Implementation Issues for the Deployment of a WMN with a Hybrid Fixed/Cellular Backhaul Network in Emergency Situations

Elias Chafic Haddad [#1], Jean-Charles Grégoire [*2]

[#] *Department of Electrical Engineering, Faculty of Engineering (ESIB), St-Joseph University*
CST-Mar Roukoz, Mkalles, PO Box 11-0514, 1107 2050, Beirut, LEBANON
[1] elias.haddad@fi.usj.edu.lb

[*] *INRS-EMT, Place Bonaventure 800, de la Gauchetière O. bureau 6900, Montréal,QC H5A 1K6 Canada*
[2] gregoire@emt.inrs.ca

***Abstract*- In this paper we present a research project of the research council of St-Joseph University (USJ) at its faculty of engineering (ESIB) in Beirut, Lebanon, in collaboration with professors at INRS-EMT, Montreal Canada. This project aims at addressing the issues of deployment of a *Wireless Mesh Network* (WMN) on parts of the Lebanese territory, supported by an already installed dense infrastructure of WiFi hotspots (in urban areas), cellular and fixed telecommunications networks. In particular, we wish to address issues of using such networks in emergency situations, where parts of the telecommunications infrastructure have been damaged, with the need to maintain predominantly voice communications and urgent data communications over any available telecommunications infrastructure that is still operational. The architecture that we look at is a two-tier WMN supporting VoIP and data communications between *mesh clients* and *mesh routers* (tier 1), with *mesh routers* either communicating directly between themselves or, in case of overload or priority traffic, via a backhaul network based on the cellular (GPRS/EDGE) or fixed telecommunications network (tier 2). In this paper, we discuss the issues to be addressed in such a scenario, particularly admission control and priorities with limited backhaul resources, radio interference between closely located mesh routers and clients, and other related issues.**

The structure of the paper is as follows: section I will give an introduction to ad hoc wireless networks and WMN; section II will discuss the migration issues from independent WiFi hotspots to a fully connected two tier WMN, where the backhaul tier may use other types of networks; in section III, we address the issues for emergency scenarios with limited connectivity between mesh routers. In section IV, we present the simulation scenarios to be considered and the planned tests on a prototype network for a WMN that will be deployed at ESIB, Lebanon. We conclude in section V.

I. AD HOC WIRELESS NETWORKS

In the days where infrastructure-based cellular systems are deployed across the globe, the limitations and vulnerabilities of such systems are a major source of concern. The main reason is that all services offered depend on the installed infrastructure and, if this infrastructure or any part thereof suffers a disaster (either natural or intentional), the services are completely lost. Furthermore, the architecture on which these types of systems are based is typically centralized, where each user communicates ***only*** via the infrastructure with any destination, even though on some occasions communications may be local. These considerations also affect capacity, which leads to the necessity of more infrastructures to be installed in order to increase capacity. These have given rise to renewed interest in *wireless ad hoc* communications, which rely on multi-hop relaying with no or little need of infrastructure.

Ad hoc communications trace their origin back to thousand of years ago, to the use of repeaters using sound (drums, shouts, etc.) or visual signals (smoke, mirrors, fires, etc.) between source and destination, where each repeater received a signal and relayed it to the following repeater. These repeaters may or may not know the content of the messages. Nowadays, a main application of ad hoc networks is military, as demonstrated by the *Defense Advanced Research Project Agency's* (DARPA) interest through its MANET (for Mobile Ad hoc NETworking) project, which also included mobility for users [1]. Other variants have been defined further (e.g. IAMANET) to compensate deficiencies that are characteristics of the Internet, another original DARPA project. Military applications are usually required to operate in environments with no infrastructure but do not have stringent budgets or reduced costs as would civilian applications. However, like many military technologies that have found their way into civilian and commercial applications, for example spread spectrum communications implemented using CDMA technology (e.g. 2G CDMA one, 3G UMTS and CDMA 2000 systems), wireless ad hoc networks are being considered through various scenarios to complement, replace or simply be implemented in conjunction with existing systems.

Although wireless ad hoc networks are designed and able to operate with no infrastructure, we see in the case of civilian applications proposals for *Hybrid Wireless Networks* (HWN) that enable ad hoc users to use the infrastructure already installed. *Multi-Hop Cellular Networks* (MCNs) [3] are one example, as well as the Self-Organizing Packet Radio Network with Overlay (SOPRANO) network [4]. The combination of the routing capacity of the cellular network, together with the flexibility and low power budget of ad hoc users increases the capacity of the system significantly. Looking at the features of both cellular and ad hoc wireless networks, we see that they complement each other very well, which leads to clear advantage for HWNs.

