El títol de la tesi: Obligatori

El subtítol de la tesi: Opcional

Autor: Obligatori

TESI DOCTORAL UPF / ANY L'any de la tesi: Obligatori

DIRECTOR DE LA TESI
Director: Obligatori Departament Departament: Obligatori

Escriviu aquí la vostra dedicatòria

Acknowledgments This work was partially supported by the European Commission through the project Commons for Europe (CIP-ICT-PSP-2011-5-297191)

Abstract

This is the abstract of the thesis in English. Please, use less than 150 words.

Resum

Vet aquí el resum de la tesi en català. Si us plau, utilitzeu menys de 150 paraules.

Prefaci

Contents

List of Figures

List of Tables

List of Abbreviations

WMN Wireless Mesh Networks

AP Access Point

BSS Basic Service Set

MANET Mobile Ad-Hoc Network

GSF Gracia Sense fils

QMP Quick Mesh Project

NAT Network Address Translation

BMX6 BatMan-eXperimental version 6

OLSR6 Optimized Linked State Routing version 6

DRP Dynamic Routing Protocol

IID Internal IDentifier

Chapter 1

INTRODUCTION

TODO

Chapter 2

STATE OF THE ART

This project consists on studying how are, currently, being build the open mesh networks in cities and what mechanisms we have to contribute or improve them. There are many different ways to improve this networks, namely, we can use different hardware, different software, build applications which run over them, etc.

First of all, we will analyze how these networks are, and how are they operating to have a better idea of what we want to improve.

2.1 Mesh and MANET networks

2.1.1 Definition and properties

When we talk about mesh networks, we refer to networks where all the participant are also routers. If we had to set a single definition the following can be a good one:

”*A Mesh network is one where all nodes (participants) are routers, meaning that all the nodes accept and forward packets from other nodes according to the routing rules.*” [Escrich, 2012a]

More specifically, we want to talk about Wireless Mesh Networks (WMN) which may refer also to the users of the network, and can be defined as follows:

”*Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet.*” [Huynh,] To summarize, we have that mesh networks are basically networks which are not defined by the topology (physical layer) or the kind of links between two nodes (link layer). They are defined by the way the nodes operate among them, there are not master/slave or node/supernode distinctions and so, all the nodes have a similar function. In addition, the clients (end users) do not notice any difference (between mesh or other kind of networks) when they connect to the mesh, they are totally transparent for them.

As mentioned above, there are only two different kind of nodes: mesh routers and mesh gateways. They operate in exactly the same way when they have to route packets within the network, the only difference is that the gateways may be connected to a wider network, namely, the Internet and they can route packets to this other network. So, mesh routers just route packets inside the mesh while mesh gateways can also route packets to the outside.

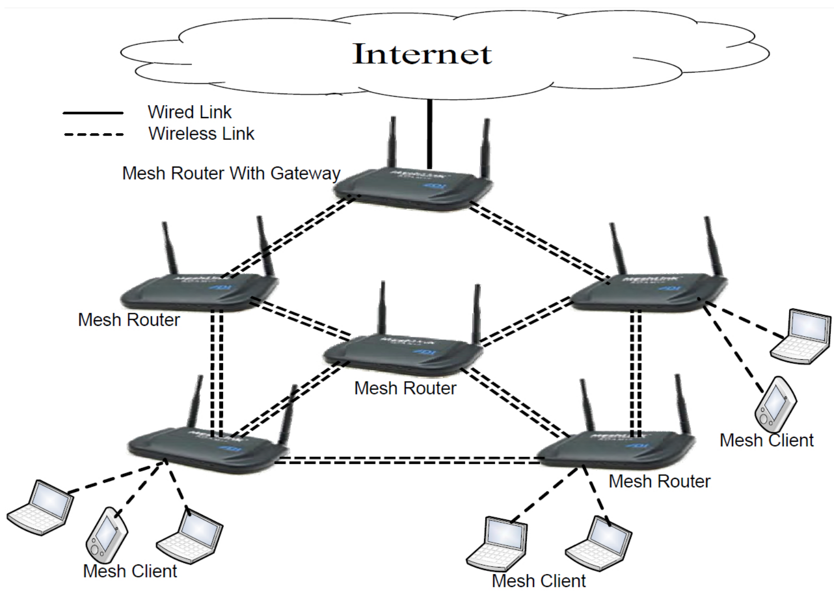

Figure 2.1: Wireless Mesh Network Example

http://www.intechopen.com/source/html/37888/media/wmn11.jpg

Then, we can say that WMN are a subtype of mesh networks. They have all the properties of these networks with the only difference that all the nodes are connected wirelessly.

