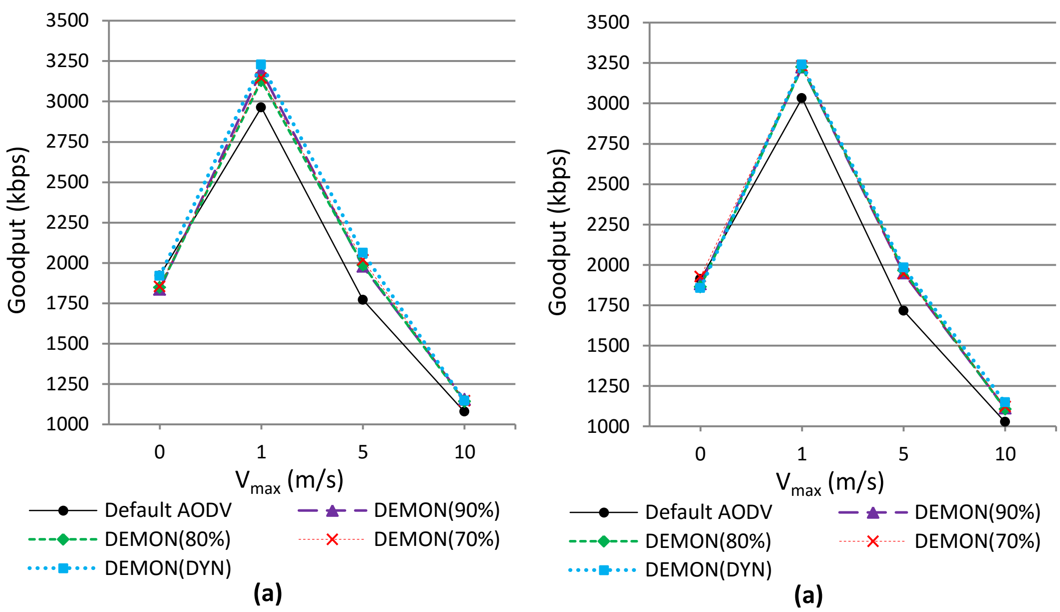


Fig. 5.25: TCP analysis, results of scenario 2. a) ETT metric for route discovery. b) WCIM metric for route discovery.

As in the congestion case, compared to the UDP scenarios analyzed in Section 5.2.3.3, the improvement of DEMON under mobility is less remarkable. It was founded that two of the main mechanisms of the TCP congestion control, the Congestion Window Limit (CWL) and the Retransmission Timeout (RTO), limit the benefits of DEMON. The negative impact of these two mechanisms on performance of multi-hop wireless networks is a well-known problem [75][76]. Due to the inter- and intra-flow interference, the CWL should be set to low values in order to avoid heavy congestion at the MAC layer. In fact, in all carried out simulations the best performance was obtained by using a CWL of 1 maximum segment size, both for basic AODV and DEMON. This was also the case in other state-of-the-art studies [76]. On the other hand, TCP RTO is frequently triggered in wireless multi-hop networks due to transmission errors. In such case, the exponential increase of TCP RTO as a congestion control mechanism is unnecessarily activated, which reduces significantly the sending rate of TCP sources despite absence of congestion [149].

In the simulations, the combination of these two phenomena causes the source node sending rate to decrease down to values in the order of one packet per second (i.e. the minimum TCP RTO). This situation limits the applicability and accuracy of DEMON, which is based on traffic monitoring, since very few or even no packets are transmitted in some Hello cycles. This is especially detrimental in the mobile scenario, whereby detecting the presence of nodes in a gray zone cannot be done as rapidly as in the UDP scenarios, but also occurs in the first scenario, leading to a reduction of the number of recovered routes with increasing load. In addition, this issue also impacts the passive monitoring extension of WCIM, leading to unstable load estimations and limiting its benefits, as shown in the results of these two scenarios.

Compared to other state-of-the-art solutions, in mobile TCP scenarios, DEMON results, which achieves in average 5%-10% of goodput increase, are slightly worse than those of CPDSR and LAW (see Table 5.2). Since the link quality estimation mechanism of CPDSR and LAW is based on the received power of data packets, they are less affected by the data rate decrease due to TCP congestion control: a single received packet under the received power threshold is taken as a sign of mobility and triggers route recovery. However, note that both CPDSR and LAW are applied to the DSR routing protocol and use cache-enabled route recovery, which improves their results [140].

5.3 Conclusions

Contributions of this chapter focus on the benefits of preemptive route recovery strategies for on-demand routing protocols in MIWNs. By default, reactive routing protocols rely on link break detection in order to recover active routes, leading to large intervals of performance degradation and even disconnections. Therefore, preemptive recovery aims to anticipate link breaks by monitoring the quality of the links and recovering routes before disconnection occurs. However, state-of-the-art preemptive route recovery mechanisms are mainly designed with the objective of detecting node mobility, while, as analyzed in previous chapters, other phenomena like inter-flow interference or congestion can severely compromise the performance of active flows. This fact motivates the design of the DEMON proposal.

DEMON, which has been designed as an extension to FB-AODV, uses pETX, a link-quality metric based on a passive estimation of link data loss rate for monitoring the performance of active links. When a node detects that link quality falls below a threshold (which can be statically or dynamically configured), route recovery is triggered in order to find a new route for the affected flow whose recovery optimizes network performance. DEMON performs preemptive, source-based route recovery due to any cause of link quality degradation. In contrast with state-of-the-art solutions, DEMON can operate regardless of the link layer implementation since it only uses information available at the network layer.

The performance of DEMON is studied by means of simulation, to which end a wide range of scenarios is considered, each of them with particular characteristics in terms of offered load, number of flows, spatial node distribution, link rates, mobility and use of single- or multi-radio nodes. According to the results, DEMON outperforms default AODV in all the scenarios of the evaluation due to its preemptive recovery of degraded routes. In mobile scenarios, DEMON can provide an increase of up to 90% of goodput by anticipating link breaks and minimizing route disconnections. The improvement is equal to or greater than that achieved by state-of-the-art preemptive solutions according to the literature. In stationary networks the average improvement is smaller, about 10%-30%, since as load increases congestion and interference leave little margin for improving performance by changing the flow distribution in the network. In absence of mobility, the performance of other state-of-the-art preemptive solutions would be analogous to that of default AODV.

With regard to the link quality thresholds used in DEMON, fixed thresholds set to high values obtain good results under low load or high mobility conditions, since they provide a fast reaction to performance degradation. However, in congested networks, fixed thresholds set to high values may lead to excessive route recoveries, which become counterproductive. On the other hand, fixed thresholds set to low values are less sensitive to performance degradation under low load or high mobility; however, under high load, they are more consistent with actual link qualities and thus give rise to a low number of route recoveries, which leads to good performance. In most considered cases, the best performance is obtained by using a fixed threshold appropriately tuned to the scenario. Nevertheless, the dynamic threshold performs reasonably well in all the scenarios and load conditions.

The behavior of DEMON is analyzed when two different state-of-the-art routing metrics are used for route discovery, ETT and WCIM, which are link-quality and load-aware, respectively. In most cases, WCIM obtains better results than ETT, since its load-awareness leads to better route selection. However, results show that, in some cases, the performance of DEMON improves by using the ETT metric for route discovery. This is an interesting feature, since the use of load-aware metrics can lead to network instability under highly variable network conditions. By using DEMON, the routing metric can remain load-unaware, as ETT is, while route recovery can be load-aware by means of the link quality estimation mechanism based on pETX. In fact, according to the obtained results, it can be concluded that in these scenarios the route recovery mechanisms have a greater influence on the performance of the routed flows than the routing metrics used for route discovery. This is remarkable, since the state-of-the-art on preemptive and route recovery solutions is scarce compared to the wide literature on routing metrics and route discovery solutions.

The performance of DEMON in combination with TCP congestion control mechanisms is also analyzed. DEMON can provide an average increase of up to 5%-10% of network goodput in the presence of TCP flows. However, DEMON benefits are limited by the congestion control mechanisms of TCP; thus, additional cross-layer mechanisms are needed. One possibility is providing DEMON with mechanisms at the end nodes capable of monitoring the state of TCP algorithms, in order to identify signs of performance degradation, such as the number of TCP retransmissions or RTO variance. On the other hand, it would be interesting to evaluate DEMON when improved TCP mechanisms are used. These include state-of-the-art TCP modifications designed for wireless multi-hop networks, like the use algorithms to distinguish the cause of RTO expirations [149] or to adapt the value of the CWL [150]. These studies are left for future work.

As analyzed for the case of the higher fixed thresholds, an elevate number of route recoveries can compromise the stability of the network. Future work includes studying other dynamic strategies for setting the threshold, for instance varying it according to the cause of the degradation: e.g.

mobility, node congestion, interference caused by active flows, temporary fluctuations of the radio channel…

Also, from the analysis of the results, it can be concluded that one of the main drawbacks of DEMON is its route recovery procedure. Alerting the source and starting a new route creation phase requires a non-negligible amount of time and signaling overhead, which can limit DEMON benefits in congested or very dynamic scenarios. Next chapter will introduce a DEMON enhancement which makes use of channel assignment in multi-radio networks in order to avoid the route recovery phase.

6

Channel assignment in multi-radio MIWNs

The IEEE 802.11 standard defines multiple channels, some of them orthogonal to each other. This fact, combined with the increasing availability of multi-radio devices, permits considering channel assignment into routing procedures.

Channel distribution can be seen as another parameter to be integrated into the routing metric. This way, as analyzed in Chapter 4, channel diversity along the paths can be favored in order to decrease contention and interference. In such proposals, there is an algorithm assigning channels independently of the routing protocol, while the routing metric considers channel information as a cross-layer parameter.

However, since the channel assignment of a network defines the available routes and the interference between adjacent links, in recent years many CAA proposals have focused on joining routing and channel assignment in order to maximize throughput. But this adds complexity to the algorithms due to the circular dependency between routing and channel assignment, limiting its application in real deployments.

The first section of this chapter introduces the basics of channel assignment in multi-radio MIWNs, paying special attention to the different problems and trade-offs than can affect the performance of the flows. Also, the most significant proposals of the state-of-the-art are discussed. Next, two proposed solutions are presented and analyzed: first, a Dynamic Channel Assignment (DCA) algorithm which assigns channels considering the load and interference of the active flows of the network; secondly, an extension of the DEMON routing maintenance solution presented in Chapter 5, which permits channel reallocation when performance degradation is monitored. Finally, the last section of this chapter presents the conclusions.

6.1 Channel Assignment in multi-radio MIWNs

Chapter 3 introduced some of the benefits and problems of multi-radio routing. The main objective of channel assignment algorithms is to minimize contention and interference in order to maximize the throughput of MIWNs [25][26]. However, as was shown in Fig. 3.16, there is a trade-off or circular dependency between channel diversity and network connectivity, leading to a NP-hard problem when trying to find an optimal solution in order to minimize the interference of the network [99]. In addition, channel assignment should deal with complexities related with the multi-hop nature of MIWNs, like assuring broadcast and avoiding deafness [27], and hardware limitations of nowadays NICs, like the non-negligible channel switching delay [102] or the cross-channel interference between theoretically non-overlapping channels [96][97]. Also, CAAs can suffer of ripple-effect problem or a non-convergent behavior, compromising the stability of the network [28].

CAAs can be classified according to the frequency with which the assignment is modified [27][100]. In fixed assignments, the radio interfaces remain in the same channel permanently or for long periods of time. Although usually leading to more stable topologies and minimizing overhead, fixed assignments do not react with network dynamics, like mobility or the arrival of new flows [100]. On the other hand, dynamic approaches permit frequent channel reassignments which can deal with these variations. However, very dynamic reassignments (e.g. in a per-packet basis) are not possible due to the channel switching delay of NICs. Also, they can lead to broadcast and deafness problems if appropriate coordination mechanisms between neighbors are not implemented [27]. Finally, hybrid CAAs aim to mitigate the limitations of both fixed and dynamic assignments; at least one interface of the nodes is fixed to a channel in order to facilitate coordination, while the rest can be reassigned in a dynamic way [100]. Indeed, some hybrid proposals assign a common channel to one fixed interface of all the nodes in order to assure connectivity and signaling [99][101]. In general, most state-of-the-art CAAs solutions are hybrid or semi-dynamic (i.e. channel assignment is recomputed periodically).

Other basic classification of CAAs considers centralized and distributed approaches [151]. Centralized solutions make use of a global view of the network in order to obtain a channel assignment that maximizes the throughput of the network. On the other hand, in distributed solutions only local information is exchanged between neighbors in order to obtain a channel assignment which permits communication and reduces local interference. Next subsections introduce significant state-of-the-art centralized and distributed CAAs.

6.1.1 Centralized solutions

In centralized approaches, the channel assignment is performed by a central entity (e.g. a gateway or an external server) applying an algorithm which uses global information of the network. The usual input parameters of this type of algorithms are the number of nodes, the number of available channels, the interfaces per node and the interference or conflict graph of the network [28][151]. Also, solutions aiming to join routing and channel assignment consider a prior knowledge of the traffic pattern of the network (i.e. the sources, the destinations, the load of the flows, etc.). Due to these requirements, centralized solutions are usually complex or less practical to implement, but can can offer an upper bound of performance [151]. In fact, most state-of-art centralized solutions do not offer a discussion on how the central entity obtains all the required parameters to apply the algorithm or how channel assignment and traffic performance is affected by network dynamics (e.g. link failures, nodes joining/leaving the network, traffic variations, etc.).

In general, centralized solutions make use of graph-based heuristics [28][152]. As shown in Fig. 6.1a, the connectivity graph represents the topology of the network, where nodes are the vertices of the graph and the links are the edges. Then, an interference or conflict graph can be created, where the vertices are the active links and the edges represent an interfering relationship. The conflict graph depends on the interference model being applied [152]; for instance, Fig. 6.1b considers that links interfere up to two hops of distance. This way, the amount of interference can been seen as the number of edges of the conflict graph and the CAA should minimize this number considering the number of available channels and radio interfaces. However, as proved in [99], resolving this problem is NP-hard. Therefore, most CAAs are based on heuristics.

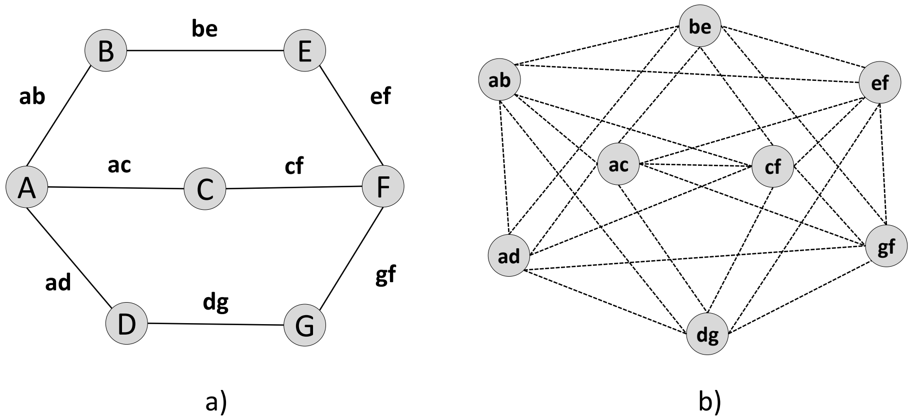


Fig. 6.1: Centralized Channel Assignments: (a) Connectivity and (b) Conflict graphs

Authors in [153] propose a single pass greedy heuristic algorithm to obtain a channel assignment which minimizes interference while preserving the links of the original connectivity graph. The algorithm starts from a common channel assignment and then, ordered by a priority (e.g. the number or radio interfaces), nodes greedily assign channels to its interfaces. During algorithm execution, the priority of the nodes without free radios is dynamically set to the maximum value in order to preserve topology, leading to a recursive algorithm.

On the contrary, in [154] an iteration-based algorithm using Tabu search is proposed. The algorithm starts from a random assignment for all the links without considering radio constraints (i.e. the number of radios of the nodes). Then, in each iteration, it creates a defined number of alternatives which only differ on the assignment of one link and selects the one which minimizes interference. After a defined number of iterations, the best case is selected. Finally, the algorithm selects the nodes which violate radio constrains and merges the different channels of its links in order to obtain a solution which can be applicable.

In [101], a breadth-first search CAA is proposed, using gateways as the root of spanning trees. Starting from the gateway, channels are assigned trying to minimize the interference between links. Links are prioritized based on their distance in hops to the gateway and then sorted by their ETT metric. In addition, all nodes assign a common channel to one of its interfaces in order to preserve topology and use it as backup channel during channel reassignment. The common channel is the one which minimizes interference with external networks.

Centralized CAA focused on joining routing and channel assignment needs information about the expected flows or routes of the network in order to maximize its throughput. For instance, by using traffic patterns, the algorithm proposed in [99] estimates the expected load on the links of the network and gives an initial channel assignment in order to support these conditions. Channel assignment is performed by using a greedy algorithm to minimize interference with link prioritization based on the expected load. Then, by means of a path creation strategy based on load balancing, the algorithm evaluates if the created routes can serve the expected load. Otherwise, the channel assignment is done again and the whole process is repeated. The algorithm iterates until no better routes and channel assignment can be found. Fig. 6.3 illustrates the procedures performed in [99] in order to obtain a valid CAA.

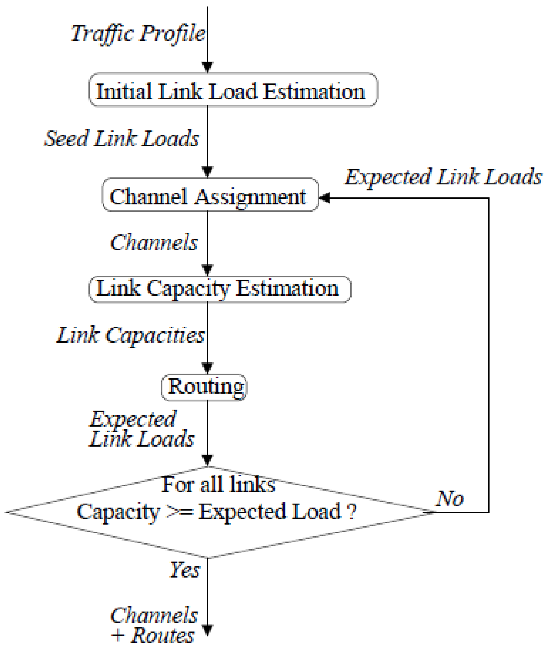


Fig. 6.2: Flowchart of the CAA defined in [100]

In general, considering the routes and load of the flows adds complexity to the CAA algorithms. For instance, [155] makes use of Linear Programming methods in order to resolve the joint routing and channel assignment problem.

Finally, some centralized CAAs make use of neighbour partitioning, where each node partitions its neighbours into groups and assigns each group to a channel and interface. In addition, channels are distributed in order to minimize interference [99]. This scheme requires a centralized way to partition neighbors that results in a uniform channel assignment across the network. Fig. 6.3 shows an example of the application of this type of CAA to a grid topology (hereinafter, Grid Channel Assignment or GCA).

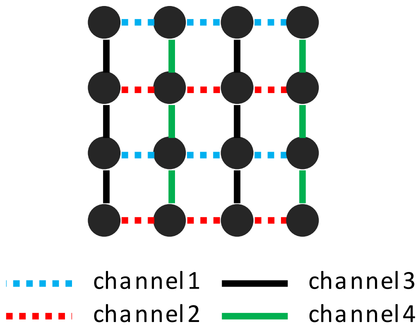


Fig. 6.3: Example of a neighbor partitioning CAA in a grid topology with 2 radios and 4 channels.