Cellular networks are based on the deployment of infrastructure, a single hop link between *mobile station* (MS) and *base station* (BS), centralized routing, high cost & long deployment times, complex frequency planning and difficulties to adapt dynamically to varying conditions. Furthermore, MSes have low complexity and no role in routing. Also in countries where only 2G systems are available (GSM or CDMA-1), like in Lebanon, connections are usually circuit-switched (CS) but are now evolving to 3G and packet switching (PS). In ad hoc networks, an infrastructure is not needed: all communications are MS to MS, with some acting as relays for a multi hop operation, supported by distributed routing among the MSes, using channels that are sensed as having the least interference. In this case, MSes have more complexity and we thus have a trade-off between the intensive infrastructure of the system and the complexity of the MS. The MS will then have routing and switching capabilities, as well as self configuration and maintenance properties with low cost for both.

It is to be noted that in hybrid systems (HWN), major advantages arise in terms of used transmitted power and decreased interference in cells, as illustrated below. Figure 1 presents a case with a clear advantage for HWN over GSM in terms of power budget for the users and in terms of resources of the network consumed in routing the information from one cell to another. In the HWN case, we see that we can benefit from proximity communications, and relieve the resources of the core network.

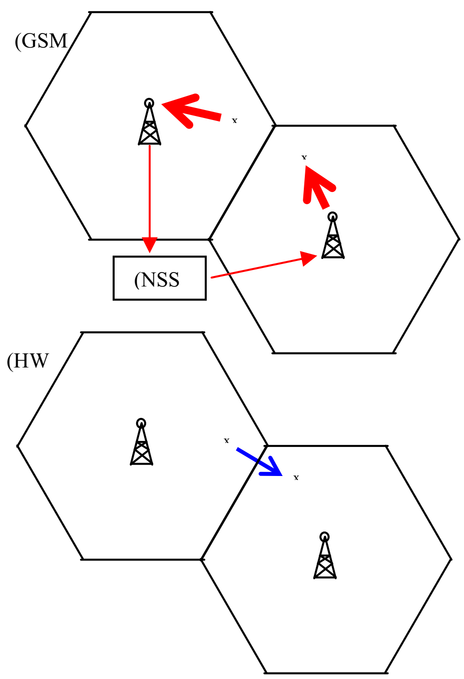

Fig. 1. Routing and power transmission for short distance users located at the cell boundaries of two different cells.

The usefulness of ad hoc networks is not restricted to the case presented above. They extend to many aspects of wireless communications, but the best cases are to complement and improve the performance of current telecommunications systems. One particular application is in the case of emergency operations where a large number of people are affected (police, firemen), ad hoc mobile networks can be deployed with minimal configuration and no infrastructure needed. Voice communications are usually the dominant applications in these cases.

Still, depending on applications, ad hoc networks can take different specialized forms. Of particular interest is the *Wireless Mesh Networks* (WMN) and a variant that resembles *Hybrid Wireless Network* (HWN). We are considering a two-tier architecture for WMN [6] , which are composed of mesh routers acting as fixed relays using wireless communications, and mesh clients possibly mobile and offering services similar to traditional PS services such as triple play (voice, data, and multimedia). However, in particular scenarios with emergency scenarios or in disaster areas, the mesh routers may be connected to cellular networks (2G/EDGE or 3G) for certain types of traffic like voice for emergency services which do not need a high capacity for forwarding links but rather guaranteed bandwidth and short delays. This configuration becomes close to HWN, although direct interconnection between mesh routers will still exist. We will discuss the emergency scenarios in more detail in section III.

Wireless Mesh Networks consist of clients and routers, the latter being organized in a mesh structure, for redundancy/reliability purpose. As in a typical (IP) network, routers communicate with each other to establish a topology, in a form of self-organization and react when connectivity is lost to re-establish the topology.

One salient feature of typical (i.e. commercial) WMN technology is its use of popular wireless technology, with multiple benefits:

- The use of 802.11 (WiFi) technology supports a large variety of popular devices as clients, e.g. PDAs, portable computers, etc.
- Another network technology (e.g. 802.11a, WiMAX) can be used between routers, to minimize interference but also to provide more bandwidth to forward traffic. Mesh routers will thus have several wireless interfaces.
- Depending on the technology used, it may even be able to provide forms of quality of service.
- Communications are low power because of the high density of nodes.
- Communications can be performed on licensed and/or unlicensed (i.e. ISM) bands.
- Overall cost of nodes is low, for the above-mentioned reasons.

A WMN will typically be connected to a wired network in several locations, through gateways, to provide access to the Internet, or specific services [7]. One can thus distinguish the infrastructure side – i.e. facing the Internet – from the client side – to which mobiles are connected – with a routing infrastructure in the middle. WMN literature may distinguish infrastructure-oriented mesh networks from client MN or hybrid forms, according to the presence and/or relative importance of these three elements.

This technology has already generated a lot of interest across the world for various applications such as community or campus networking. Beyond low costs, we can find other benefits to this technology and see how it complements other wireless technologies, e.g.

- It circumvents line of sight (LOS) restrictions through multi-hop communications and routing.
- It allows incremental growth.
- It supports integration with other wireless technologies (through routing).
- It is low power.