2.1.2 Operating modes

Mesh networks can operate in two different modes: Infrastructure mode and Ad-Hoc mode.

- **Infrastructure Mode:** In this mode we have a central point named Access Point (AP) that creates a Basic Service Set (BSS) zone in which all the packets have to go through the AP. This zone is identified by the MAC address of the AP, which is called BSSID in this context. Furthermore, we can say that a master/slave model is followed in infrastructure mode.

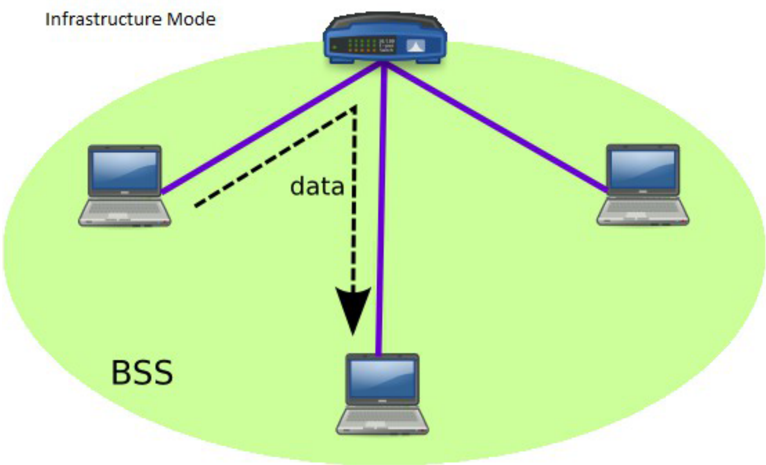

Figure 2.2: Infrastructure Mode BSS

[Escrich, 2012b]

- **Ad-Hoc Mode:** In Ad-Hoc mode, all the participants play the same role. Therefore, every single node connects with all the nodes it can, and so the central point idea disappears. To identify which participants are in the same network we just need to find those who have the same BSSID. At this point, all the machines directly connected can exchange information but, a layer 3 routing protocol is required to allow the communication between nodes which are not connected directly.

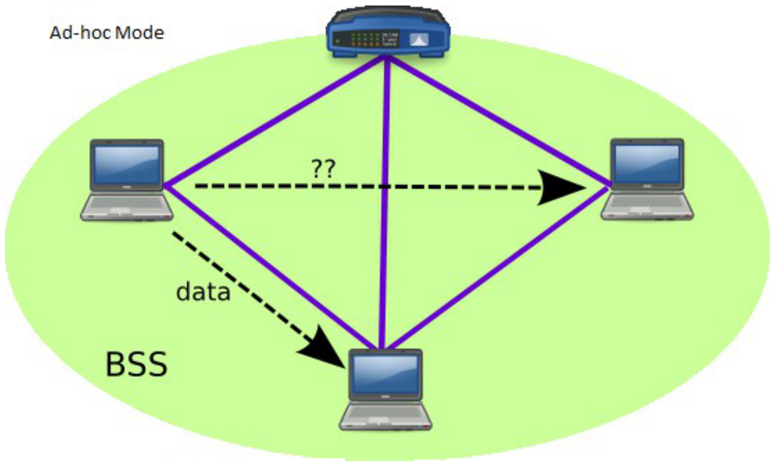

Figure 2.3: Ad-Hoc Mode BSS

[Escrich, 2012b]

2.1.3 MANET Networks

MANET is a subtype of a mesh network. That is to say, when we have a mesh network which uses a wireless system to interconnect the nodes and is built in Ad-hoc mode, we talk about MANET. Another way to define it can be: A MANET network is a WMN which operates in Ad-Hoc mode.