6.1.2 Distributed solutions

While centralized algorithms can give an upper bound on performance, distributed approaches are usually more practical to implement and more adaptable to different environments where obtaining a global view of the network is not feasible or realistic [151]. Oppositely, in distributed solutions only local information is exchanged between neighbors in order to obtain a channel assignment which permits communication and reduces interference.

The simplest distributed solutions are the Common Channel Set (CCS) and Random Channel Assignment (RCA). These solutions are usually combined with channel- and load-aware routing metrics in order to minimize the interference of active routes; indeed, channel-aware routing metrics can be seen as a way of assigning channels [151].

CCS consists on statically assigning the same set of channels to all the nodes of the network [43]. This way, the connectivity of the network is identical as the single-channel single-radio case, but the capacity of the network is increased due to the additional interfaces. However, when the number of available channels is higher than the number of interfaces (i.e. in the most common scenarios), more advanced channel assignment strategies obtain better performance by increasing the channel diversity of the network.

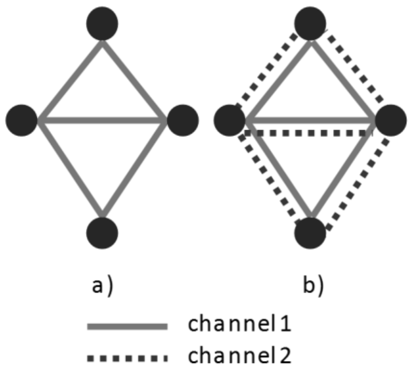


Fig. 6.4: Example of CCS assignment. a) Single-radio single-channel; b) CCS with 2 radios and 2 channels

In order to improve CCS performance, instead of relying on routing decisions in order to select the channel to be used, some proposals implement a driver which dynamically and transparently decides the best channel/interface to be used in the transmissions to a specific neighbor according to the perceived quality of the channel [156][157].

On the other hand, using RCA each node selects randomly one of the available channels for each one of its interfaces. This type of static assignment is fully distributed, since there is no need to exchange information between nodes. However, it only preserves the connectivity of the network if the number of available channels is less than two times the number of interfaces. In such a case, due to the pigeonhole principle, all neighbor nodes will share at least one common channel, as shown in Fig. 6.5a. Otherwise, as shown in Fig. 6.5b, network partitioning can occur. Even in cases where connectivity is assured, RCA does not guarantee that the interference is minimized or that assigned channels will be useful (e.g. channel 3 of the upper node of Fig. 3b). However, it offers higher channel diversity than the CCS solution even with routing metrics which are not aware of channel assignment.

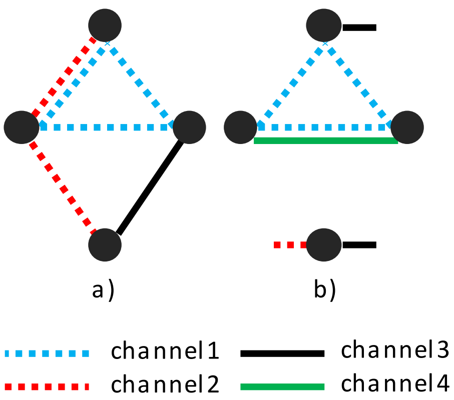


Fig. 6.5: Random Channel Assignment. a) 2 radios and 3 channels. All nodes are connected through at least one channel; b) 2 radios and 4 channels. The bottom node does not share any channel with its neighbors and is disconnected from the network.

As in the centralized case, more complex solutions make use of heuristic algorithms in order to obtain a channel assignment which minimizes interference locally. This is the case of the greedy algorithm presented in [154], where each link is owned by a node (the one with the highest priority) which tries to locally reduce interference considering its conflict graph. The algorithm considers the radio constraints of both nodes forming the links and reassignments are not allowed in order to avoid ripple-effect. Assigned channels are confirmed by using a three-way handshake and propagated through the n-hop neighborhood in order to update the conflict graphs.

In [158], in order to preserve connectivity, one interface is fixed to a common channel. The rest of interfaces are assigned dynamically, where each node selects the channel which minimizes its interference using only local information (the channel selection of the other nodes within its interference set). In order to avoid dead interfaces (i.e. an interface assigned to a channel which is not shared with any neighbor), at least one neighbor should share the same channel to allow the new assignment. The algorithm converges to a solution since interference is proved to decrease monotonically with each channel assignment.

A hierarchical distributed solution is proposed in [159] for scenarios where traffic is destined to the Internet through some nodes defined as gateways. Spanning-trees rooted at the gateways define the routes of the network. According to the formed spanning trees, each node will have one upstream interface (to the parent) and, if available, downstream interfaces (to the children). Then, starting from the nodes closer to the gateway, parent nodes assign the less loaded channels to their downlink interfaces. According to route dynamics, channel assignments are periodically readjusted.

In [160], a receiver-based distributed channel assignment solution for networks with at least two interfaces per node is proposed. Each node assigns a fixed channel to one of its interfaces, which will be used for data reception. Fixed channels are announced in order to minimize its reutilization by other nodes in the neighborhood (i.e. each node tries to select as reception channel the less used or loaded one) and to permit communication. The rest of the interfaces are used for transmissions and change dynamically according to the channel of the receiver. In order to avoid the channel switching time problem [102], senders queue the packets according to receiver's channels and serve each queue sequentially. Broadcast packets should be transmitted through all available channels in order to assure signaling flooding.

6.2 Proposed approach

As has been illustrated in the results presented in previous chapters, proper route creation and recovery procedures can improve the performance of traffic flows in multi-radio networks; the WCIM routing metric is able to distribute the load through the different active channels in order to alleviate interference, while the DEMON mechanism can detect degraded channels and change active paths in order to avoid them. However, as pointed out in the previous sections of this chapter, channel distribution has a significant impact on the topology of the network, affecting the availability of the routes and, therefore, the performance of the flows.

A first approach in order to improve performance in multi-radio networks is to design a CAA which fits well with WCIM and DEMON mechanisms. Therefore, it should satisfy the following requirements:

- Distributed: a distributed solution is preferred in order to obtain a practical solution which can be applied in a variety of environments where a global view of the network is not always feasible.
- Dynamic: channel assignment should vary in time according to network conditions. This comprehends changes of topology (e.g. mobility, node activation/deactivation, link breaks, etc.) and interference-awareness.

The designed CAA, called Interference-based Dynamic Channel Assignment (IDCA), will be presented and analyzed in Section 6.2.1.

A second approach relies on joining channel assignment and routing procedures. As has been previously discussed, joining route creation and channel assignment is complex due to the circular dependency between both mechanisms. In fact, there is not any practical and implementable way of assigning channels during route creation due to the isotonic property discussed in Section 4.2: intermediate nodes cannot decide the best channel and interface for a new flow without knowing the rest of the path. Therefore, some CAAs presented in previous sections use traffic patterns and precomputed routes in order to obtain heuristic solutions.

Section 6.2.2 introduces an alternative way of joining routing and channel assignment procedures based on route recovery instead of route creation. This approach is designed as an enhancement of DEMON, which, instead of recovering degraded routes from the source, permits the nodes forming the degraded link to negotiate an alternative channel using other available interfaces and channels. This version of DEMON is called Multi-Radio DEMON (MR-DEMON).

6.2.1 Interference-based Dynamic Channel Assignment

The main objective of the IDCA algorithm is to dynamically change the channels assigned to the interfaces according to the perceived interference and the topology of the network. The algorithm is executed in a distributed and greedy way by each node of the network.

First of all, the algorithm should assure the connectivity of the network in order to avoid network partitions. A common strategy in distributed algorithms is to assign a common channel to one of the interfaces of all the nodes [101][158]. This condition facilitates the different procedures of the routing protocol, like neighbor discovery or the flooding of signaling messages. Also, compared to other multi-radio solutions, it permits the routing protocol to access to a greater set of available routes (i.e. the same set of the single-radio case), which can avoid performance problems, including disconnections, in dynamic conditions caused by mobility, interference or link-quality degradations.

On the contrary to other state-of-the-art solutions [101], in IDCA the common channel can be used to route traffic flows. In fact, this is the only way to permit nodes with a single interface to join the network. In order to avoid congesting the common channel, routing metrics can penalize its usage in front of other available channels.

Then, IDCA algorithm assigns the rest of channels to the other interfaces of the nodes in the following way, which is also illustrated in Fig. 6.6:

- First, non-common interfaces are assigned following a simple CAA algorithm, like RCA or CCS.
- Nodes periodically compute which is the best available channel for the non-common interfaces. In order to avoid channel switching delays and packet losses, only free interfaces (i.e. not traversed by active routes) are considered by the dynamic assignment mechanism.
- The best channels are decided according to the following rules:
    1. The less loaded or interfered channel is selected taking into account the load of the nodes with active routes within the two-hop neighborhood of the node. In a similar way to the WCIM routing metric case, the interference is defined as a percentage of channel occupancy (see Equation 4.23) and weighted according to the position of the nodes: the load of the one-hop neighbors is multiplied by 2, while the load of the two-hop ones only by 1.
    2. If two or more channels are equally interfered or not interfered, the best channel is the one which connects the node with a number of neighbors which is closer to the value N_{opt} and different of zero. This value is defined as the total number of neighbors divided by the number of interfaces. This procedure is similar to the performed by neighbor partitioning mechanisms.

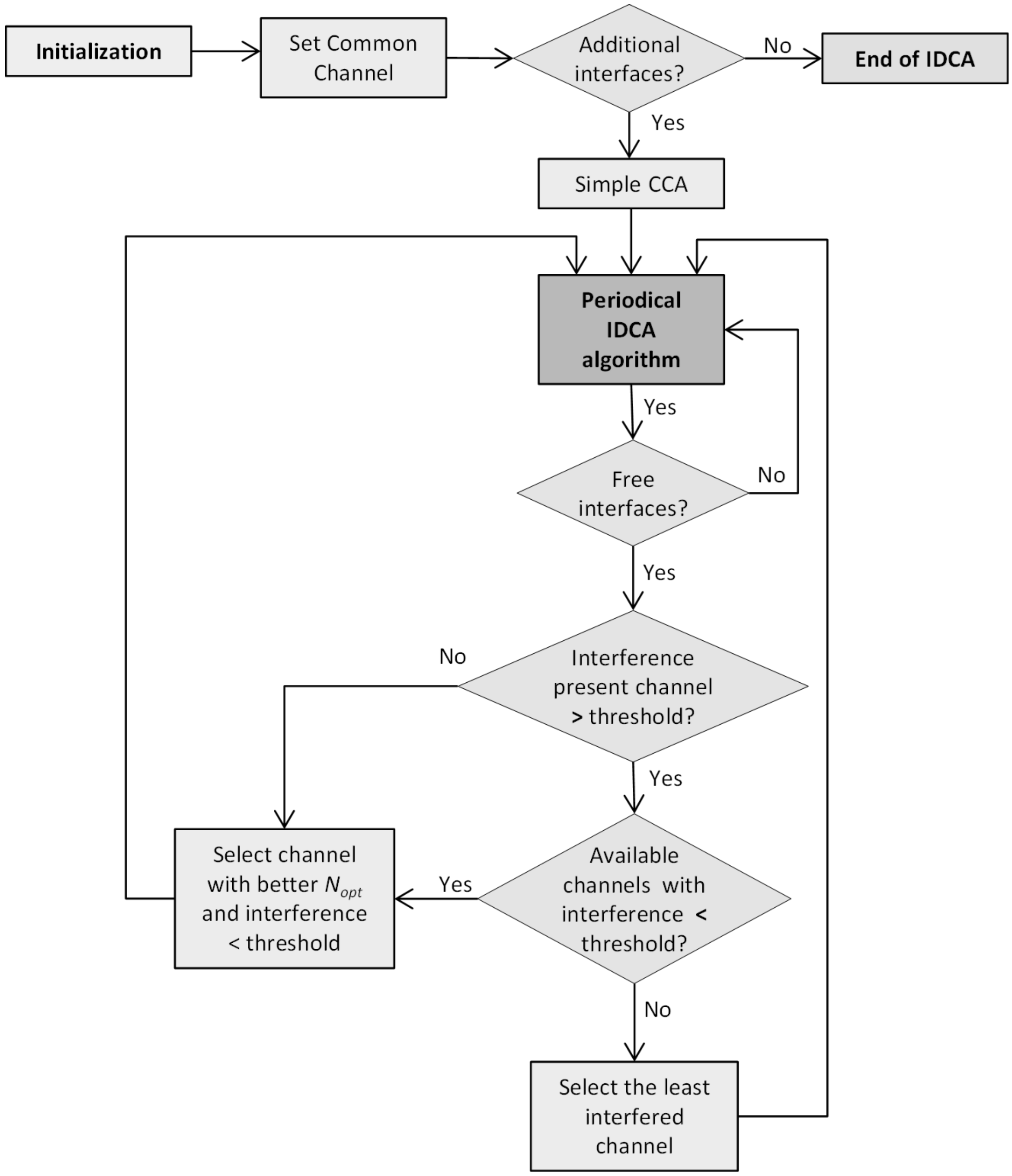


Fig. 6.6: IDCA algorithm chart

When using RCA as initial channel assignment and in absence of traffic, IDCA tends to distribute the channels of non-common interfaces in zones due to the definition of N_{opt}. This channel distribution is similar to the one performed by clustering protocols, where the common channel is used in order to traverse links between nodes in different "clusters". This is illustrated in Fig. 6.7.

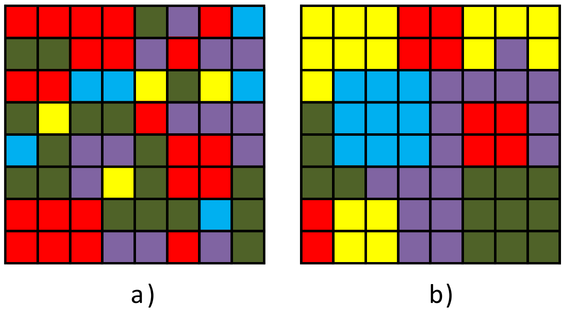


Fig. 6.7: Channel allocation of the non-common interface in a grid of 8x8 nodes with 2 interfaces and 6 available channels (1 common, 5 dynamic). The different colors represent the 5 different channels. a) Initial allocation using RCA. b) Final allocation after applying IDCA.

On the other hand, when the initial assignment is based on CCS, since any channel reassignment will break the condition of having at least one neighbor, CCS is preserved until interference is noticed (i.e. new routes are created). As illustrated in Fig. 6.8, this will tend to distribute channels according to the routed flows.

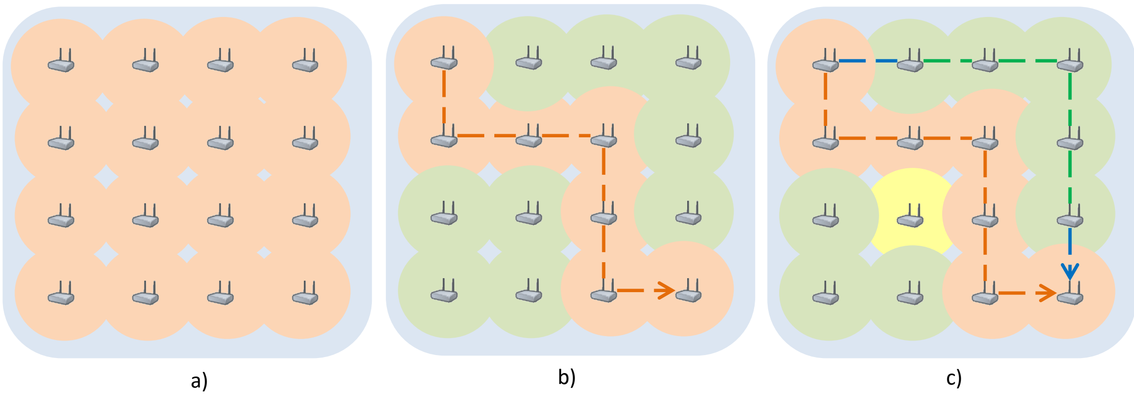


Fig. 6.8: Channel allocation of the non-common interface in a grid of 4x4 nodes with 2 interfaces and 4 available channels (1 common, 3 dynamic). The different colors represent the 4 different channels (the common channel is the blue one). a) Initial allocation using CCS. b) IDCA reassigns channels due to the interference of the first flow. c) New channel reallocations are performed due to the arrival a new flow. Note that the common channel is used between nodes which do not share any other channel.

Regarding the stabilization and convergence of the algorithm, in IDCA nodes can only perform one reassignment per period and periods are jittered to minimize simultaneous decisions between neighbor nodes. In addition, a minimum interference threshold is considered to avoid channel reassignments because of small interference variations. Finally, since only free interfaces are considered by the algorithm, the possible presence of unstable assignments would only limit the number of alternative routes for a new flow. In any case, unstable situations have not been noticed during the evaluation of IDCA.

Next section analyzes the performance of IDCA in different scenarios.

6.2.1.1 Performance analysis

For the evaluation of IDCA, three practical channel assignment solutions were selected: CCS, RCA and GCA. Their performance in different scenarios was compared to the case of IDCA combined with these solutions (as initial channel assignment). The basic simulation scenario is based on the grid of 64 nodes detailed in Section 2.2.3.3 (Fig. 2.14 and Table 2.9). The link bit rate of the nodes is fixed at 12 Mbps. Simulated traffic is UDP, CBR and unidirectional. Results are the average of 10 simulations.

The WCIM routing metric is used for path creation. In order to discourage the selection of the common channel, a node receiving a RREQ through a link assigned to the common channel "artificially" increases the current load of this link in a 25% (i.e. its CN^i parameter as defined in Equation (4.26)).

Regarding the stability of IDCA, the threshold which allows channel reassignments based on the interference is fixed to a 5%. The period of the IDCA is determined by using a uniform random distribution within the interval [15, 20] seconds. In particular, unstable configurations were not noticed during the realization of the simulations.

6.2.1.1.1 Scenario 1: 64 flows, random node spatial distribution

In the first scenario the nodes were statically located in the simulation area using a uniform random distribution. At a random time between second 100 and 300, each node initiated a flow of 250 kbps and 300 seconds of duration with a random destination. Thus the maximum offered load to the network was 16 Mbps. Fig. 6.9 shows the goodput of the analyzed channel assignment solutions with 2 interfaces per node and up to 6 available channels.

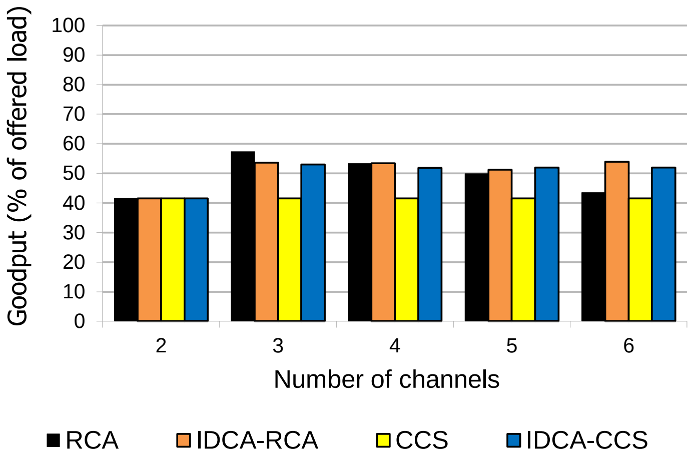


Fig. 6.9: IDCA's analysis: Goodput obtained in Scenario 1 using 2 interfaces.

Results show that the maximum goodput is obtained with RCA when 2 interfaces and 3 channels are used. In such a case, due to the pigeonhole principle, the network connectivity is preserved and RCA combined with the WCIM routing metric offers an efficient channel allocation, as shown Fig. 6.10a. This figure shows the percentage of the total number of links used during communication (i.e. hops selected by the routing protocol) that use each different channel. In the case of 3 channels RCA obtains a totally equitable distribution, which favors high throughput because of less interference between the active flows. However, as the number of channels increases, the goodput of RCA decreases due to disconnected nodes and network partitioning. On the other hand, the channel assignment based on CCS yields the worst results. Since only two fixed channels are used, they become easily congested by traffic load. As shown in Fig. 6.10b, WCIM distributes the load equally between the two available channels.

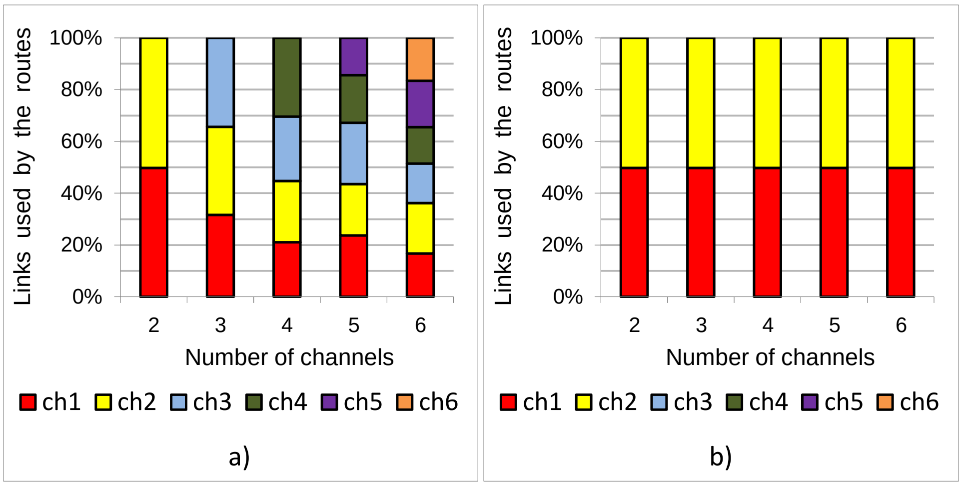


Fig. 6.10: IDCA's analysis: Channel allocation in Scenario 1 (2 interfaces). a) RCA and b) CCS

The IDCA solution obtains similar throughput results by using RCA or CCS as the initial channel assignment, although they lead to different channel allocations, as shown in Fig. 6.11. The common channel has a utilization between 40% and 50% in all the cases, which, compared with RCA, induces more congestion in cases where connectivity is assured (3 channels), but avoids network partitioning with a higher number of channels. On the other hand, compared to CCS, IDCA-CCS can use more available channels due to its dynamic allocation, obtaining better results in all the cases considered.

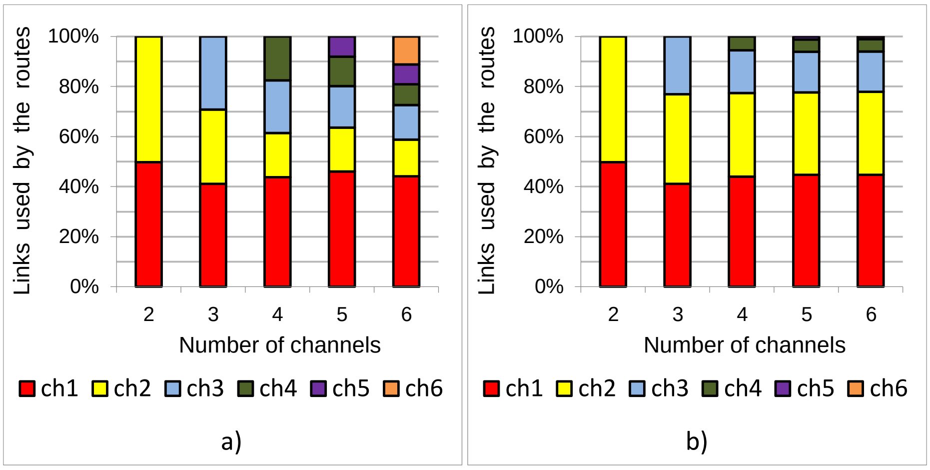


Fig. 6.11: IDCA's analysis: Channel allocation in Scenario 1 (2 interfaces). a) IDCA-RCA and b) IDCA-CCS

Compared to IDCA-RCA, IDCA-CCS tends to increase the use of the 3 first channels due to its initial allocation. However, since the number of interfaces is limited (only one dynamic channel is available) and congestion is high, in this scenario higher channel diversity does not lead to a significant better performance.

Fig. 6.12 shows the results when three interfaces are used. In this configuration, IDCA-RCA obtains the best results in all the cases.

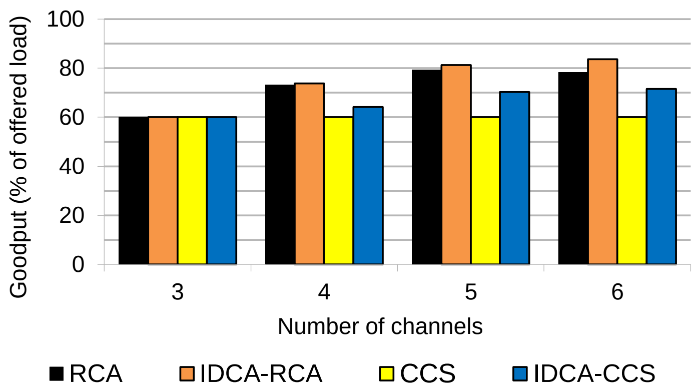


Fig. 6.12: IDCA analysis: Goodput obtained in Scenario 1 using 3 interfaces.

As illustrated in Fig. 6.13, the additional interface leads to a lower utilization of the common channel thus decreasing congestion. Indeed, using IDCA-RCA the routes are distributed almost equitably through all available channels. On the other hand, IDCA-CSS leads again to a higher utilization of the three first channels, which in this case is detrimental, as shown in Fig. 6.12; the additional interface increases the number of available links and, thus, the benefits of channel diversity.

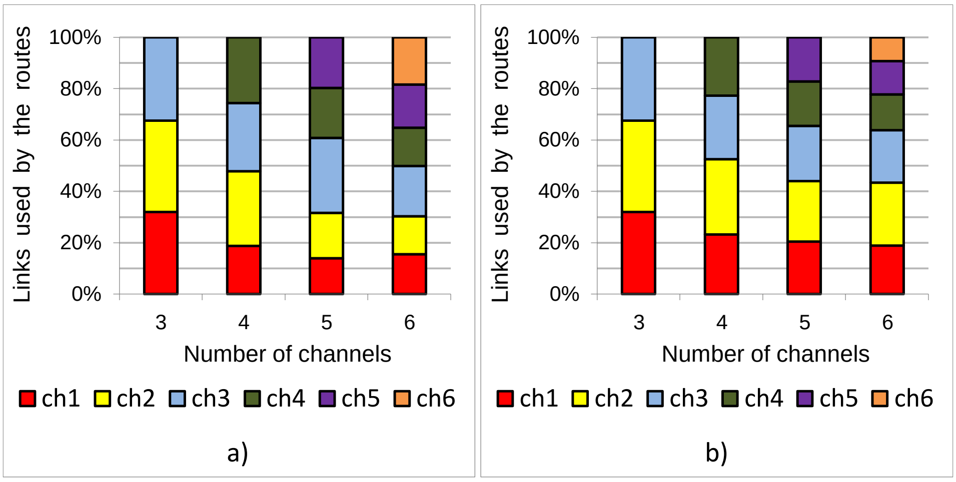


Fig. 6.13: IDCA analysis: Channel allocation in Scenario 1 (3 interfaces). a) IDCA-RCA and b) IDCA-CCS

Finally, Fig. 6.14 illustrates the impact in performance of using a common channel, where RCA-CC stands for RCA with one interface dedicated to the common channel. As shown in the figure, the utilization of the common channel degrades the performance of RCA in all the cases. However, by dynamically allocating the rest of the interfaces, IDCA compensates this degradation and even outperforms RCA in some cases.

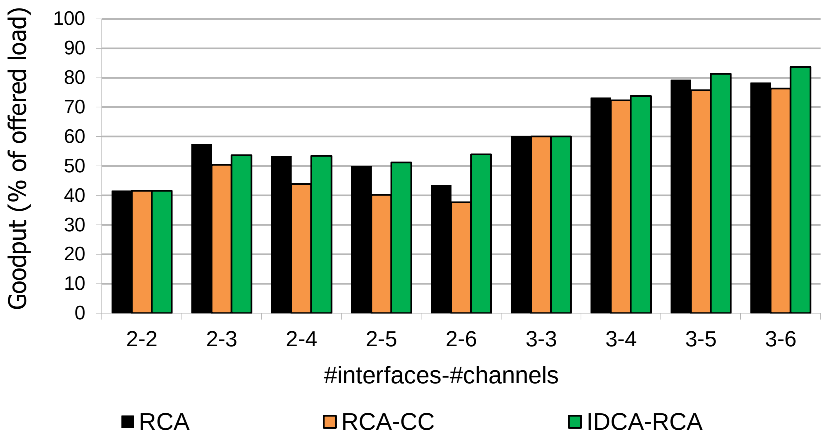


Fig. 6.14: IDCA analysis: Goodput obtained in Scenario 1 by using different versions of RCA

6.2.1.1.2 Scenario 2: 64 flows, grid distribution

In this scenario, the nodes were located in a regular grid topology of 8 x 8 nodes, with a distance between consecutive nodes in the same row or column of 140 meters. The traffic pattern was identical to the one in the previous scenario. Fig. 6.15 shows the goodput of the analyzed channel assignment solutions with 2 interfaces per node and 2 to 6 available channels.

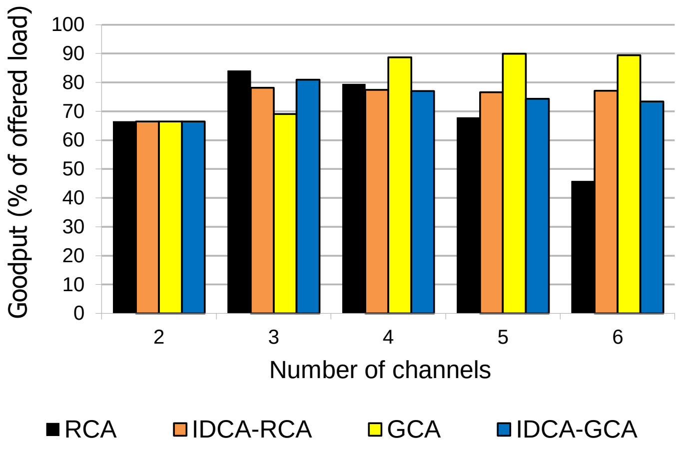


Fig. 6.15: IDCA analysis: Goodput obtained in Scenario 2

Again, RCA obtains the best results with 3 channels, but performance becomes degraded due to disconnected nodes when the number of channels increases. On the other hand, IDCA obtains a similar goodput in all the analyzed cases by using the common channel for preserving the connectivity and the dynamic assignment of the other channels for avoiding congestion. As expected, in this case the GCA obtains the best results for 4 or more channels, since the channel assignment was planned and optimized for this topology (i.e. centralized assignment based on neighbor partitioning) and the routing metric can take profit of it.

6.2.1.1.3 Scenario 3: 7 flows, random node spatial distribution

In this scenario the nodes were located again using a uniformly random distribution. However, in this case, there were 7 active flows with random source and destination. The first flow started at second 100 and then every 20 seconds a new flow was initiated. The data rate of each flow was 1500 kbps. The following figures show the results during the time interval in which all the flows were active (i.e. the total load offered to the network was 10.5 Mbps).

Fig. 6.16 shows that in this scenario IDCA obtains the best results. Since the number of flows is lower, the routing protocol has more available paths using free interfaces and the common channel is less congested. Therefore, the dynamic channel assignment mechanism of IDCA has more chances to select less interfered channels even in the case of 2 interfaces. Indeed, in this scenario it is very noticeable how the availability of additional channels significantly improves the performance of the network compared to the case of 2 channels and 2 interfaces.

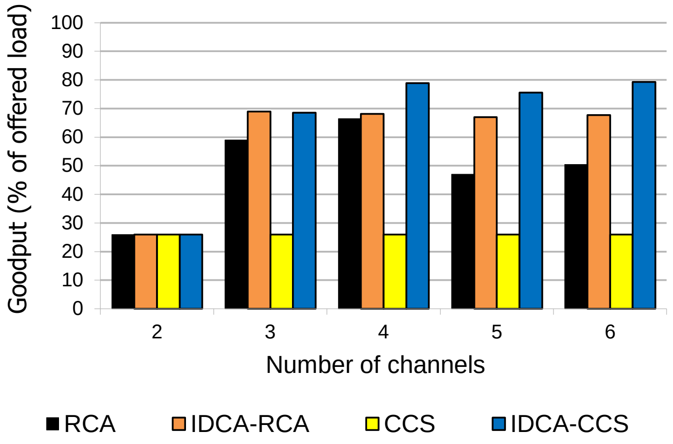


Fig. 6.16: IDCA analysis: Goodput obtained in Scenario 3 using 2 interfaces

As aforementioned, Fig. 6.17a shows that the use of the common channel of IDCA-RCA has decreased a little compared to previous scenarios. Also, in this case IDCA-CCS obtains better results than IDCA-RCA. Using IDCA-CCS, the channels of the interfaces are initially assigned to channels 1 (common channel) and 2, which are used by the first flows. Then, the dynamic assignment moves the free interfaces to a less loaded channel, which is used by the subsequent flows. This way, as was previously illustrated in Fig. 6.8, each route tends to be formed by links using the same channel, which in this case, due to the low number of flows, benefits the performance of the network.

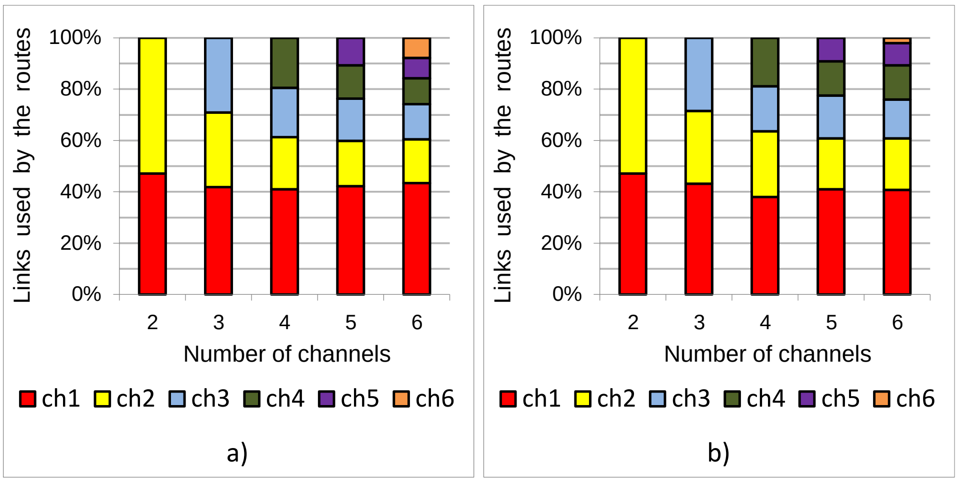


Fig. 6.17: IDCA analysis: Channel allocation in Scenario 3 (2 interfaces). a) IDCA-RCA and b) IDCA-CCS

Fig. 6.18 shows the goodput of the scenario when the nodes are equipped with three interfaces. Again, the benefits of using additional channels are very noticeable; IDCA-RCA using 6 channels nearly doubles the goodput of the 3 channels case. Indeed, results are similar to the case of two interfaces, with IDCA obtaining the best performance. However, in this case IDCA-RCA obtains higher goodput than IDCA-CSS when the number of available channels is high. Due to the additional interface, IDCA-RCA can decrease the usage of the common channel and increase channel diversity in the routes.

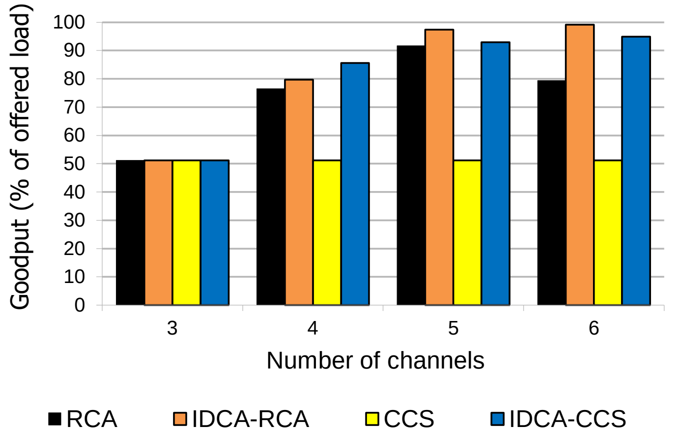


Fig. 6.18: IDCA analysis: Goodput obtained in Scenario 3 using 3 interfaces

In conclusion, the IDCA solution offers an interesting trade-off between the connectivity preservation of CCS and the channel diversity of RCA. Results show that it adapts well to different network topologies and traffic patterns, leading in general to a satisfactory performance.

However, the main disadvantage of IDCA remains on the circular dependency between channel assignment and routing, as is, in fact, also the case of any other algorithm which is not aware of the future traffic demands, as was introduced in Section 6.1. Depending on the created routes, IDCA can lead in some cases to the congestion of the common channel and the underuse of other channels. Indeed, in some situations the algorithm based in avoiding interference assigns some interfaces to isolated channels, as was illustrated in Fig. 6.8.

Next section presents MR-DEMON, which, combined with IDCA, can minimize the impact of these disadvantages by detecting performance degradations and reallocating routes to other available channels and interfaces.

6.2.2 Multi-Radio DEMON

As pointed out in the performance analysis of DEMON in Chapter 5, one of the disadvantages of this route maintenance solution is the high number of route recoveries from the source that are necessary depending on the scenario and the link quality threshold. The objective of MR-DEMON is to decrease the number of route recoveries by permitting the nodes forming the degraded link to negotiate the usage of an alternative channel. This way, performance degradation can be avoided locally without needing to initiate a new route discovery phase from the source (i.e. performing local repair), thus decreasing the overhead due to signaling and the duration of the degradation.

In fact, MR-DEMON can be seen as a form of joining routing and channel assignment based on route recovery instead of route creation. As was remarked in IDCA analysis, depending on traffic demands and the formed routes, channel assignments can lead to some congested channels (e.g. the common channel) while others remain underused. MR-DEMON can mitigate these limitations by locally changing channel assignments according to traffic performance, as shown in Fig. 6.19.

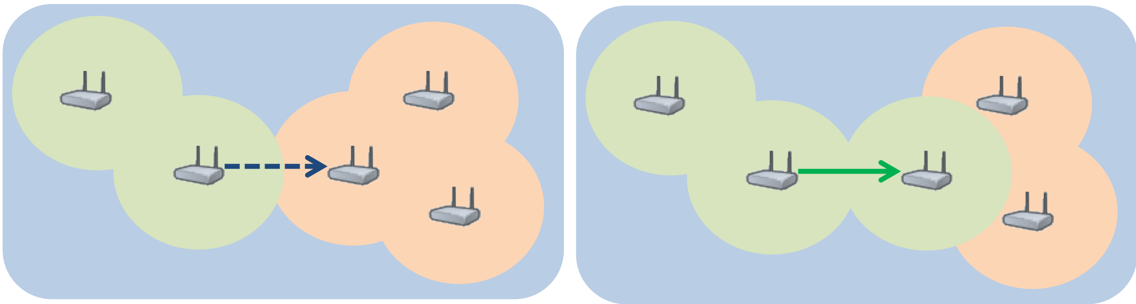


Fig. 6.19: MR-DEMON as a way of joining routing and channel assignment. a) A route traversing a link assigned to the common channel (blue) becomes degraded. b) By using MR-DEMON, one of the nodes changes one of its free interfaces to an alternative channel (green), which is also available to the other end of the link. The new formed link can now be used to route the degraded flow.