Usually, when we talk about MANET we are also referring to networks which have a self-configuring property. This property relies on the fact that the routers within the network are free-to-move anytime and to anywhere. A good definition could be this:

"A Mobile Ad hoc NETwork (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) con-

nected by wireless links - the union of which forms an arbitrary topology."[Ramesh et al., 2010]

2.2 Open MANET Networks in Barcelona

Nowadays, in Barcelona (and in some other cities) some MANET networks are being deployed. We will study this case in particular because is the one we are more familiar with. In general terms, all the deployments work in the same manner and so, studying one single case can give us a general a idea of all of them.

Normally, all these deployments only differ in some points, these are the more relevant ones:

- The funding scheme
- The kind of hardware
- The firmware used

2.2.1 Funding scheme in Barcelona's MANET networks

There are some examples of MANET networks successfully deployed in Barcelona:

- Gràcia
- Sants
- Poble Nou
- Sant Joan Despí

All these networks have been deployed using the same funding scheme, promoted by the Guifi.net foundation, and is, somehow, based on crowd-funding. Basically, anyone can install a new node and join to the mesh. There is just one restriction: you have to have direct vision with, at least, another node in the network. If you achieve this requirement, you can buy and install the node yourself and you expand the network. So, this is crowd-funding because every person joining the network funds its own equipment, which has the only requirement of being compatible with the firmware used. Since many people has no experience on installing and configuring the nodes, and despite the fact that both the hardware and software are specially designed to allow non-technical people to use it without problems, the foundation provides technical support for those who do not achieve in the installation.

2.2.2 The Kind of hardware in Barcelona's MANET networks

Being that the users are the owners of the network and so, the people who buy the equipment, usually low-cost hardware is used. Low-cost does not mean, low-quality, in fact some of the hardware used have very high features and a very good performance. Normally, the hardware used is from Ubiquity Networks (NanoStation, Rocket, Bullet, etc.), but it is not strictly necessary. Actually, any hardware compatible with the linux distribution openWRT is accepted.

There are more information about some of this devices in annex 2.

2.2.3 The Firmware used in Barcelona's MANET networks

This is maybe the most important difference between all the deployments around the world. In most of them, there is a common point: all the firmwares are openWRT based, but they have some differences. Particularly, in Barcelona the first deployments used the Gracia Sense fils (GSF) firmware, developed since 2003 for the Gracia Sense Fils Wireless Community[1]. Some year later, the firmware became outdated since the protocol versions where old and the configuration of the nodes was hard. Then, they decided to create a new firmware with bigger scope, they named it QMP and is the one being used currently (some nodes have to be migrated to QMP yet).

QMP has been chosen in Barcelona because is a firmware that covers perfectly the needs in the deployments carried out there, and has been developed by themselves. Nowadays, in most of the deployments a new firmware is designed specially for them, and despite the fact that many of them could be used in other deployments, it does not normally happen. It is not an efficient way to work, and because of it a new initiative has just started, it is called ”libre-mesh”[2]. This initiative tries to build a new firmware based on three existent ones: QMP (Spain), AlterMesh (Argentina) and eigenNet (Italy). It can be a good opportunity to merge all the best points of every firmware a create a new version that fits in many different scenarios.

2.3 QMP firmware basics

[3]

[1] More information at: http://graciasensefils.net/

[2] More information at: http://libre-mesh.org/

[3] http://qmp.cat

2.3.1 Main Features

QMP is an Operating System designed for embedded devices, a firmware. The main features of this firmware are:

- OpenWRT based
- 802.11a/b/g/n support
- IPv6 native
- IPv4 tunneled over IPv6
- Auto configuration system
- Web GUI to monitor and configure
- Visualization tools (maps, graphs, etc.)
- Automatic dynamic routing (zero-conf)
- BGP (Border Gateway Protocol) support
- Open Source

2.3.2 Quick Deployments

QMP has been specially designed and developed to achieve quick network deployments. To do so, they have created the auto configuration feature which plays a very important role within the firmware. When we talk about quick deployments, we mean that we have to accomplish these requirements:

- The deployment must be performed as fast as possible.
- It must be able to be done by non-technical people.
- It must be possible in most situations.

2.3.3 Addressing

QMP uses three different kind of IP addresses:

- IPv6 ULA: IPv6 private range to be used internally in the mesh. These IPs are used for the communication among the nodes in the mesh network, and so they are not neither valid nor routable outside.

- IPv6 RIPE: IPv6 public IPs range (6to6 tunneling). These are globally valid and routable.