Link quality monitoring is performed as in DEMON, which was detailed in Section 5.2.2. However, in MR-DEMON two thresholds are used. When the quality of a link degrades under the highest threshold, the algorithm intends to shift one of the degraded routes to another channel. On the other hand, if channel reallocation is not possible and the quality of the link degrades under the lower threshold, a route recovery from the source is initiated as in the DEMON case. The intention of this proposal is to be more aggressive when trying to locally avoid degradations and more conservative when initiating route recoveries from the source.

First, once the quality of a link degrades under the highest threshold, the node which notices the degradation (i.e. the receiver of the data packets) searches for a suitable channel with the highest available bandwidth. In order to be eligible, a link using this channel should exist between both nodes or the nodes should have free interfaces which can be assigned to this channel in order to form a new link between them. As in IDCA case, interfaces being used by active flows or assigned to a common channel are not considered by the algorithm. This way, active routes are not disrupted and network connectivity is preserved.

If a channel fulfilling these requirements exists, the node then searches for the most loaded route traversing the degraded link which can be routed through the new channel without exceeding its available bandwidth. If such a route exists, a three-way handshake is performed in order to alert the other end of the link, as illustrated in Fig. 6.20. Note, that the transmission of data packets through the degraded routes is maintained during the whole procedure.

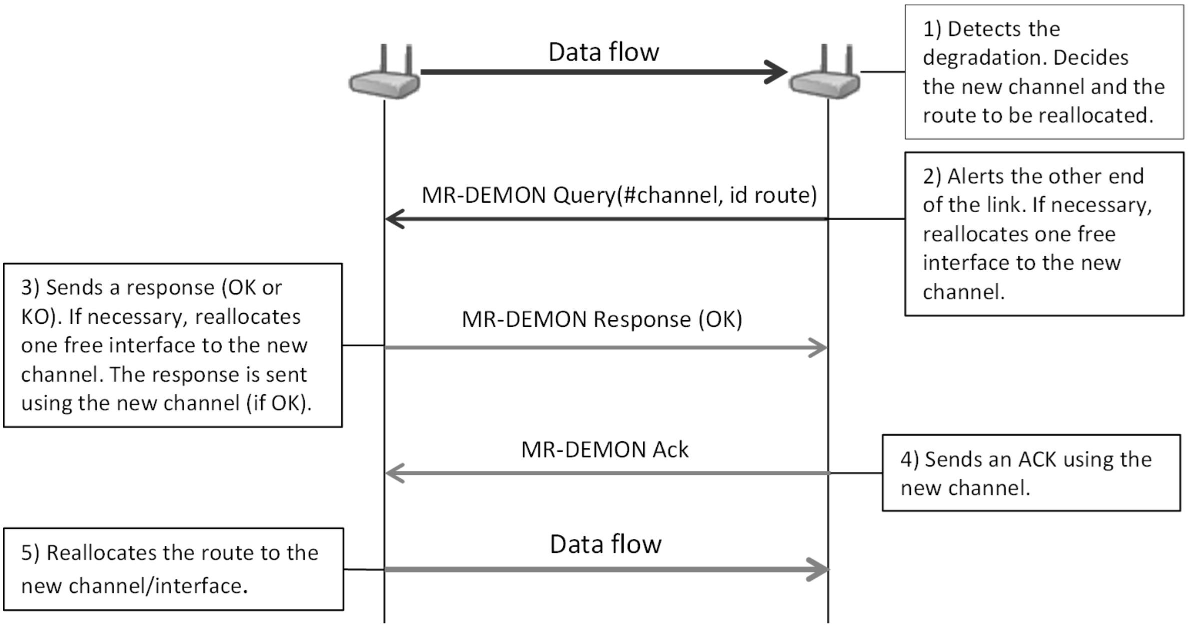


Fig. 6.20: Three-way handshake of MR-DEMON. Timeouts and retransmission are used in the different phases in order to assure the correctness of the procedure. If a MR-DEMON Response with code KO is received, the procedure is cancelled.

The following section studies the performance of MR-DEMON in different scenarios.

6.2.2.1 Performance analysis

As in the case of IDCA, CCS and RCA were selected as basis of the evaluation in order to compare results and obtain an initial channel assignment. The simulated scenarios are based on the grid of 64 nodes detailed in Section 2.2.3.3 (Fig. 2.14 and Table 2.9). In all cases, the 95% confidence interval of each result was computed. These intervals were found to be more dependent on the scenario than on the analyzed mechanism (e.g. random deployments lead to higher values than grid deployments). Therefore, for the sake of illustration clarity, confidence intervals of the results, which did not get over the 3-5%, are not included in the corresponding figures. Table 6.1 summarizes the generic parameters of the simulations.

Parameter	Value or Configuration
#Simulations per result	25
Link bit rate	12 Mbps
Traffic	UDP, CBR, unidirectional
Routing metric	WCIM (25% of load inflation for the common channel)
IDCA's threshold	5%
IDCA's period	random [15, 20] s
DEMON's α (EWMA)	0.5
DEMON's β (LSR)	10%

Table 6.1: Basic simulation parameters of MR-DEMON performance analysis

For the sake of a fair comparison with MR-DEMON, the other evaluated solutions also used the basic version of DEMON in order to react to performance degradations. The dynamic threshold was used in these cases, since, as evaluated in Chapter 5, it offers a satisfactory performance in a variety of scenarios. In the case of MR-DEMON, the threshold which controls local channel reallocation was fixed to the 90%, while the threshold managing route recoveries from the source (i.e. DEMON's threshold) was fixed to the 50%. It is worth to say that a fine adjustment of the different thresholds may lead to better results depending on the scenario. Nevertheless, this configuration permits to analyze the benefits of the channel reassignment solution performed by MR-DEMON.

Finally, the available bandwidth computation used to decide the best channel during route reallocation was based on WCIM's model, which was defined in Section 4.3.2.1 (see Fig. 4.8).

6.2.2.1.1 Scenario 1: 8 flows, random node spatial distribution

In the first analyzed scenario the nodes were located using a uniformly random distribution and 8 flows were routed with random source and destination. The first flow started at second 100 and then every 20 seconds a new flow was initiated. The data rate of each flow was 1500 kbps. The following figures show the results during the time interval in which all the flows were active (i.e. between seconds 250 and 400, with a total offered load of 12 Mbps).

Fig. 6.21 shows the goodput obtained according to the different mechanisms and the number of available interfaces and channels. First, results illustrate the benefits of using multi-radio deployments; while the goodput using 1 interface hardly reached the 15% of the offered load, using 2 and 3 interfaces the performance of the network increased over the 60% and 90%, respectively. Also, the poor results of CCS-DEMON compared to the rest of CAA algorithms remark the importance of using additional orthogonal channels in an efficient way.

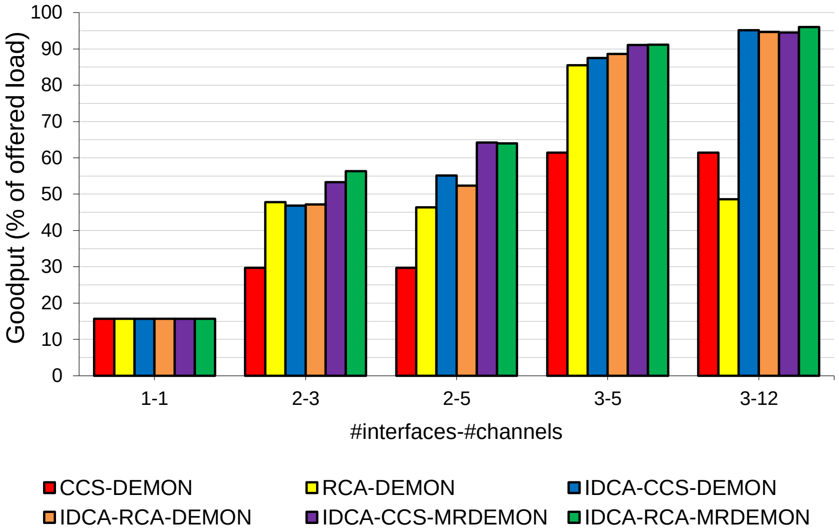


Fig. 6.21: MR-DEMON analysis: Goodput obtained in the first scenario.

As was also pointed out in IDCA's analysis (Section 6.2.1.1), due to the pigeonhole principle, RCA-DEMON obtains good results when network connectivity is assured (i.e. 2-3 and 3-5) but degrades with the increment of channels. On the contrary, the performance using IDCA usually improves with the number of channels since this leads to more chances of avoiding interference.

Goodput results show that MR-DEMON clearly benefits the performance of IDCA, especially in the case of two interfaces. As illustrated in Fig. 6.22, MR-DEMON decreases the number of reallocated routes by using alternative channels or interfaces between the nodes forming the degraded link. This procedure permits to obtain a better channel allocations according to the routes and the loads of the active flows, forming for instance new links between nodes which initially only shared the common channel. The usage of DEMON and MR-DEMON also make IDCA results less dependent on the initial channel assignment scheme (i.e. RCA or CCS), due to the numerous route and channel reallocations (i.e. the initial assignment scheme becomes rapidly changed).

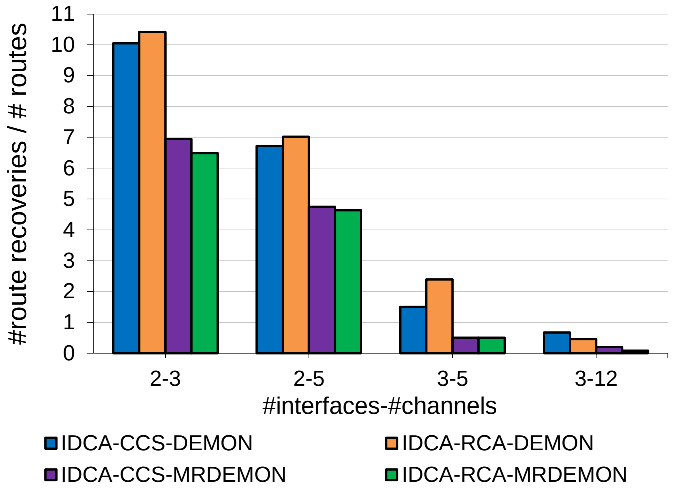


Fig. 6.22: MR-DEMON analysis: Route recoveries in the first scenario.

Finally, Fig. 6.23 shows the average delay per flow. Although in general the delay performance obtained in this evaluation was almost complementary to the goodput one, in this scenario the results of some IDCA-based mechanisms in the two interfaces case were slightly worse when using 5 channels. This occurred due to a slightly increase of the length of the routes because of a higher channel diversity.

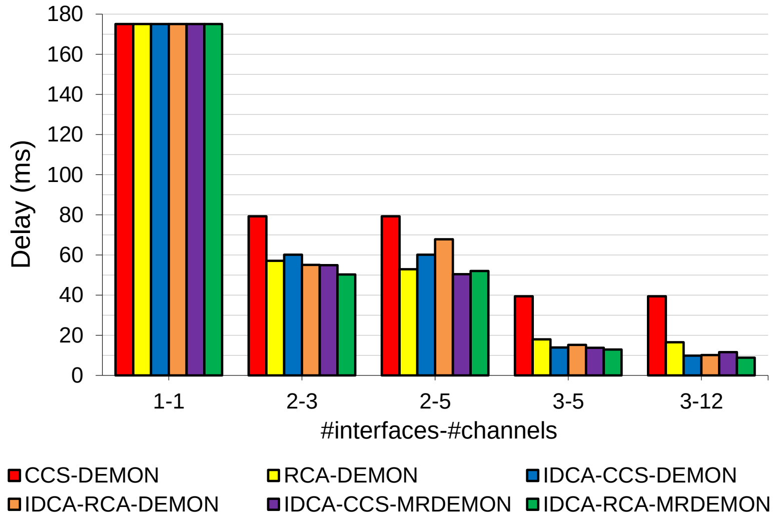


Fig. 6.23: MR-DEMON analysis: Delay obtained in the first scenario

6.2.2.1.2 Scenario 2: 64 flows, grid distribution

Scenario 2 consisted of 64 nodes located in a grid and 64 flows of 250 kbps initiated in a random time between seconds 100 and 300. The duration of the flows was 300 seconds and the destinations were randomly decided. Fig. 6.24 shows the goodput obtained by the different evaluated CAAs. The GRID-DEMON algorithm was simulated only in the 2-5 case to be used for comparative purposes; as expected, it obtained the best results since this centralized CAA is optimized for this type of topology.

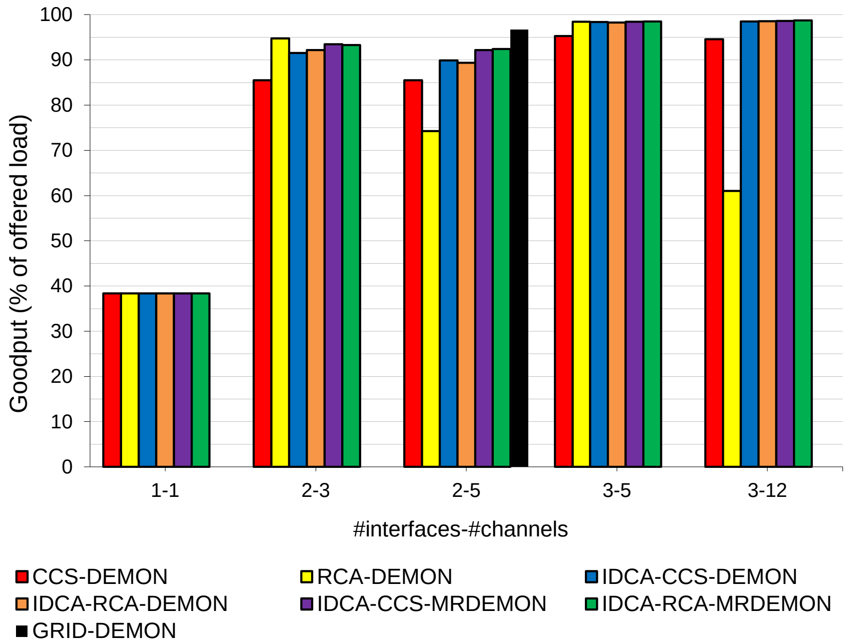


Fig. 6.24: MR-DEMON analysis: Goodput obtained in the second scenario

Indeed, all CAAs leaded to similar results. CSS-DEMON obtained again the worst results due to its poor channel diversity, while RCA-DEMON performed very well when the pigeonhole principle was satisfied and inefficiently when not.

In this scenario, the benefits of MR-DEMON, although slightly improving the standalone versions of IDCA in all cases, were not very noticeable. Due to the high number of flows and the regular topology, the number of free interfaces to apply MR-DEMON's local recovery was sparse. Also, since the performance of the network was over the 80%, the low degradation threshold that controls the route recovery procedure of MR-DEMON (i.e. degradation of the 50%) was unproductive. Nevertheless, the obtained results were close to the GRID-DEMON case although the penalty of using the common channel to assure connectivity.

6.2.2.1.3 Scenario 3: random number of interfaces

In this scenario, the number of interfaces of each node was randomly assigned, applying the following scheme: 16 nodes with one interface, 32 with two interfaces and 16 with three interfaces. Five orthogonal channels were available. The grid and random topologies, and the two traffic patterns of 64 and 8 flows were analyzed. The objective of this scenario was to evaluate how the trade-off between connectivity and channel diversity determines the performance of the different CAAs in the case of having nodes with different capacities.

Fig. 6.25 shows the throughput of the scenarios traversed by 8 flows. As expected, the performance of RCA-DEMON was the worst one because of the lack of a method to assure connectivity. On the contrary, CSS-DEMON offered better results than in previous scenarios, indeed similar to the obtained by the IDCA-CCS-DEMON mechanism. In such a scenario, the common channel set assures the connectivity of the nodes with one interface, while the nodes with two or three interfaces can make use the other orthogonal channels to minimize interference.

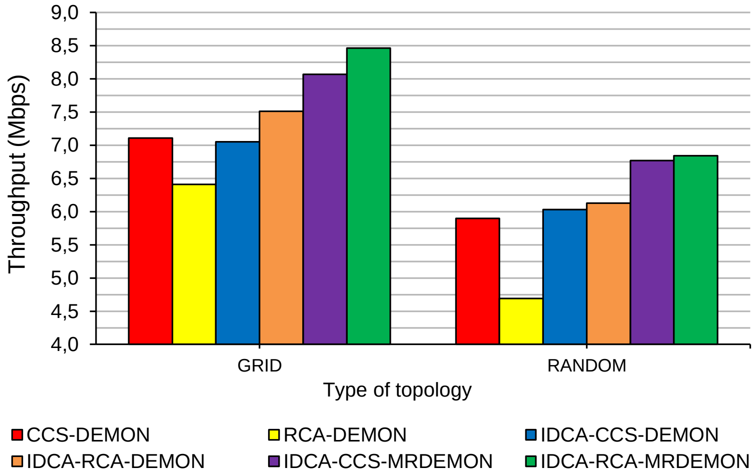


Fig. 6.25: MR-DEMON analysis: Performance of the third scenario (8 flows)

As was discussed in the IDCA analysis of Section 6.2.1.1, the channel allocation of IDCA-CSS tends to a higher usage of the channels of the CSS. On the other hand, IDCA-RCA tends to group the channels in zones, according to the algorithm based on the optimal number of neighbors introduced in Section 6.2.1, leading to a higher channel diversity than IDCA-CCS, while overcoming the problems of the standalone version of RCA.

Finally, results show that MR-DEMON improved the performance of both standalone versions of IDCA in a similar way. As pointed out in previous scenarios, MR-DEMON reduces the number of route recoveries by locally reallocating flows through free channels and interfaces. Due to the variable number of interfaces, in this scenario the initial assignment of IDCA was more probable to lead to isolated interfaces, which can be later reassigned by using MR-DEMON.

In the case of the scenarios traversed by 64 flows, Fig. 6.26 shows that results were similar, obtaining IDCA-RCA-MRDEMON the best performance in both node distributions. As also occurred in previous scenarios, results combining the grid topology with a high number of flows left less improvement capacity since all available interfaces and channels were rapidly occupied.

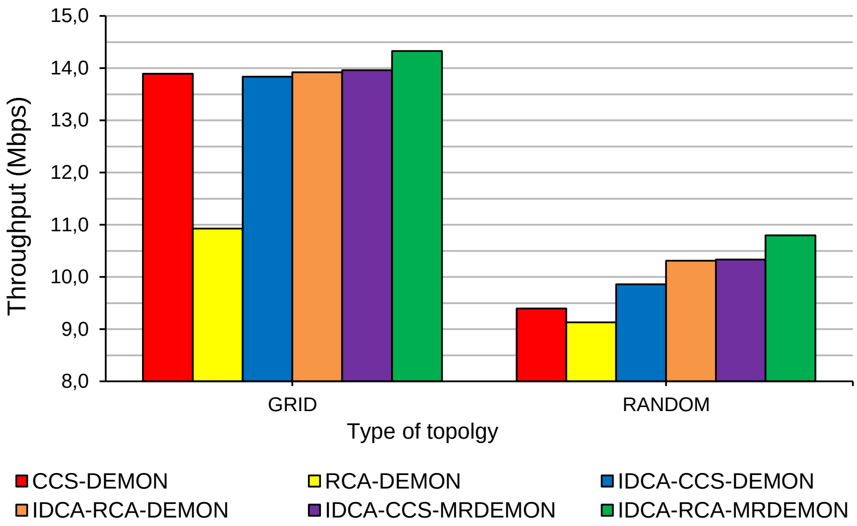


Fig. 6.26: MR-DEMON analysis: Performance of the third scenario (64 flows)

6.3 Conclusions

Contributions of this chapter focus on multi-radio solutions for MIWNs, especially on distributed and practical strategies. Although more complex and centralized algorithms can usually offer an upper bound on the expected performance of a network, as was the case of the GRID or neighbor partitioning solution in the evaluated grid scenarios, they are not always applicable in real deployments, where obtaining a global view of the network is not always feasible or realistic. On the other hand, distributed algorithms fit better with the dynamic nature of MIWNs and can offer an efficient and readily applicable solution in a variety of scenarios. Following this premise, two mechanisms related with channel assignment procedures have been presented and evaluated in this chapter: IDCA and MR-DEMON.

IDCA uses a dynamic and distributed algorithm in order to allow nodes to reallocate the channels of free interfaces (i.e. not traversed by active flows) according to the load and interference caused by active routes. Also, it applies a neighbor partitioning mechanism in order to distribute neighbors between the different interfaces. In order to avoid network partitions, IDCA makes use of a common channel which has to be assigned to one of the interfaces of all the nodes. Finally, depending on the initially applied CAA, IDCA can lead to different channel distributions; using CCS IDCA tends to distribute channels according to the created routes (i.e. most links of a route use the same channel), while using RCA it leads to the formation of clusters of nodes sharing the same channel.

Results show that IDCA offers an interesting trade-off between the connectivity preservation of CCS and the channel diversity of RCA. Its major problem is the usage of a common channel, which can become congested with the increase of offered load, especially in the case of nodes with two interfaces, since links using the common channel are usually the only available ones between two neighbor nodes. On the other hand, with a higher number of interfaces IDCA can better distribute the nodes between the different interfaces, thus incrementing the number of eligible routes which do not use the common channel.

Nevertheless, as other CAAs which do not join channel assignment and routing, depending on the routes, IDCA can lead to the congestion of some channels while others remain underused. Therefore, MR-DEMON is introduced as a way of joining channel assignment and routing procedures, but oriented to route recovery instead of route creation, which is the usual case in literature. Following the same principle as DEMON, MR-DEMON permits neighbor nodes to reallocate the routes through other channels in order to avoid performance degradations. This way, local recovery and channel assignment procedures are joined. MR-DEMON defines two different thresholds. The highest one, which is more aggressive, is used to initiate channel reallocation. The lowest one, more conservative, starts the basic DEMON procedure, which recovers routes from the source node.

Results show that MR-DEMON benefits the performance of IDCA in all evaluated cases. It permits to allocate channels according to the routes and performance of the active flows, creating for instance new links between nodes which initially only shared the common channel. Also, compared to the results of DEMON, the number of route recoveries becomes significantly lower, decreasing the overhead of the network.

Regarding other evaluated CAAs, simulations show that the RCA obtains good results when network connectivity is assured by the relationship between the number of interfaces and the number of available channels. This is for instance the usual case of a network whose nodes are equipped with two IEEE 802.11b interfaces, since this technology offers 3 non-overlapping channels. However, when connectivity is not assured, as is the case of networks where nodes have a variable number of interfaces, RCA degrades the performance due to network partitioning. On the other hand, the CCS-based channel assignment obtains usually the worst results in all the considered scenarios. Although, when combined with a proper routing metric it increases the bandwidth of the network compared to the single-interface case, the channels become easily congested. Indeed, CCS results remark the importance of channel diversity in order to lower congestion and interference in multi-radio networks.

Future work related with IDCA includes considering physical parameters or phenomena which impact the performance of the channels. For instance, the interference created by other networks or technologies operating in the same channels, or the utilization of partial overlapped channels. Also, ways to assure connectivity without needing to define a common channel should be studied. In the case of MR-DEMON, as was the case of the basic DEMON, different thresholds, channel reallocation and route recovery strategies could be defined and studied.

7

Conclusions and Future Work

This chapter summarizes the conclusions and the main contributions of this thesis. Also, a brief discussion about future work is included. Finally, the publications and projects related with this research are listed.

7.1 Conclusions

The IEEE 802.11 standard was not initially designed to provide multi-hop capabilities. Therefore, providing a proper traffic performance in MIWNs becomes a significant challenge. Indeed, assuring a determined quality of service is complex even in the single-hop or infrastructure scenario [161] and the success of WLANs has been supported by the constant improvement of the standard based on its amendments [2], especially the increase of bandwidth in order to manage the high demand of traffic.

In the case of MIWNs, the MAC layer has to deal with high levels of contention and interference. Due to half-duplex behavior and the presence of hidden nodes, a single flow traversing a multi-hop path incurs in intra-flow interference and leads to the well-known throughput division by the number of hops [13]. In addition, flows traversing adjacent paths compete for the same channel time, causing inter-flow interference [24].

The approach followed in this thesis has been focused on the routing layer in order to obtain applicable solutions not dependent on a specific hardware or driver. Nevertheless, as is the case of most of the research on this field, a cross-layer design has been adopted in order to consider physical and MAC issues which affect the quality of the flows [17][18]. In this regard, one of the first tasks of this work was devoted to the study of the phenomena which affect the performance of the flows in MIWNs. Specifically: link quality, contention and interference, and the utilization of multiple channels and radios.

The characterization and estimation of link errors and bit rates by means of probe packets, and its integration into routing procedures, is almost standardized due to the success of ETX [59] and ETT [43] routing metrics. In the case of interference models, although being usually based on the neighborhood of the nodes, numerous solutions have been published without obtaining a prevailed one [17][20][37][117]. The proposal presented in this thesis weights differently the interference of the one- and two-hop neighbors of the transmitter and the receiver in order to consider the different impact of contending, hidden and remote interfering nodes [52]. The model also defines interference as a measure of channel consumption, according to the data rate, the link bit rate (including its efficiency) and the link error rate.

The effectiveness of this interference model was validated by means of its integration in a routing metric called Weighted Contention and Interference routing Metric (WCIM) [52]. Results showed that WCIM can be considered as a reliable estimator of the performance of the routes at a given time, concretely of the end-to-end delay. This clearly benefits the quality of the flows, as was proved through extensive simulations of different scenarios. In all cases, WCIM outperformed the other analyzed state-of-the-art routing metrics due to a proper leveraging of the number of hops, the link quality and the suffered interference. Indeed, the results obtained by other routing metrics remark the importance of appropriately combining the different phenomena which impact the performance of the flows in order to obtain a proper route creation strategy. For instance, only considering link quality parameters can induce congestion, but overestimating interference can lead to the formation of long or slow routes.

In addition to the design of a novel routing metric, an enhancement of the AODV routing protocol was implemented. The Flow-based AODV (FB-AODV) creates routes and forwards packets according to the flows (i.e. source, destination and ToS), on the contrary to basic AODV which is destination-based [52]. First, this enhancement permits to balance the load of the network in the case of having flows with a common destination (e.g. traffic to the Internet through a common gateway). Secondly, it gives a finer granularity in the control and monitoring of the flows. Results showed that it clearly benefits the performance of the flows, regardless of the routing metric.

The second main contribution of this thesis focuses on route maintenance. Even in the best case of obtaining the optimal route for a flow at a given time, network conditions may vary and routes should adapt to them in order to conserve traffic performance. Generally, route recovery procedures are devoted to the detection of link breaks due to mobility or fading. In the case of proactive routing, routes can become updated by means of periodical signaling according to the routing metric. However, the propagation of route modifications can be slow and requires high overhead [136][137]. Also, proactive procedures do not fit well with load balancing or flow-based routing [132]; thus, they are usually combined with link quality aware routing metrics. On the other hand, on-demand protocols by default do not modify routes until disconnections are noticed. Therefore, preemptive solutions have been introduced as a way of anticipating link breaks and prevent traffic disruptions [55].

The preemptive approach introduced in Chapter 5, which is called DEMON, enhances FB-AODV by monitoring the performance active flows and recovering degraded routes. While the majority of preemptive solutions of the state-of-the-art are based on the received signal in order to detect mobility, DEMON captures any phenomena causing the loss of data frames during their transmission [54]. This way, the routing protocol can also react to the congestion and interference caused by the arrival of new flows, thus improving load balancing in the network. Results showed that DEMON obtains similar or better results than other published solutions in mobile scenarios, while it clearly outperforms default AODV performance under congestion. DEMON evaluation also included an analysis of the impact on traffic performance of different design parameters, like the threshold controlling degradation alerts or the frequency and number of Hello messages.

Finally, another interesting feature of DEMON is the fact that it obtains good results when combined with a load-unaware routing metric like ETT. Since load-aware routing metrics can lead to instability under highly variable network conditions [37], using DEMON the routing metric can remain load-unaware, while route recovery can become load-aware by means of performance monitoring. In fact, according to the obtained results, it can be concluded that in some scenarios route recovery mechanisms have a greater influence on the performance of the routed flows than the routing metrics used for route discovery.

The last chapter of this thesis deals with multi-radio solutions. In previous chapters, multi-radio scenarios have been considered in the evaluation of FB-AODV, WCIM and DEMON solutions. Indeed, routing metrics which are aware of the channels of the links can be considered as a distributed channel assignment mechanism [151], since they select the channels that will be traversed by the paths. This circular relationship between channel assignment and routing is certainly its major challenge [28][100]; channel assignment determines the routes that can be created, while the created routes decide the real channel diversity of the network and the level of interference between the links. Therefore, obtaining an optimal channel assignment algorithm which minimizes interference is a NP-hard problem [99] and proposals which join routing and channel assignment are generally complex, centralized and based on traffic patterns [26][151], limiting their practical application.

The first contribution to this research area is IDCA, a distributed and dynamic channel assignment based on the interference caused by active flows [56]. Since channels are dynamically changed, a common channel is fixed in one of the interfaces of all the nodes to assure network connectivity and avoid deafness and broadcast issues [27]. Also, only free interfaces are allowed to modify its channel to avoid disrupting active flows. Although it can be also used for routing traffic, results showed that the common channel became rapidly congested in scenarios with only two interfaces per node. On the other hand, when using three interfaces per node, IDCA results were significantly better and traffic became intelligently distributed through all the available channels. In general, IDCA leads to an interesting trade-off between the connectivity preservation of CCS and the channel diversity of RCA.

However, as other state-of-the-art algorithms which do not join channel assignment and routing, depending on the routes, IDCA can lead to the congestion of some channels while others remain underused. Therefore, MR-DEMON is also introduced in Chapter 6 as a novel way of joining channel assignment and routing. As DEMON, MR-DEMON monitors the performance of the active flows traversing the links, but, instead of alerting the source in the case of noticing degradation, permits reallocating the flows to less interfered channels. Only if channel reallocation is not possible, the default route recovery procedure of DEMON is initiated. Joining route recovery instead of route creation simplifies its application, since traffic patterns are not needed and channel reassignments can be locally decided. The evaluation of MR-DEMON proved that it clearly benefits the performance of IDCA. Also, it improves DEMON functionality by decreasing the number of route recoveries from the source, leading to a lower overhead.

As concluding remark, all designed approaches have achieved their purpose of improving the routing of traffic flows traversing MIWNs. The proposed enhancements have been evaluated under different network conditions (e.g. mobility, multi-radio, variable load...) and compared to other state-of-the-art methods. Finally, all mechanisms can be integrated, obtaining a complete routing solution which includes route creation, route recovery and channel assignment procedures.

7.2 Future work

As has been remarked in the particular conclusions of each chapter, the different proposals of this thesis include parameters or procedures which can be fine-tuned according to the specific characteristics of the scenarios, or enhanced by including more information from lower layers.

In the case of WCIM, the interference model assumes some simplifications in order to facilitate its implementation and not being limited to particular NIC drivers or hardware [71]. However, considering physical information like the RSSI of the received packets could enhance the model by better weighting the interference of hidden and remote interfering nodes.

DEMON includes several mechanisms whose impact on traffic performance can be studied more deeply, probably leading to some enhancements. For instance, in case of degradation, the route selection algorithm selects each time a unique route to be recovered. However, in the case of mobility or fading, recovering all the flows traversing the degraded link could lead to better results. A possible solution could be to infer the cause of the degradation by using physical information like the RSSI of received packets (i.e. taking a decrease of RSSI as a sign of mobility as other preemptive solutions) or by detecting load variations in the neighborhood (i.e. noticing a degradation without load/interference variations could be an indication of mobility). Also, during the realization of this thesis, different dynamic threshold implementations were evaluated and discarded; for instance, decreasing the threshold of a link each time degradation was noticed and increasing it after a period of time without degradations. However, other dynamic thresholds could be implemented and evaluated in order to increase the benefits of DEMON.

Regarding IDCA and MR-DEMON mechanism, the interference of external networks into the channel assignment algorithm, especially in the case of the common channel [101], should be considered in real deployments due to the high presence of Wi-Fi networks. Also, although the usage of a common channel offers some advantages [135], other mechanisms to assure connectivity should be studied. Finally, in the case of MR-DEMON, as also occurs with DEMON, the study of different thresholds and route recovery strategies should be considered in future enhancements of the mechanism.

Most results presented in this thesis have been obtained by means of simulations in order to evaluate the benefits of the different mechanisms in a variety of network conditions. As future work, it would be interesting to validate them in real deployments. Indeed, an implementation of FB-AODV and WCIM for Linux-based platforms is publicly available under GPL license [134], and has been used by other researchers in order to create MIWNs with Android phones [62][63]. Also, a previous version of this routing solution was used in the research project described in

Appendix I and evaluated in [162] and [163], while a specific multi-radio solution was implemented in the project presented in Appendix II.

The proper routing of TCP traffics in MIWNs is challenging due to the deficient operation of its congestion mechanisms. First, it tends rapidly to channel saturation by increasing the data rate of the flows, systematically producing intra-flow interference [150]. On the other hand, it assumes that data losses are caused by congestion, while in MIWNs often occur due to transmission errors [149]. To avoid the inherence of these mechanisms on the analysis of the contributions, most evaluations of this thesis were carried out by routing UDP flows. However, due to its interest, the performance of WCIM and DEMON with TCP was also analyzed, concluding in both cases that cross-layer information is needed in order to improve their behavior with this traffic type. For instance, in the case of DEMON, parameters like the Contention Window or the Retransmission Timeout could be used as a sign of degradation.

Although the contributions of this thesis are devoted to the improvement of traffic routing in MIWNs, QoS related mechanisms like performance assurance or admission control have not been considered. However, some of the proposals and the obtained conclusions can be relevant for this research area. First, QoS solutions for MIWNs are usually based on on-demand routing protocols, using route discovery as a way of estimating the quality of the routes [108] and implementing admission control [107]. In this regard, FB-AODV offers a way of increasing the control over routed flows and applying load-balancing, while WCIM has been proved to be a proper estimator of the performance of the routes. In addition, as was found during its evaluation, WCIM can also work as a sort of admission control, discarding new routes when the available bandwidth of the network is too scarce. On the other hand, DEMON uses passive monitoring to recover degraded routes, which can be useful when implementing performance assurance policies. In conclusion, future work could include the integration of some of the contributions of this thesis into QoS frameworks.

In this thesis channel assignment has been considered as an issue related to the routing layer. However, maybe in the future this task should be left to lower layers, as is the case of data rates, which are determined by the NIC drivers [30]. Indeed, challenges related with multi-radio are similar to those related with multi-rate; there is a trade-off between performance improvement (i.e. higher channel diversity and higher data rates) and connectivity (i.e. common channels and robust data rates). It would be expected that future hardware improvements might lead to negligible channel switching delays, allowing switching channels in a per-packet basis and integrating channel selection into MAC procedures.

On the other hand, according to the new amendments of the IEEE 802.11 standard, which permit the usage of wide channels [35], channel assignment strategies could become useless if the number of orthogonal channels tends to match the number of interfaces. Or at least, connectivity would be assured by the pigeonhole principle, facilitating the design of the algorithms. On the contrary, the emergence of Cognitive Radio Networks, which relay on spectrum sensing and allocation, opens a new application field for channel assignment strategies [164][165].

The 802.11s amendment presents several challenges and opportunities related with the contributions of this thesis. First, the usage of MCCA would need a redefinition of the proposed interference model; MCCA can overcome some limitations of CSMA/CA coordinating the access to the medium by reserving transmission slots in advance [2][40], but it doesn't avoid all interfering cases [166]. On the other hand, the default routing solution of 802.11s is based on the AODV protocol and the ETT metric [42], thus facing similar issues to those studied in this work. Indeed, the extensible path selection framework of the standard permits the implementation of different routing solutions [2][42]. Also, 802.11s defines the Intra-Mesh Congestion Control (IMCC), which, in a similar way to DEMON, detects congestion at intermediate nodes and warns the transmitters of the flows to decrease the data rate [167]. Finally, although multi-radio is contemplated by the standard, no concrete solutions for channel assignment are proposed [2].

Finally, contributions of this thesis could be relevant to the application of the SDN paradigm in MIWNs deployments, which is an emerging research area [168]. SDNs can improve the management of the flows (e.g. routes, policies, monitoring, etc.) by decoupling network control and forwarding functions [169]. Network control is defined by software and centralized, offering a global view of the network which can be useful in order to enhance routing, maintenance and channel assignment procedures in MIWNs. In particular, SDN frameworks and tools could be used to facilitate the design and implementation of centralized and more complex CAAs.

7.3 Publications and research projects

7.3.1 Publications

- **A performance study of practical channel assignment solutions in multi- radio multi-hop IEEE 802.11 networks.** Miguel Catalan-Cid, Carles Gomez and Josep Paradells. The Tenth ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN), 2013, Barcelona.
- **DEMON: preemptive route recovery for AODV in multi-hop wireless networks based on performance degradation monitoring.** Miguel Catalan- Cid, Josep Lluis Ferrer, Carles Gomez and Josep Paradells. EURASIP Journal on Wireless Communications and Networking, 2013.
- **Contention- and Interference-Aware Flow-based Routing in Wireless Mesh Networks: design and evaluation of a novel routing metric.** Miguel Catalan-Cid, Josep Lluis Ferrer, Carles Gomez, and Josep Paradells. EURASIP Journal on Wireless Communications and Networking, 2010.
- **Red mallada asistida por UMTS/GPRS**. J. Paradells, M. Catalan, J. L. Ferrer, M. Catalan-Cid, X. Sánchez, V. Beltran, C. Gómez, P. Plans, E. García, J. Rubio, D. Almodóvar, and D. Rodellar. VI Jornadas de Ingeniería Telemática (JITEL), 2007, Málaga.
- **Design of a UMTS/GPRS Assisted Mesh Network (UAMN).** J. Paradells, J.L. Ferrer, M. Catalan, W. Torres, M. Catalan-Cid, X. Sánchez, V. Beltran, E. García, C. Gómez, P. Plans, et al. The 7th Wireless World Resarch Forum Meeting (WWRF), 2006, Heidelgberg.

7.3.2 Resarch projects related to this thesis

- **SIStema de Telecontrol Mallado Multi-radio Adaptativo (SISTEMMA).** Design and implementation of a multi-radio hardware and software solution for devices operating in UHF narrowband channels. Farell Instruments, i2CAT and UPC, AVANZA Competividad (I+D+I), 2010-2011.
- **UMTS/GPRS Assisted Mesh Network (UAMN).** Deployment of a multi-hop IEEE 802.11 wireless network assisted by a remote central server. Design and implementation of a routing protocol which differentiates flows and balances the load to the UMTS/GPRS gateways. Vodafone, SwissCom Innovations, I2CAT and UPC, 2007. Transferred to ADTelecom, PROFIT, 2008.