- IPv4: IPv4 private range to connect with the final user (4to6 tunneling). They are assigned to the final users attached to a node in the mesh, when they transmit any packet that has to travel throughout the mesh it is encapsulated in an IPv6 packet (tunneling).

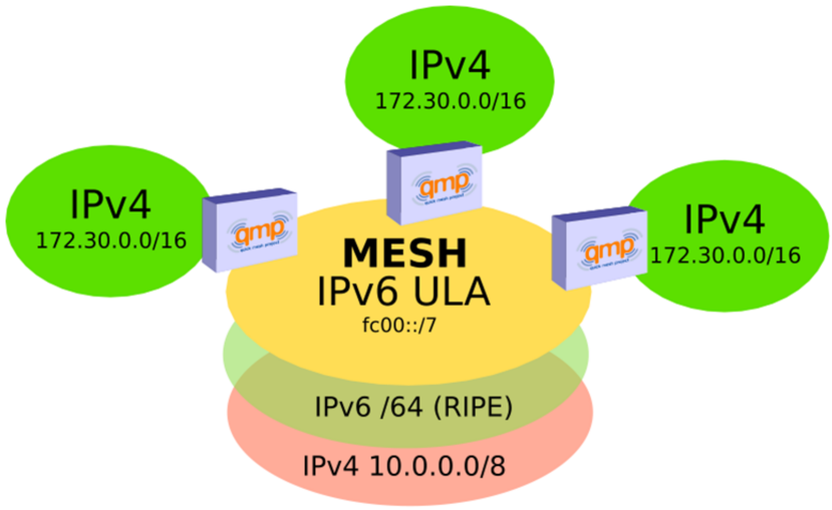

Figure 2.4: QMP Addressing

[Escrich, 2012b]

2.3.4 Operating modes

The firmware has two different operating modes, depending on the scenario we should choose one or the other:

- Roaming for fast deployments: All the access points in this mode will have the same IP and the same ESSID in order to allow users mobility, namely, they will not lose the connection although they switch from an AP to another. Every AP implements a Network Address Translation (NAT) and so, two users attached to different APs will not have direct vision between them.

- Community: Every node will have a randomly assigned IPs range and will announce this range through the mesh. There is not NAT, every user has direct vision with the others (1 hope away from the IPv4 network layer point of view), but mobility is not allowed (no roaming).

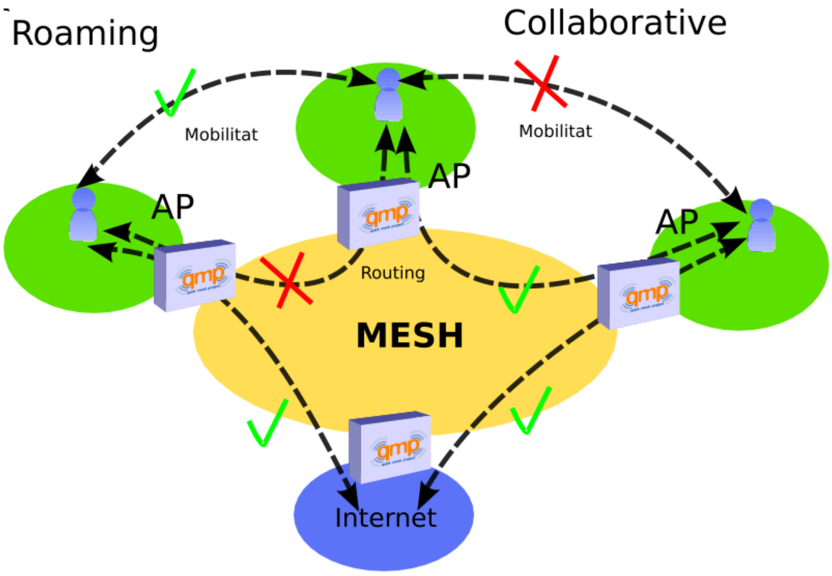

Figure 2.5: QMP Operating Modes

[Escrich, 2012b]

2.3.5 DRP

The firmware uses different protocols:

- BMX6 as the main DRP.
- Optimized Linked State Routing version 6 (OLSR6) as a backup DRP.
- Babel as a backup DRP but optional.