- **Atomic Services-based Internet Architecture for Constrained and Ubiquitous Networks (ASIACUN).** The main objective of this project was the design, construction and evaluation of a proof-of-concept new Internet architecture, suitable for constrained and ubiquitous networks, that is, suitable for the Internet of Things. Ministerio de Economía y Competitividad, TEC 2012-32531. Wireless Networks Group, UPC.
- **New Architectures for ubiquitous Internet: design and evaluation.** The main objective of this project was to advance in the conception of a new protocol architecture, mainly oriented to the connectivity of sensors and actuators, to improve the possible transitional Internet. This new architecture must support the communication among functionalities as a natural approach, mobility and auto configuration. Ministerio de Ciencia e Innovación, TEC 2009-11453. Wireless Networks Group, UPC.

References

[1] Cisco. **Cisco Visual Networking Index: Forecast and Methodology, 2014–2019.** White paper. May 2015.

[2] IEEE. **IEEE 802.11-2012 Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification.** March 2012. Revision of IEEE Std. 802.11-2007.

[3] Wi-Fi Alliance. **Wi-Fi Alliance celebrates 15 years of Wi-Fi**. Retrieved from http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-celebrates-15-years-of-wi-fi Last modification in September 2014.

[4] R. Ramanathan and J. Redi. **A brief overview of ad hoc networks: challenges and directions.** IEEE Communications Magazine. Volume 40, Issue 5, Pages 20-22. May 2002. doi:http://dx.doi.org/10.1109/MCOM.2002.1006968

[5] A. Goldsmith. **Wireless Communications.** Cambridge University Press. 2005. ISBN=0521837162

[6] M. Conti and S. Giordano. **Multihop Ad Hoc Networking: The Theory**. IEEE Communications Magazine. 2007. Volume 45, Issue 4, Pages 78-86. April 2007. doi:10.1109/MCOM.2007.343616

[7] M. Conti and S. Giordano. **Multihop Ad Hoc Networking: The Practice**. IEEE Communications Magazine. 2007. Volume 45, Issue 4, Pages 88-95. April 2007. doi: 10.1109/MCOM.2007.343617

[8] C. S. R. Murthy and B. S. Manoj. **Ad hoc Wireless Networks. Architectures and Protocols.** Prentice Hall. 2004. ISBN=0133007065

[9] S. Basagni, M. Conti, S. Giordano and I. Stojmenovic. **Mobile Ad hoc Networking**. John Wiley & Sons. 2004. ISBN=0471373133

[10] Y. Zhang, J. Luo and H. Hu. **Wireless Mesh Networking: Architectures, Protocols and Standards**. Auerbach Publications. USA, 2006. ISBN= 9780849373992

[11] I. Chlamtac, M. Conti and J.Liu**. Mobile ad hoc networking: imperatives and challenges.** Elsevier Ad Hoc Networks. Volume 1, Issue 1, Pages 13–64. July 2003. doi: doi:10.1016/S1570-8705(03)00013-1

[12] C. Chaudet, D. Dhoutaut, and I.G. Lassous. **Performance issues with IEEE 802.11 in ad hoc networking**. IEEE Communications Magazine. Volume 43, Issue 7, Pages 110-116. July 2005. doi: 10.1109/MCOM.2005.1470836

[13] J. Li, C. Blake, S.J. De Couto, H.I. Lee, and R. Morris**. Capacity of ad hoc wireless networks**. The 7th annual international conference on Mobile computing and networking (MobiCom 2001). Rome, Italy. July 2001. doi:http://doi.acm.org/10.1145/381677.381684

[14] X. Shugong. **Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?** IEEE Communications Magazine. Volume 39, Issue 6, Pages 130 – 137. June 2001. doi: 10.1109/35.925681

[15] A. Iyer and C. Rosenberg. **Understanding the key performance issues with MAC protocols for multi-hop wireless networks**. Wireless Communications and Mobile Computing. Volume 6, Issue 6, Pages 745-760. September 2006. doi:10.1002/wcm.v6:6

[16] E. Alotaibi and B. Mukherjee. **A survey on routing algorithms for wireless Ad-Hoc and mesh networks**. Elsevier Computer Networks. Volume 56, Issue 2, Pages 940–965. February 2012. doi:10.1016/j.comnet.2011.10.011

[17] V.C.M. Borges, M. Curado and E. Monteiro. **Cross-layer routing metrics for mesh networks: Current status and research directions**. Elsevier Computer Communications. Volume 34, Issue 6, Pages 681–703. May 2011. doi:doi:10.1016/j.comcom.2010.12.001

[18] I.F. Akyildiz, W. Xudong and W. Wang. **Wireless mesh networks: a survey**. Elsevier Computer Networks. Volume 47, Issue 4, Pages 445–487. March 2005. doi:doi:10.1016/j.comnet.2004.12.001

[19] X. Wang and A.O. Lim. **IEEE 802.11s wireless mesh networks: Framework and challenges.** Elsevier Ad Hoc Networks. Volume 6, Issue 6, Pages 970–984. August 2008. doi: doi:10.1016/j.adhoc.2007.09.003

[20] S. Ghannay, S.M. Gammar, F. Filali and F. Kamoun. **Multi-radio multichannel routing metrics in IEEE 802.11s-based wireless mesh networks - And the winner is…** First International Conference on Communications and Networking (ComNet 2009). Hammamet, Tunisia. November 2009. doi: 10.1109/COMNET.2009.5373550

[21] D. Aguayo, J. Bicket, S. Biswas, G. Judd and R. Morris. **Link-level measurements from an 802.11b mesh network.** The 2004 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM 2004). Oregon, USA. September 2004. doi:10.1145/1015467.1015482

[22] T. Clausen, P. Jacquet and L. Viennot. **Comparative study of routing protocols for mobile ad-hoc networks**. The First Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2002). Sardegna, Italy. September 2002.

[23] G. Anastasi, E. Borgia, M.Conti and E. Gregori. **Wi-Fi in ad hoc mode: a measurement study**. The Second IEEE Annual Conference on Pervasive Computing and Communications (PerCom 2004). Orlando, USA. March 2004. doi:10.1109/PERCOM.2004.1276853

[24] J. Lee, S-J. Lee, W. Kim and D. Jo. **Understanding interference and carrier sensing in wireless mesh networks**. IEEE Communications Magazine. Volume 47, Issue 7, Pages 102-109. July 2009. doi: 10.1109/MCOM.2009.5183479

[25] P. Kyasanur and N. H. Vaidya. **Capacity of multichannel wireless networks under the protocol model**. IEEE/ACM Transactions in Networking. Volume 17, Issue 2, Pages 515-527. April 2009. doi:10.1109/TNET.2008.926504

[26] P. Li, N. Scalabrino, Y. Fang, E. Gregori and I. Chlamtac. **How to Effectively Use Multiple Channels in Wireless Mesh Networks**. IEEE Transaction on Parallel and Distributed Systems. Volume 20, Issue 11, Pages 1641-1652. November 2009. doi: 10.1109/TPDS.2008.256

[27] J. Crichigno, M.-Y. Wu and W. Shu. **Protocols and architectures for channel assignment in wireless mesh networks**. Ad Hoc Networks. Volume 6 Issue 7, Pages 1051-1077. September 2008. doi: 10.1016/j.adhoc.2007.10.002

[28] W. Si, S. Selvakennedy and A.Y. Zomaya. **An overview of Channel Assignment methods for multi-radio multi-channel wireless mesh networks.** Journal of Parallel and Distributed Computing. Volume 70, Issue 5, Pages 505-524. May 2010. doi: 10.1016/j.jpdc.2009.09.011

[29] G.R. Hiertz, D. Denteneer, L. Stibor and Y. Zang. **The IEEE 802.11 universe.** IEEE Communications Magazine. Volume 48, Issue 1, Pages 62-70. January 2010. doi:10.1109/MCOM.2010.5394032

[30] S. Biaz and S. Wu. **Rate adaptation algorithms for IEEE 802.11 networks: A survey and comparison**. IEEE Symposium on Computers and Communications (ISCC 2008). Marrakech, Morocco. July 2008. doi:10.1109/ISCC.2008.4625680.

[31] M. Lacage, M. H. Manshaei and T. Turletti. **IEEE 802.11 rate adaptation: a practical approach**. The 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems (MSWiM 2004). Venice, Italy. October 2004. doi: 10.1145/1023663.1023687

[32] A. Kamerman and L. Monteban. **WaveLAN-II: A High-performance wireless LAN for the unlicensed band**. Bell Lab Technical Journal. Volume 2, Issue 3, Pages 118-133. Summer 1997. doi: 10.1002/bltj.2069

[33] Mac80211 driver. **Minstrel Rate Control Algorithm**. Retrieved from https://wireless.wiki.kernel.org/en/developers/documentation/mac80211/ratecontrol/minstrel. Last modification in March 2015.

[34] D. Xia, J. Hart and Q. Fu. **Evaluation of the Minstrel rate adaptation algorithm in IEEE 802.11g WLANs**. IEEE International Conference on Communications (ICC 2013). Budapest, Hungary. June 2013. doi: 10.1109/ICC.2013.6654858

[35] IEEE. **IEEE 802.11ac-2013 Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. - Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.** December 2013. Amendment toIEEE Std. 802.11-2007

[36] I. Ramachandran and S. Roy. **Clear channel assessment in energy-constrained wideband wireless network**. IEEE *Wireless Communications*. Volume 14, Issue 3, Pages 70–78. June 2007. doi: 10.1109/MWC.2007.386615

[37] Y. Yang, J. Wang and R. Kravets. **Designing routing metrics for mesh networks**. The IEEE Workshop on Wireless Mesh Networks (WiMesh 2005). Santa Clara, USA. September 2005.

[38] S. Kumar, V. S. Raghavan and J. Deng. **Medium Access Control protocols for ad hoc wireless networks: A survey**. Ad Hoc Networks. Volume 4, Issue 3, Pages. 326–358. May 2006. doi: doi:10.1016/j.adhoc.2004.10.001

[39] J. Mo, H-S. W. So and J. Walrand. **Comparison of Multichannel MAC Protocols**. IEEE Transaction on Mobile Computing. Volume 7, Issue 1, Pages 50–65. January 2008. doi: 10.1109/TMC.2007.1075

[40] G. R. Hiertz, S. Max, R. Zhao, D. Denteneer and L. Berlemann**. Principles of IEEE 802.11s**. The 16th International Conference on Computer Communications and Networks. Honolulu, Hawaii. August 2007. doi: 10.1109/ICCCN.2007.4317949

[41] C. Perkins, E. Belding-Royer, and S. Das. **Ad hoc On-Demand Distance Vector (AODV) Routing.** RFC 3561. IETF MANET Group. July 2003.

[42] M. Bahr. **Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s**. IEEE, 2007. IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2007). Pisa, Italy. October 2007. doi: 10.1109/MOBHOC.2007.4428721

[43] R. Draves, J. Padhye and B. Zill. **Routing in multi-radio, multi-hop wireless mesh networks**. The 10th annual international conference on Mobile computing and networking (MobiCom 2004). Philadelphia, USA. October 2004. doi:10.1145/1023720.1023732

[44] M. Esquius. **IEEE 802.11s Mesh Networking Evaluation under NS-3**. Final Degree Project, UPC. April 2011.

[45] S.K. Bhoi and P.M. Khilar. **Vehicular communication: a survey**. IET Networks. Volume 3, Issue 3, Pages 204-217. doi:10.1049/iet-net.2013.0065

[46] T. Clausen and P.Jacquet. **Optimized Link State Routing Protocol (OLSR).** RFC 3626. IETF MANET Group. October 2003.

[47] R. Ogier, F. Templin and M. Lewis. **Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)**. RFC 3684. IETF MANET Group. February 2004.

[48] D. Johnson, Y. Hu and D.Maltz. **The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4.** RFC 4728. IETF MANET Group. February 2007

[49] C. Perkins, S. Ratliff, J. Dowdell, L. Steenbrink and V. Mercieca. **Ad Hoc On-demand Distance Vector Routing Version 2 (AODVv2).** Internet-draft. IETF MANET Group. Last update October 2015.

[50] T. Clausen, C. Dearlove, P. Jacquet and U. Herberg. **The Optimized Link State Routing Protocol Version 2**. RFC 7181. IETF MANET Group. April 2014.

[51] M. E. M. Campista, P. M. Esposito, I. M. Moraes, L. H. M. K. Costa, O. C. M. B. Duarte, D. G. Passos, C. V. N. De Albuquerque, D. C. M. Saade and M. G. Rubinstein. **Routing Metrics and Protocols for Wireless Mesh Networks**. IEEE Network. *V*olume 22, Issue 1, Pages 6–12. January 2008. doi:10.1109/MNET.2008.4435897

[52] M. Catalan-Cid, J.L. Ferrer, C. Gomez and J. Paradells. **Contention- and interference-aware flow-based routing in wireless mesh networks: design and evaluation of a novel routing metric**. EURASIP Journal on Wireless Communications and Networking. Volume 2010, Article 106. December 2010. doi: 10.1155/2010/313768

[53] L. Chen and W. B. Heinzelman. **A Survey of Routing Protocols that Support QoS in Mobile Ad Hoc Networks**. IEEE Network. Volume 21, Issue 6, Pages 30–38. December 2007. doi: 10.1109/MNET.2007.4395108

[54] M. Catalan-Cid, C. Gomez, J. Paradells and J.L. Ferrer. **DEMON: preemptive route recovery for AODV in multi-hop wireless networks based on performance degradation monitoring.** EURASIP Journal on Wireless Communications and Networking. Volume 2013, Article 286. December 2013. doi: 10.1186/1687-1499-2013-286

[55] T. Goff, N.B. Abu-Ghazaleh, D.S. Phatak and R. Kahvecioglu. **Preemptive routing in ad hoc networks**. The 7th Annual International Conference on Mobile Computing and Networking (MobiCom 2001). Rome, Italy. July 2001. doi:10.1016/S0743-7315(02)00059-X

[56] M. Catalan-Cid, C. Gomez and J. Paradells. **A performance study of practical channel assignment solutions in mult- radio multi-hop IEEE 802.11 networks.** The Tenth ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN 2013). Barcelona, Spain. November 2013. doi: 10.1145/2507248.2507258

[57] R. Bruno, M. Conti, and E. Gregori. **Mesh networks: commodity multihop ad hoc networks**. IEEE Communications Magazine. Volume 43, Issue 3, Pages 123–131. March 2005. doi: 10.1109/MCOM.2005.1404606

[58] Tropos. **Tropos Mesh OS: Foundation of the Tropos mesh network architecture**. White paper. February 2014.

[59] D. S. J. De Couto, D. Aguayo, J. Bicket and R. Morris. **A high-throughput path metric for multi-hop wireless routing.** The 9th Annual international Conference on Mobile Computing and Networking (MobiCom 2003). San Diego, USA. September 2003. doi: 10.1145/938985.939000

[60] Meraki. **Technologies: Mesh routing**. Retrieved from https://meraki.cisco.com/technologies/mesh-routing. Accessed in October 2015.

[61] Firetide. **AutoMesh Networking Technology.** White paper. 2015.

[62] N. Corriero, E. Covino and A. Mottola. **An approach to use FB-AODV with Android**. The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011). Ontario, Canada. September 2011. doi:10.1016/j.procs.2011.07.044

[63] N. Corriero, A. Mottola and E. Zhupa. **How to Work with Android within a (FB-)Aodv Network**. International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2011). Barcelona, Spain. October 2011. doi:10.1109/3PGCIC.2011.16

[64] D. Camps-Mur, A. Garcia-Saavedra and P. Serrano. **Device-to-device communications with Wi-Fi Direct: overview and experimentation.** IEEE Wireless Communications. Volume 20, Issue 3, Pages 96–104. June 2013. doi:10.1109/MWC.2013.6549288

[65] T. R. Andel and A. Yasinsac. **On the credibility of MANET simulations**. IEEE Computer. Volume 39, Issue 7, Pages 48–54. July 2006. doi: 10.1109/MC.2006.242

[66] S. Kurkowski, T. Camp and M. Colagrosso. **MANET simulation studies: the incredibles.** ACM SIGMOBILE Mobile Computing and Communications Review. Volume 9, Issue 4, Pages 50–61. October 2005. doi: 10.1145/1096166.1096174

[67] D. Kotz, C. Newport and C. Elliott. **The mistaken axioms of wireless-network research.** Dartmouth College Computer Science Technical Report. Dartmouth TR2003-467. July 2003.

[68] P. Di, Y. Houri, K. Kutzner and T. Fuhrmann**. Towards Comparable Network Simulations**. Department of Computer Science, University of Karlsruhe. Internal Report 2008-9. Aug 2008.

[69] M. Takai, J. Martin and R. Bagrodia. **Effects of wireless physical layer modeling in mobile ad hoc networks**. International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2001). Long Beach, USA October 2001. doi:10.1145/501426.501429

[70] M. Takai, R. Bagrodia, A. Lee and M. Gerla. **Impact of channel models on simulation of large scale wireless networks**. The 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems (MSWiM 1999). Seattle, USA. August 1999. doi:10.1145/313237.313243

[71] A. Iyer, C. Rosenberg, and A. Karnik. **What is the right model for wireless channel interference?** IEEE Transactions on Wireless Communications. Volume 8, Issue 5, Pages 2662–2671. May 2009. doi:10.1109/TWC.2009.080720

[72] S, Cocorada and I. Szekely. **Simulation-Based Performance Analysis of Multicast Transmissions in an 802.11g WLAN**. The International Symposium on In Signals, Circuits and Systems (ISSCS 2007). Iasi, Romania. July 2007. doi: 10.1109/ISSCS.2007.4292735

[73] A. Quintana. **INETMANET Framework for OMNeT**. Retrieved from http://webpersonal.uma.es/~AARIZAQ/. Last modification in September 2010.

[74] G. Judd and P. Steenkiste. **Characterizing 802.11 wireless link behavior**. Wireless Networks. Volume 16, Issue 1, Pages 167–182. January 2010. doi:10.1007/s11276-008-0122-5

[75] A. Al-Jubari, M. Othman, B. Mohd Ali and N. A. W. Abdul Hamid. **TCP performance in multi-hop wireless ad hoc networks: challenges and solution**. EURASIP Journal on Wireless Communications and Networking. Volume 2011, Article 198. doi:10.1186/1687-1499-2011-198

[76] Z. Fu, X. Meng and S. Lu. **How bad TCP can perform in mobile ad hoc networks.** In Seventh International Symposium on Computers and Communications (ISCC 2002). Naxos, Italy. July 2002. doi:10.1109/ISCC.2002.1021693

[77] I. D. Chakeres and E.M. Belding-Royer. **The utility of hello messages for determining link connectivity**. The 5th International Symposium on Wireless Personal Multimedia Communications. Honolulu, Hawaii. October 2002. doi:10.1109/WPMC.2002.1088225

[78] C. Gomez, M. Catalan, X.Mantecon, J. Paradells and A. Calveras. **Evaluating Performance of Real Ad-hoc Networks Using AODV with Hello Message Mechanism for Maintaining Local Connectivity**. IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications. Berlin, Germany. September 2005. doi:10.1109/PIMRC.2005.1651656

[79] C.E. Koksal and H. Balakrishnan. **Quality-Aware Routing Metrics for Time-Varying Wireless Mesh Networks.** IEEE Journal on Selected Areas in Communications. Volume 24, Issue11, Pages 1984–1994. November 2006. doi:10.1109/JSAC.2006.881637

[80] A. Vlavianos, L.K. Law, I. Broustis, S.V. Krishnamurthy and M. Faloutsos. **Assessing link quality in IEEE 802.11 Wireless Networks: Which is the right metric?** The IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008). Cannes, France. September 2008. doi:10.1109/PIMRC.2008.4699837

[81] H. Lundgren, E. Nordströ and C. Tschudin. **Coping with communication gray zones in IEEE 802.11b based ad hoc networks**. The 5th ACM international workshop on Wireless mobile multimedia (WOWMOM 2002). Atlanta, USA. September 2002. doi:10.1145/570790.570799

[82] E. Ancillotti, R. Bruno, and M. Conti. **Experimentation and performance evaluation of rate adaptation algorithms in wireless mesh networks**. The 5th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN 2008). Vancouver, Canada. October 2008. doi:10.1145/1454609.1454612

[83] R. Prosad, C. Davrolis, M. Murray and K. C. Claffy. **Bandwidth estimation: metrics, measurement techniques, and tools.** IEEE Networks. Volume 17, Issue 6, Pages 27–35 November 2003. doi:10.1109/MNET.2003.1248658

[84] C. Dovrolis, P. Ramanathan and D. Moore. **What do packet dispersion techniques measure?** 20th IEEE International Conference on Computer Communications (INFOCOM 2001). Alaska, USA. April 2001. doi: 10.1109/INFCOM.2001.916282

[85] P. Chung and S.C. Liew. **Throughput Analysis of IEEE 802.11 Multi-Hop Ad Hoc Networks**. IEEE/ACM Transactions on Networking. Volume 15, Issue 2, Pages 309–322. April 2007. doi: 10.1109/TNET.2007.892848

[86] S. Ray, J.B. Carruthers and D. Starobinski. **RTS/CTS-induced congestion in ad hoc wireless LANs**. IEEE Wireless Communications and Networking Conference (WCNC 2003). New Orleans, USA. March 2003. doi: 10.1109/WCNC.2003.1200611

[87] L. Chen and W.B. Heinzelman**. QoS-Aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks**. IEEE Journal on selected areas in communications. Volume 23, Issue 3, Pages 561-572. March 2005. doi: 10.1109/JSAC.2004.842560

[88] Waharte, B. Ishibashi, R. Boutaba and D. Meddour. **Interference-Aware Routing Metric for Improved Load Balancing in Wireless Mesh Networks.** IEEE International Conference on Communications (ICC 2008). Beijing, China. May 2008. doi: 10.1109/ICC.2008.56

[89] W. Kim, J. Lee, T. Kwon, S.J. Lee and Y. Choi. **Quantifying the Interference Gray Zone in Wireless Networks: A Measurement Study**. IEEE International Conference on Communications (ICC 2007). Glasgow, Scotland. June 2007. doi:10.1109/ICC.2007.619

[90] S.J. Lee and M. Gerla. **Dynamic load-aware routing in ad hoc networks.** IEEE International Conference on Communications (ICC 2001). Helsinki, Finland. June 2001. doi:10.1109/ICC.2001.937263

[91] H. Hassanein and A. Zhou. **Routing with load balancing in wireless Ad hoc networks**. The 4th ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems (MSWIM 2001). Rome, Italy. July, 2001. doi: 10.1145/381591.381614

[92] A. Raniwala, P. De, S. Sharma, R. Krishnan and T. C. Chiueh. **Globally fair radio resource allocation for wireless mesh networks.** IEEE International Symposiumon Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS 2009). London, United Kingdom. September 2009. doi: 10.1109/MASCOT.2009.5366631

[93] C. Chaudet, D. Dhoutaut and I.G. Lassous. **Experiments of Some Performance Issues with IEEE 802.11b in Ad Hoc Networks**. Second Annual Conference on Wireless On-demand Network Systems and Services (WONS 2005). Lugano, Italy. January 2005. doi:10.1109/WONS.2005.16

[94] L. Xiaolong and Z. Qing-An. **Capture Effect in the IEEE 802.11 WLANs with Rayleigh Fading, Shadowing, and Path Loss**. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. (WiMob 2006). Montreal, Canada. June 2006. doi:10.1109/WIMOB.2006.1696386

[95] A. Lyakhov, I. Pustogarov, A. Safonov and M. Yakimov. **Starvation effect study in IEEE 802.11 mesh networks.** 6th International Conference on Mobile Adhoc and Sensor Systems (MASS 2009) Macau, China. October 2009. doi:10.1109/MOBHOC.2009.5336940

[96] P. Fuxjager, D. Valerio and F. Ricciato. **The myth of non-overlapping channels: interference measurements in IEEE 802.11**. Fourth Annual Conference on Wireless on Demand Network Systems and Services (WONS 2007). Oberguyrgl, Austria. January 2007. doi: 10.1109/WONS.2007.340486

[97] J. Nachtigall, A. Zubow and J.-P. Redlich. **The Impact of Adjacent Channel Interference in Multi-Radio Systems using IEEE 802.11**. International Wireless Communications and Mobile Computing Conference (IWCMC 2008).Crete, Greece. August 2008. doi: 10.1109/IWCMC.2008.151

[98] Y. Ding, Y. Huang, G. Zeng and L. Xiao. **Using Partially Overlapping Channels to Improve Throughput in Wireless Mesh Networks**. IEEE Transaction on Mobile Computing. Volume 11, Issue 11, Pages 1720–1733. November 2012. doi:10.1109/TMC.2011.215

[99] A. Raniwala, K. Gopalan and T.C. Chiueh. **Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks**. ACM SIGMOBILE Mobile Computing and Communications Review. Volume 8, Issue 2, Page 50–65. April 2004. doi: 10.1145/997122.997130

[100] H. Skalli, S. Ghosh, S.K. Das and L. Lenzini. **Channel Assignment Strategies for Multiradio Wireless Mesh Networks: Issues and Solutions**. IEEE Communications Magazine. Volume 45, Issue 11, Pages 86–95. doi: 10.1109/MCOM.2007.4378326

[101] K.N. Ramachandran, E.M. Belding, K.C. Almeroth and M.M. Buddhikot. **Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks**. 25th IEEE International Conference on Computer Communications (INFOCOM 2006). Barcelona, Spain. April 2006. doi:10.1109/INFOCOM.2006.177

[102] D. Murra, T. Koziniec and M. Dixon. **An Analysis of Handoff in Multi-band 802.11 Networks**. IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2007). Pisa, Italy. October 2007. doi::10.1109/MOBHOC.2007.4428661

[103] Y. Yang and J. Wang. **Design Guidelines for Routing Metrics in Multihop Wireless Networks**. The 27th Conference on Computer Communications (INFOCOM 2008). Phoenix, USA. April 2008. doi:10.1109/INFOCOM.2007.222

[104] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer and K. Almeroth. **On the Design and Implementation of Infrastructure Mesh Networks**. IEEE Workshop on Wireless Mesh Networks (WiMesh 2005). Santa Clara, USA. September 2005.

[105] T. Clausen, C. Dearlove, J.Dean and C. Adjih. **Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format.** RFC 5444. IETF MANET Group. February 2009.

[106] T. Clausen, C. Dearlove and J.Dean. **Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP).** RFC 6130. IETF MANET Group. April 2011.

[107] L. Hanzo and R. Tafazolli. **Admission control schemes for 802.11-based multi-hop mobile ad hoc networks: a survey.** IEEE Communications Surveys and Tutorials. Volume 11, Issue 4, Pages 78-108. December 2009. doi: 10.1109/SURV.2009.090406

[108] T.B. Reddy, I. Karthigeyan, B.S. Manoj and C.S.R. Murthy. **Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions.** Elsevier Ad Hoc Networks. Volume 4, Issue 1, Pages 83-124. January 2006. doi: 10.1016/j.adhoc.2004.04.008

[109] S. Mueller, R. P. Tsang and D. Ghosal. **Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges.** Lecture Notes in Computer Science, Performance Tools and Applications to Networked Systems. Volume 2965, Pages 209-234. April 2004. doi: 10.1007/978-3-540-24663-3_10

[110] S. Waharte and R. Boutaba. **Totally Disjoint Multipath Routing in Multihop Wireless Networks**. IEEE International Conference on Communications (ICC 2006). Istanbul, Turkey. June 2006. doi: 10.1109/ICC.2006.255550

[111] S.J. Lee, E.M. Belding-Royer, and C.E. Perkins. **Scalability study of the ad hoc on-demand distance vector routing protocol**. International Journal of Network Management. Volume 13, Issue 2, Pages 97–114. April 2003. doi: 10.1002/nem.463

[112] X. Hong, X. Kaixin and M. Gerla. **Scalable routing protocols for mobile ad hoc networks**. IEEE Networks. Volume 16, Issue 4, Pages 11–21. August 2002. doi: 10.1109/MNET.2002.1020231

[113] Z.J Haas and M.R. Pearlman. **The performance of query control schemes for the zone routing protocol.** IEEE/ACM Transactions on Networking. Volume 9, Issue 4, Pages 427–438. August 2001. doi: 10.1109/90.944341

[114] Open-mesh.org. BATMAN protocol concept. Retrieved from http://www.open-mesh.org/projects/open-mesh/wiki/BATMANConcept. Accessed in October 2015.

[115] W.A.M. Junior, R.L. Gomes and A.J.G. Abelem. **A multiple-metric approach for routing in Wireless Mesh Networks.** IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops (WOWMOM 2009). Kos, Greece. June 2009. doi:10.1109/WOWMOM.2009.5282473

[116] J.P. Vasseur, M. Kim, K- Pister, N. Dejean and D. Barthel. **Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks.** RFC 6551. IETF MANET Group. March 20112.

[117] D. Passos, C.V.N. Albuquerque, M.E.M. Campista, L.H.M.K. Costa and O.C.M.B. Duarte. **Minimum loss multiplicative routing metrics for wireless mesh networks**. Journal of Internet Services and Applications. Volume 1, Issue 3, Pages 201-214. February 2011. doi:10.1007/s13174-010-0015-6

[118] B. Awerbuch, D. Holmer and H. Rubens. **The medium time metric: high throughput route selection in multi-rate ad hoc wireless networks**. Mobile Networks and Application. Volume 11, Issue 2, Pages 253 – 266. April 2006. doi:10.1007/s11036-005-4477-x

[119] M. Arisoylu, S. Ergut, R.L. Cruz and R. Rao Ramesh. **Packet Size Aware Path Setup for Wireless Networks**. The 5th IEEE Consumer Communications and Networking Conference (CCNC 2008). Las Vegas, USA, January 2008. doi:10.1109/ccnc08.2007.8

[120] W. Jiang, S. Liu, Y. Zhu and Z. Zhang. **Optimizing Routing Metrics for Large-Scale Multi-Radio Mesh Networks**. International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2007). Shanghai, China. September 2007. doi: 10.1109/WICOM.2007.390

[121] M. Genetzakis and V.A. Siris **A Contention-Aware Routing Metric for Multi-Rate Multi-Radio Mesh Networks**. 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2008). San Francisco, USA. June 2008. doi:10.1109/SAHCN.2008.38

[122] R. Langar, N. Bouabdallah, R. Boutaba and G. Pujolle. **Interferer Link-Aware Routing in Wireless Mesh Networks**. IEEE International Conference on Communications (ICC 2010). May 2010. Cape Town, Southafrica. doi:10.1109/ICC.2010.5502159

[123] H. Aiache, V. Conan, L. Lebrun and S. Rousseau. **A load dependent metric for balancing Internet traffic in Wireless Mesh Networks**. The 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MAHSS 2008). Atlanta, USA. September 2008. doi:10.1109/MAHSS.2008.4660098

[124] L. Ma and M.K. Denko. **A Routing Metric for Load-Balancing in Wireless Mesh Networks**. The 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 2007). Ontario, Canada. May 2007. doi:10.1109/AINAW.2007.50

[125] A-N. Le, D-W. Kum, Y-Z. Cho and I-S. Lee. **LARM: A Load-Aware Routing Metric for multi-radio Wireless Mesh Networks**. International Conference on Advanced Technologies for Communications (ATC 2008). Hanoi, Vietnam. October 2008. doi:10.1109/ATC.2008.4760546

[126] D.M. Shila and T. Anjali. **Load-aware Traffic Engineering for Mesh Networks**. The 16th International Conference on Computer Communications and Networks (ICCCN 2007). Hawaii, USA. August 2007. doi: 10.1109/ICCCN.2007.4317955

[127] J. Sangiamwong and T. Sugiyama. **Hidden Node Problem Aware Routing Metric for Wireless LAN Mesh Networks**. The 18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC, 2007). Athens, Greece. September 2007. doi:10.1109/PIMRC.2007.4394208

[128] A.P. Subramanian, M.M. Buddhikot and S.C. Miller. **Interference aware routing in multi-radio wireless mesh network**. The Second International Workshop on Wireless Mesh Networks (WiMesh 2006). Reston, USA. September 2006. doi: 10.1109/WIMESH.2006.288620

[129] Open-mesh.org. **The OLSR.ORG story**. Retrieved from http://www.open-mesh.org/projects/open-mesh/wiki/The-olsr-story. Accessed in October 2015.

[130] Z.R. Zaidi and S. Shastry. **What is wrong with broadcast probing based ETX estimation for wireless links?** The 10th ACM international symposium on Mobility management and wireless access (MobiWac 2012). Paphos, Cyprus. October 2012. doi:10.1145/2386995.2387021

[131] Z. Zaidi, T.Y. Tan and Y. Cheng**. ETX Could Result in Lower Throughput**. The 18th International Conference on Computer Communications and Networks (ICCCN, 2009). San Francisco, USA. August, 2009. doi:10.1109/ICCCN.2009.5235384

[132] H. Badis, I. Gawedzki and K. Al Agha. **QoS routing in ad hoc networks using QOLSR with no need of explicit reservation**. The IEEE 60th Vehicular Technology Conference, (VTC2004-Fall). Los Angeles, USA. September 2004. doi:10.1109/VETECF.2004.1400538

[133] Guide to IP Layer Network Administration in Linux. **Routing Policy Database**. Retrieved from http://linux-ip.net/html/routing-rpdb.html. Accessed in October 2015.

[134] Miguel Catalan-Cid. **Flow-based AODV routing protocol (FB-AODV) and Weighted Contention and Interference routing Metric (WCIM) for Wireless Mesh Networks kernel module**. Available in http://sourceforge.net/projects/fbaodv

[135] J.C. Wang, M. Abolhasan, D.R. Franklin, F. Safaei and J. Lipman. **On Separating Route Control and Data Flows in Multi-radio Multi-hop Ad Hoc Networks.** The 15th IEEE International Conference on Networks (ICON 2007). Adelaide, Australia. November 2007. doi: 10.1109/ICON.2007.4444055

[136] M. Abolhasan, B. Hagelstein and J.C-P. Wang. **Real-world performance of current proactive multi-hop mesh protocols**. 15th Asia-Pacific Conference on Communications, (APCC 2009) Shanghai, China. October 2009. doi:10.1109/APCC.2009.5375690

[137] C. Gomez, D. Garcia and J. Paradells. **Improving Performance of a Real Ad Hoc Network by Tuning OLSR Parameters**. The 10th IEEE Symposium on Computers and Communications (ISCC 2005). Cartagena, Spain. June 2005. doi:10.1109/ISCC.2005.83

[138] E.M. Belding-Royer and C.E. Perkins. **Evolution and future directions of the ad hoc on-demand distance-vector routing protocol**. Elsevier Ad Hoc Networks. Volume 1, Issue 1, Pages 125–150. July 2003. doi: 10.1016/S1570-8705(03)00016-7

[139] P. Srinath, P. Abhilash and I. Sridhar. **Router handoff: a preemptive route repair strategy for AODV**. IEEE International Conference on Personal Wireless Communications (ICPWC 2002). New Delhi, India. December 2002. doi:10.1109/ICPWC.2002.1177270

[140] W. Zhu and X. Zhang. **Improve preemptive routing performance in mobile ad hoc networks with Cache-enabled method**. Third International Conference on Communications and Networking in China (ChinaCom 2008). Hagzhou, China. August 2008. doi:10.1109/CHINACOM.2008.4685128

[141] W. Zhu, X. Zhang and N. Li. **Improve TCP performance with link-aware warning method in mobile ad hoc networks**. The 4th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM 2008). Dalian, China. October 2008. doi: 10.1109/WiCom.2008.634

[142] H. Soliman and M. AlOtaibi. **An efficient routing approach over mobile wireless ad-hoc sensor networks**. The 6th IEEE Consumer Communications and Networking Conference (CCNC 2009). Las Vegas, USA. January 2009. doi: 10.1109/CCNC.2009.4784700

[143] Z.K. Lee, G. Lee, H.R. Oh and H. Song. **QoS-aware routing and power control algorithm for multimedia service over multi-hop mobile ad hoc network**. Wireless Communications and Mobile Computing. Volume 12, Issue 7, Pages 567-579. May 2007. doi: 10.1002/wcm.995

[144] A. Yaday, Y.N. Singh, R.R. Singh**. Improving Routing Performance in AODV with Link Prediction in Mobile Adhoc Networks**. Wireless Personal Communications. Volume 83, Issue 1, Pages 603-618. July 2015. doi: 10.1007/s11277-015-2411-5

[145] S. Crisostomo, S. Sargento and P. Brandao. **Improving AODV with preemptive local route repair**. International Workshop on Wireless Ad-Hoc Networks (IWWAN 2004). Oulu, Finland. June 2004. doi: 10.1109/IWWAN.2004.1525575

[146] E. Weiss, G. Hiertz, B. Xu, S. Hischke, B. Walke and S. Gross. **Improving routing performance in wireless ad hoc networks using cross-layer interactions**. Elsevier Ad Hoc Networks. Volume 5, Issue 5, Pages 579–599. July 2007. doi: doi:10.1016/j.adhoc.2006.03.003

[147] Z. Liang, Y. Taenaka, T. Ogawa and Y. Wakahara. **Pro-reactive route recovery with automatic route shortening in wireless ad hoc networks**. Tenth International Symposium on Autonomous Decentralized Systems (ISADS 2001). Tokyo, Japan. March 2011. doi: 10.1109/ISADS.2011.14

[148] A. Woo, T. Tong and D. Culler**. Taming the underlying challenges of reliable multihop routing in sensor networks**. The First International Conference on Embedded Networked Sensor Systems (SenSys 2003). Los Angeles, USA. November 2003. doi:10.1145/958491.958494

[149] M-Y. Park and S-H. Chung. **Distinguishing the cause of TCP retransmission timeouts in multi-hop wireless networks**. The 12th IEEE International Conference on High Performance Computing and Communication (HPCC 2010). Melbourne, Australia. September 2010. doi: 10.1109/HPCC.2010.68

[150] K. Chen, X. Yuan and K. Nahrstedt. **On setting TCP's congestion window limit in mobile ad hoc networks.** IEEE International Conference on Communications (ICC 2003). Alaska, USA. May 2003. doi: 10.1109/ICC.2003.1204525

[151] X. Hong, B. Gu, M. Hoque and L. Tang. **Exploring multiple radios and multiple channels in wireless mesh networks**. IEEE Wireless Communications. Volume 17, Issue 3, Pages 76-85. June 2010. doi: 10.1109/MWC.2010.5490982

[152] H.M. Ali, A. Busson, and V. Vèque. **Channel assignment algorithms: a comparison of graph based heuristics.** The 4th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks (PM2HW2N 2009). Tenerife, Spain. October 2009. doi:10.1145/1641913.1641931

[153] M. K. Marina and S. R. Das. **A topology control approach for utilizing multiple channels in multi-radio wireless mesh networks.** 2nd International Conference on Broadband Networks (BroadNets 2005). Boston, USA. October 2005. doi: 10.1109/ICBN.2005.1589641

[154] A.P. Subramanian, H. Gupta, S.R. Das. **Minimum Interference Channel Assignment in Multiradio Wireless Mesh Networks**. IEEE Transactions on Mobile Computing. Volume 7, Issue 12, Pages 1459–1473. May 2008. doi: 10.1109/TMC.2008.70

[155] C. Cicconetti, V. Gardellin, L. Lenzini and E. Mingozzi. **PaMeLA: A Joint Channel Assignment and Routing algorithm for multi-radio multi-channel Wireless Mesh Networks with grid topology**. IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS 2009). Macau, China. October 2009. doi:10.1109/MOBHOC.2009.5336997

[156] A. Adya, P. Bahl, J. Padhye, A. Wolman and L. Zhou**. A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks**. The First International Conference on Broadband Networks (BroadNets 2004). San José, USA. October 2004. doi:10.1109/BROADNETS.2004.8

[157] S. Kim and Y. Ko. **Wireless Bonding for Maximizing Throughput in Multi-Radio Mesh Networks.** The Fifth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM 2007). New York, USA. March 2007. doi: 10.1109/PERCOMW.2007.126

[158] B-J. Ko, V. Misra, J. Padhye and D. Rubenstein**. Distributed Channel Assignment in Multi-Radio 802.11 Mesh Networks**. IEEE Wireless Communications and Networking Conference (WCNC 2007). Kowloon, Hong Kong. March 2007. doi:10.1109/WCNC.2007.727

[159] A. Raniwala and T. Chiueh. **Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network**. 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005). Miami, USA. March 2005. doi:10.1109/INFCOM.2005.1498497

[160] P. Kyasanur and N. H. Vaidya. **Routing and Interface Assignment in Multi-Channel Multi-Interface Wireless Networks.** IEEE Wireless Communications and Networking Conference (WCNC 2005). New Orleans, USA. March 2005. doi:10.1109/WCNC.2005.1424834

[161] Q. Ni, L. Romdhani and T. Turletti. **A survey of QoS enhancements for IEEE 802.11 wireless LAN**: Wireless Communication and Mobile Computing. Volume 4, Issue 5, Pages 547–566. August 2004. doi: 10.1002/wcm.v4:5

[162] M. Catalán-Cid. **Diseño, Implementación y Evaluación de un Protocolo de Encaminamiento Basado en AODV para Proveer Calidad de Servicio en Redes Malladas Inalámbrica**. Final Degree Project, Universitat Politènica de Catalunya. September 2007.