Usually, two networks are built in parallel the main one using BMX6 and the backup on using OLSR6. There are two reasons for that:

1. To prevent that a node gets isolated (no neighbors) due to a single BMX6 failure.
2. To make performance measurements of both protocols in exactly the same environment. This was very useful at the beginning of the project to decide which protocol was better in every scenario.

All these three protocols use IPv6 ULA to talk to other nodes and are isolated at the link layer (MAC) using VLANs. It allows the protocols to work in parallel (if necessary) without interfering with the other protocols.

2.3.6 BMX6

Since BMX6 is the main DRP we are going to analyze it deeply:

BMX6 is a table-driven routing protocol for wireless mesh networks. [...] its goal is to compose a path from source to destination by deciding on each node which will be the next hop. BMX6 is a distance vector protocol, since the information each node manages is [...] destination node, next hop and cost. [Neumann et al., 2012]

In terms of dissemination - how the nodes exchange the information - we can distinguish between two different states: transient and steady.

- Transient phase: the nodes exchange information related to the environment: Internal IDentifier (IID), nodes description, links, etc. Thanks to this information, ever single node builds a dictionary table that translates between IID to the global hashes of the full node description.

- Steady phase: every node has local information state (IID-to-hash dictionary) and global information state as hash-to-description. So, during this phase there is just a small exchange of packets that inform about link metrics and network changes. Thank to the tables set up in transient phase, those packet do not need to use the 128 bit IPv6 address as the identifier, they can use the 16 bit IID which produces a much lower overhead.

To summarize, we can say say that BMX6 controls the overhead better than other protocols (some experiments demonstrate that, for example: [Neumann et al., 2012]) there is a big overhead at the very beginning (transient state) and later it becomes very low during the steady state. So the main features of this protocol are:

- Pro-active: Uses UDP flooding to periodically send Originator Messages (OGM) and build a routing table.

- Destination-sequenced, Distance-vector (DSDV): Every node just knows which neighbor is better to reach another, namely, they do not need to know the entire topology, just the best paths.

- Does not use IP as node identifier, it uses global identifiers using SHA2 hashing.

In terms of the kind of frames used by BMX6 we have two different types: periodic messages, periodically generated on every node and occasional messages, exchanged only when necessary. The most used are the periodical which are the following:

Frame name	**Description**
HELLO_ADV	Hello advertisement. Used for letting neighboring nodes detect the link quality in transmit direction (from sending to receiving node).
RP_ADV	Rx probe advertisement. Used for reporting about reception rate of hello messages from neighbouring nodes.
OGM_ADV	OGM advertisement. Used for updating periodically route and metric information over the mesh.
OGM_ACK	OGM acknowledgment. Used for acknowledging the previously reception of a full OGM_ADV frame.

Table 2.1: BMX6 Frames

[Escrich, 2012a]

Chapter 3

METHODOLOGY

This thesis has mostly followed a trial and error methodology during the experiments. In general terms, has also, somehow, followed an agile approach.

Chapter 4

CONTRIBUTION

Chapter 5

RESULTS

TODO

Chapter 6

CONCLUSIONS

TODO

Chapter 7

FUTURE WORK

TODO

Bibliography

[Escrich, 2012a] Escrich, P. (2012a). Quick deployment network using MANET. Degree thesis.

[Escrich, 2012b] Escrich, P. (2012b). Xarxes mesh. curs guifi.net 2012. Presentation.

[Huynh,] Huynh, P. Simulation and analysis of wireless mesh network in advanced metering infrastructure.

[Mogaibel et al., 8 14] Mogaibel, H. A., Othman, M., Subramaniam, S., and Hamid, N. A. W. A. (2012-08-14). Wireless mesh networks - efficient link scheduling, channel assignment and network planning strategies.

[Neumann et al., 2012] Neumann, A., Lopez, E., and Navarro, L. (2012). An evaluation of bmx6 for community wireless networks. *International Workshop on Community Networks and Bottom-up-Broadband (CNBuB 2012).*

[Ramesh et al., 2010] Ramesh, V., Subbaiah, D. P., Rao, N. K., and Raju, M. J. (2010). Performance comparison and analysis of dsdv and aodv for manet. *International Journal on Computer Science and Engineering*, 2(02):183–188.