[163] M. Catalán-Cid. **Diseño, Implementación y Evaluación del protocolo de encaminamiento AMPLE para redes malladas inalámbricas.** Master Thesis, Universitat Politènica de Catalunya. September 2008.

[164] I.F. Akyildiz, W-Y. Lee and K.R. Chowdhury**. CRAHNs: Cognitive radio ad hoc networks.** Elsevier Ad Hoc Networks. Volume 7, Issue 5, Pages 810–836. July 2009. doi: 10.1016/j.adhoc.2009.01.001

[165] E. Hossain, D. Niyato and I.D. Kim. **Evolution and future trends of research in cognitive radio: a contemporary survey.** Wireless Communications and Mobile Computing. Volume 15 Issue 11, Pages 1530–1564. August 2015. doi: 10.1002/wcm.2443

[166] A. Krasilov, A. Lyakhov and A. Safonov. **Interference, Even with MCCA Channel Access Method in IEEE 802.11s Mesh Networks**. The 8th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2011). Valencia, Spain. October 2001. doi:10.1109/MASS.2011.83

[167] B. Staehle, M. Bahr, D. Fu and D. Staehle. **Intra-Mesh Congestion Control for IEEE 802.11s Wireless Mesh Networks**. The 21st International Conference on Computer Communications and Networks (ICCCN 2012). Munich, Germany. August 2012. doi:10.1109/ICCCN.2012.6289277

[168] H. Huang, P. Li, S. Guo and W. Zhuang**. Software-defined wireless mesh networks: architecture and traffic orchestration.** IEEE Networks. Volume 29, Issue 4, Page 24–30. August 2015. doi:10.1109/MNET.2015.7166187

[169] P. Dely, A. Kassler and N. Bayer. **OpenFlow for Wireless Mesh Networks.** The 20th International Conference on Computer Communications and Networks (ICCCN 2011). Maui, Hawaii. August 2011. doi:10.1109/ICCCN.2011.6006100

[170] J. Paradells, M. Catalan, J. L. Ferrer, M. Catalan-Cid, X. Sánchez, V. Beltran, C. Gómez, P. Plans, E. García, J. Rubio, D. Almodóvar, and D. Rodellar . **Red mallada asistida por UMTS/GPRS.** VI Jornadas de Ingeniería Telemática (JITEL). Málaga, Spain. September 2007.

[171] J. Paradells, J.L. Ferrer, M. Catalan, W. Torres, M. Catalan-Cid, X. Sánchez, V. Beltran, E. García, C. Gómez, P. Plans, et al. **Design of a UMTS/GPRS Assisted Mesh Network (UAMN)**. The 7th Wireless World Resarch Forum Meeting (WWRF 2006). Heidelberg, Germany. 2006

[172] E. Garcia, R. Vidal and J. Paradells. **Load Balancing in WLAN through IEEE 802.11k Mechanisms.** The 11th IEEE Symposium on Computers and Communications (ISCC 2006). Murcia, Spain. June 2006. doi: 10.1109/ISCC.2006.94

[173] M. Catalan, C. Gomez, P. Plans, J. Paradells, A. Calveras, J. Rubio and D. Almodovar. **Extending Wireless Mesh Networks over UMTS: A proxy-based approach**. First International Workshop on "Wireless mesh: moving towards applications" (WIMESHNETS 2006). Waterloo, Canada. August 2006.

Appendixes

A. UMTS/GPRS ASSISTED MESH NETWORK (UAMN)

The UAMN project was a proposal of Vodafone, SwissCom Innovations, I2CAT and UPC in order to improve the performance of Wireless Mesh Networks by assisting some of its procedures with a central server located in the UMTS/GPRS network of the operator [170][171]

The architecture of the solution is shown in Fig. A- 1. The WMN is the backhaul and is formed by Mesh Nodes using IEEE 802.11a interfaces. Some Mesh Nodes also have an IEEE 802.11b/g interface, acting as AP in order to allow the access of Mesh Clients. Finally, other Mesh Nodes are defined as Gateways and use an UMTS/GPRS interface in order to offer Internet connectivity. Indeed, the rest of the nodes of the network may also have UMTS/GPRS connectivity to perform some of the signaling operations related with security, accounting and QoS, although in any case data traffic should be routed through the gateways.

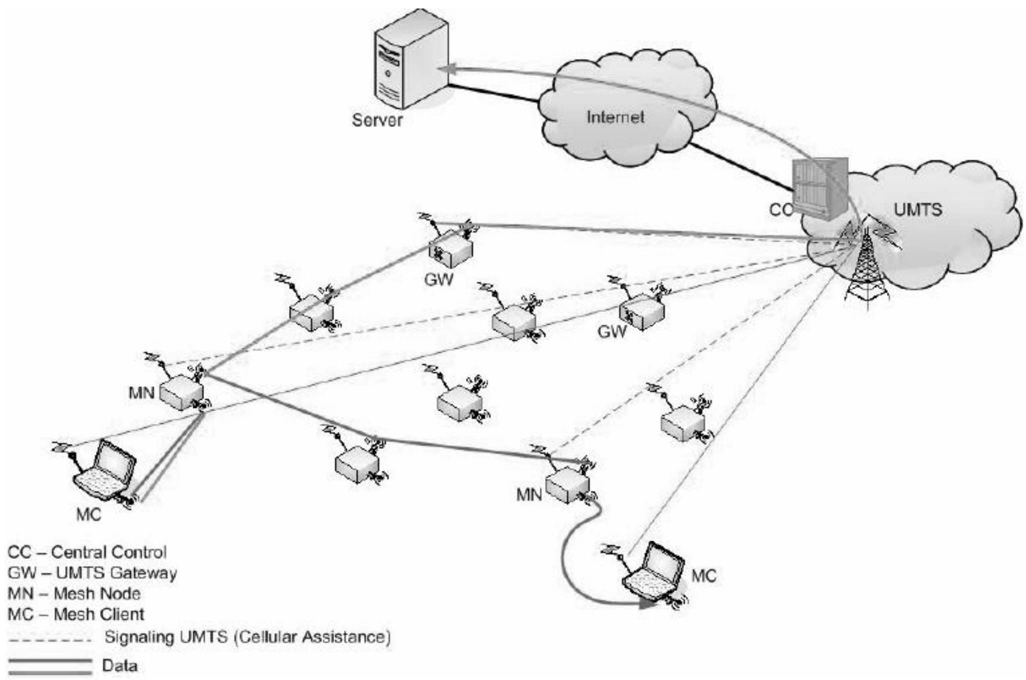


Fig. A- 1: UAMN architecture

The main design decisions and procedures of the project are described in the next paragraphs.

Security:

Since the WMN can be seen as an extension of the UMTS/GPRS network, it should offer a similar security level. This is accomplished by using the Central Control (CC) located in the operator's infrastructure. The different implemented security procedures are the following ones:

- Users are authenticated by the CC. In this phase, the user sends a list of detected AP and the CC decides the AP to which the client must associate according to a QoS mechanism. Then, the CC gives them the necessary credentials to allow a secure communication. Also, the surrounding APs are informed about the new user in order to facilitate mobility, minimizing the handoff delay if the client changes its AP.
- The Mesh Nodes make use of security keys distributed by the CC in order to secure the data traversing the backhaul, what is accomplished by using IPsec tunnels.
- The routing protocol signs its control messages with a common key in order to assure data integrity.

QoS:

The following QoS mechanisms are implemented in Mesh Nodes and Gateways:

- AP assignment protocol: After client authentication, the AP is decided by using measurements of the client (SNIR level to all detected APs) and of the surrounding APs (channel interference and load status). This way, the CC selects the AP with the best SNIR and enough empty capacity to allocate the new user. Also, APs decide their WLAN channels according to a centralized algorithm which considers external interference and the mutual interference between APs [172].
- Gateway assignment protocol: The AP selects a gateway for its new clients according to a prioritized list of Gateways (based on their available bandwidth) received from the CC and the routing metric of the paths to these Gateways. The objective is to balance load in the Internet access, but avoiding long or degraded routes. Gateways are also informed of the new users in order to implement admission control.
- Traffic classification and routing: Mesh nodes classify packets according to their ToS, prioritizing them in their queues and controlling their rates. In addition, different routing metrics and paths are used according to the ToS. Traffics with QoS requirements use a routing metric which tries to use links with a high available bandwidth, while best-effort traffics are routed through paths which minimize interference over the active QoS flows. Indeed, this routing solution can be considered an initial version of FB-AODV and WCIM.

- Protocol optimization: Optimized protocols are used in order to route traffic to the Internet in order to increase the performance of the UMTS/GPRS access. The optimization solution is based on a proxy server located in the operator’s infrastructure [173].

B. SIStema de Telecontrol Mallado Multi-radio Adaptativo (SISTEMMA)

The objective of the SISTEMMA project was to implement a multi-hop multi-radio network solution by using radios operating in UHF narrowband channels. The partners of the project were Farell Instruments, I2CAT and UPC.

The main problematic to be resolved by the project was the inefficiency of star topologies when some nodes lose their connectivity to the central station. Therefore, a multi-hop solution was proposed. However, due to the limited bandwidth of the UHF channel, implementing a MAC mechanism was discarded. Thus, multi-radio became necessary in order to avoid collisions by using orthogonal channels.

The final design of the SISTEMMA proposal contemplates the following aspects:

- Routing metric: In order to discard degraded links (e.g. due to obstacles), a routing metric based on the RSSI of the links is used. The RSSI is transformed to a link quality value according to the specifications of the radio devices.
- Common control channel and spanning tree: All nodes have at least one interface which is assigned to a common control channel. The central station, which is the destination of all the traffics, floods the network with periodic advertisements through this channel, thus creating default paths through the nodes according to the routing metric. These paths are used for traffics without reliability requirements, since collisions can occur.
- Dedicated channel and AODV: In the case of traffics which should be routed in a reliable way, the source of the traffic initiates a route discovery using AODV. Once the central station receives the RREQ, it decides a reserved channel for this flow and notifies it to the forming the path by using the RREP. The nodes which form the new path assign one of their interfaces to this channel after forwarding the RREP. This way, collisions are totally avoid without needing a MAC mechanism (intra-flow interference doesn't occur due to the low latency of the flows). In order to increase the number of concurrent flows in the network which can use dedicated channels, the nodes close to the central station should have a higher number of interfaces.

Fig. B- 1 shows the hardware architecture of the SISTEMMA nodes. As was previously introduced, the protocol layer is based on a multi-hop multi-radio solution based on AODV and Spanning Tree. Since the Linux system needs the definition of a network interface to allow IP routing over serial interfaces, the Compressed Serial Line Internet Protocol (CSLIP) is used, which requires a minimum overhead.

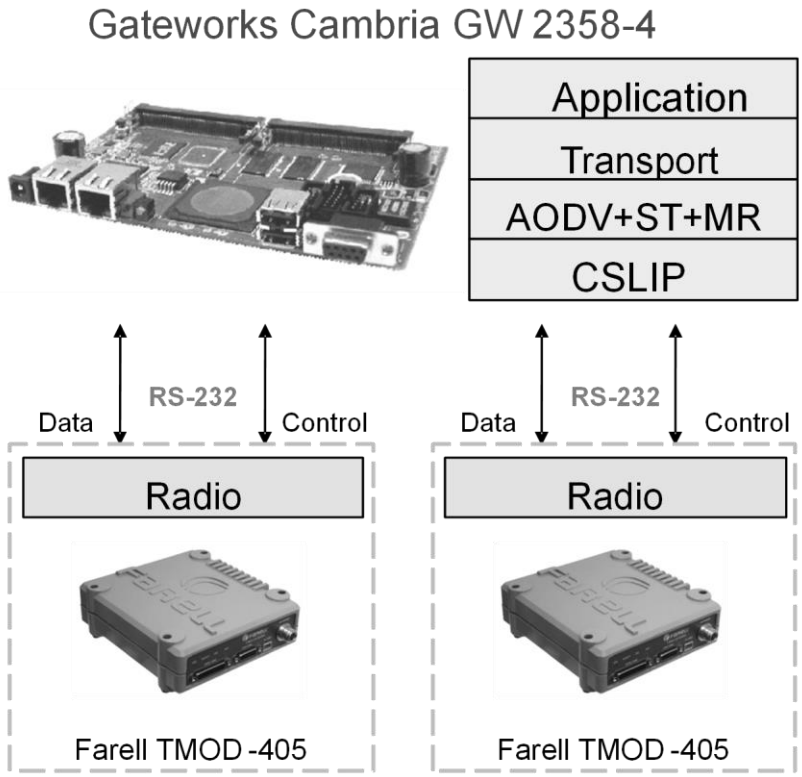


Fig. B- 1: SISTEMMA nodes

Acronyms and abbreviations

ACK	Acknowledgment
AIL	Average Interference Load
ALM	Airtime Link Metric
AODV	Ad-hoc On-demand Distance Vector
AP	Access Point
ARF	Automatic Rate Fallback
AWGN	Additive White Gaussian Noise
BATMAN	Better Approach To Mobile Ad hoc Networking
BER	Bit Error Ratio
CAA	Channel Assignment Algorithms
CATT	Contention-Aware Transmission Time
CBR	Constant Bit Rate
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CCS	Common Channel Set
CO	Channel Occupancy
CRC	Cyclic Redundancy Check
CRN	Cognitive Radio Networks
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CW	Contention Window
CWL	Congestion Window Level

CSC	Channel Switching Cost
CSLIP	Compressed Serial Line Internet Protocol
dB	Decibel
DBPSK	(Differential) Binary Phase Shift Keying
DCF	Distributed Coordination Function
DEMON	performance DEgradation MONitoring
DFS	Dynamic Frequency Selection
DIFS	DCF Interframe Space
DQPSK	(Differential) Quadrature Phase Shift Keying
DSP	Digital Signal Processing
DSR	Dynamic Source Routing protocol
DSSS	Direct-Sequence Spread Spectrum
ED	Energy Detection
EDCA	Enhanced Distributed Channel Access
EETT	Exclusive Expected Transmission Time
EIFS	Extended Interframe Space
ETT	Expected Transmission Time metric
ETX	Expected Transmission Count metric
FB-AODV	Flow-based AODV
EWMA	Exponentially Weighted Moving Average
FMRP	Firetide's Mesh Routing Protocol
GCA	Grid Channel Assignment
GHz	Gigahertz
GSM	Global System for Mobile communications
HNA	Host and Network Association message
HNPA	Hidden Node Problem Aware routing metric
HOPS	Hop count routing metric
HWMP	Hybrid Wireless Mesh Protocol

IAR	Interference Aware Routing metric
IoT	Internet of Things
ISM	Industrial Scientific Medical
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILA	Interference-Load Aware routing metric
IMCC	Intra-Mesh Congestion Control
INX	Interferer Neighbors Count
IRU	Interference-aware Resource Usage
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAETT	Load-Aware Expected Transmission Time metric
LARM	Load-Aware Routing Metric
LBAR	Load-Balanced Ad hoc Routing
IDCA	Interference-based Dynamic Channel Assignment
LET	Link Expiration Time
LOS	Line-Of-Sight
LSR	Link Success Rate
M2M	Machine to Machine
MAC	Medium Access Control
MANET	Mobile Ad-hoc Networks
Mbps	Megabits per second
MCA	Multi-Channel Architecture
MCCA	MCF Controlled Channel Access
MCF	Mesh Coordination Function
MIC	Metric of Interference and Channel-switching
MR-DEMON	Multi-radio DEMON
MTI	Metric of Traffic Interference

MTM	Medium Time Metric
mETX	Modified Expected Transmission Count metric
MHz	Megahertz
MIMO	Multiple-Input Multiple-Output
MID	Multiple Interface Declaration message
MILD	Metric for Interference, Load and Delay
MIT	Massachusetts Institute of Technology
MIWN	Multi-hop IEEE 802.11 Wireless Networks
MPR	Multipoint Relay
MSps	Mega Symbols per second
NED	NEtwork Description
NHDP	Neighbor Discovery Protocol
NIC	Network Interface Card
OFDM	Orthogonal Frequency-Division Multiplexing
PktPair	Packet Pair
PCF	Point Coordination Function
PD	Preamble Detection
PER	Packet Error Rate
pETX	Passive ETX
PHY	Physical Layer
PLCP	Physical Layer Convergence Procedure
PLR	Packet Loss Rate
PPDU	PLCP Protocol Data Unit
PRNG	PseudoRandom Number Generator
PSDU	PLCP Service Data Unit
PWRP	Predictive Wireless Routing Protocol
QAM	Quadrature Amplitude Modulation

QoS	Quality of Service
RAA	Rate Adaptation Algorithm
RCA	Random Channel Assignment
RERR	Route ERRor
RPDB	Linux Routing Policy DataBase
RREQ	Route Request
RREP	Route Reply
RSSI	Received Signal Strength Indication
RTT	Round Trip Time
SCA	Single-Channel Architecture
SDN	Software-Defined Network
SIFS	Short Interframe Space
SINR	Signal to Interference plus Noise Ratio
STA	Station
TC	Topology Control message
THD	Threshold
TLV	Type-Length-Value
ToS	Type of Service
TPC	Transmit Power Control
TTL	Time To Live
TXOP	Transmit Opportunity
UAMN	UMTS Assisted Mesh Network
UB	Unproductive Busyness ratio
UHF	Ultra High Frequency
VANET	Vehicular Ad Hoc Network
VCS	Virtual Carrier Sensing
VHF	Very High Frequency
VoIP	Voice over IP

WCIM	Weighted Contention and Interference routing Metric
WCETT	Weighted Cumulative Expected Transmission Time routing metric
WCETT-LB	Weighted Cumulative Expected Transmission Time with Load Balancing routing metric
WEP	Wired Equivalent Privacy
WMEWMA	Window Mean Exponentially Weighted Moving Average
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network
ZRP	Zone Routing Protocol