From the previous description, we see that a WMN tends to be defined by the way technology is used, i.e. it is a special case of an ad-hoc network, meant to provide wireless access to the Internet and/or specific applications to possibly mobile clients through a mesh of fixed nodes. Mobile clients do not have to contribute to routing and can have reduced power consumption. The main application in which we are currently interested is the possible use of WMN for emergency operations.

II. Interconnection of APs and Migration to WMN in Lebanon

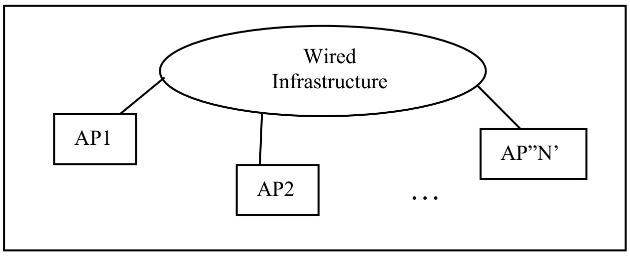

Fig. 2. IEEE 802.11 AP connected to wired infrastructure

In Lebanon as well as many other country in need of the flexibility of wireless Internet connectivity, we have seen in the last few years the proliferation of a dense infrastructure of independent WiFi hotspots acting as a*ccess points* (AP) for data users, usually attached to ISPs or fixed infrastructure to establish connectivity to the Internet in urban areas. The only way to communicate between these APs is via a wired infrastructure, either the Internet or a LAN connected to the Internet (i.e. in companies or campuses). Furthermore, these APs may use different versions of the IEEE 802.11 standard, and replacing them is not an option that can be envisaged. In order to develop the infrastructure of a WMN based on the wireless interconnection of these APs, there must be a solution to interconnect them wirelessly and implementing routing through these wireless interconnections. The IEEE 802.11s standard defines *Mesh access points* (MAP) that can interconnect these APs through the support of previous IEEE 802.11 air interfaces, as well as having compatible MAC and routing capabilities. We illustrate in fig. 2 the original infrastructure with routing via the fixed network, and in fig. 3 the interconnection via MAPs of the IEEE 802.11s standard or any improvement thereof.

The architecture in fig.3 illustrates a migration path to develop a WMN while using an already dense infrastructure of APs with no interconnection other than a cumbersome and costly fixed network between them. It follows a two-tier mesh network [6] with an access tier consisting of the previous APs as well as the new MAPs for connection with users, and a backhaul tier consisting of the network of links connecting the MAPs either directly through the use of each MAP radio interfaces and capabilities, or via routing through a fixed or cellular (3G) network. Examples of routing algorithms for WMN, their performance and possible improvements can be found in [9].

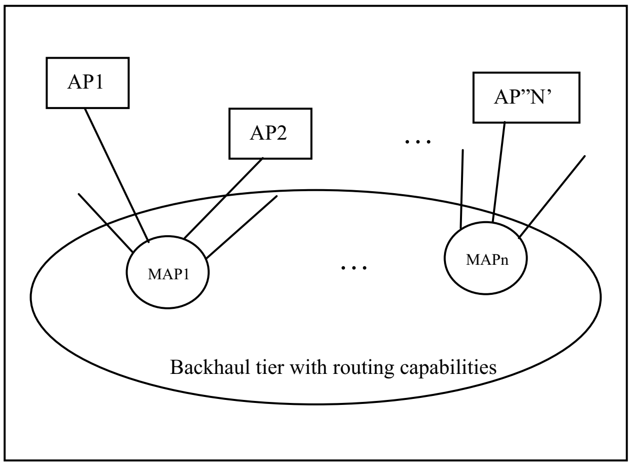

Fig. 3. IEEE 802.11Mesh Access Points (MAPs) connecting the original APs with routing capabilities.

In order for this architecture to come into effect, however, there are still a number of issues to consider.

Performance of radio links: mainly affected by the local environment and factors that are not under our control, like vehicle traffic and weather, as well as interference to closely placed hotspots acting as APs to the WMN. Furthermore, the new MAPs may use either frequencies similar to the APs', or different ones with direct radio links, or links to the fixed or cellular networks. Each one of these scenarios will lead to a different situation in terms of the interference between the different radios of the access and/or traffic forwarding.

The capacity of the backhaul network depends on the technology used, and its impact on the total traffic that can be handled by the *access tier* of the WMN.

Network dimensioning is important to limit the maximal length of the path between mobile and backhaul gateway that is connected to the Internet. Not only does length increases the probability of interference, but it also implies higher load on some links (and therefore higher radio interference) because of aggregation. A related issue is – quite naturally – the density of gateways. Beyond these issues, we also need to concern ourselves with possible dead zones, due to LOS limitations.

Issue of the optimal number of APs connected to MAPs acting as a portal node to the backhaul tier, depending on the technology used in the backhaul tier (either belonging to the WMN with IEEE 802.11s technology, or a hybrid system with interconnection via a fixed or cellular network).

The scalability of the protocols used for routing is another concern. Such traffic consumes bandwidth and it is important that changes – e.g. induced by user mobility – be as localized as possible and that the protocols be sparse in number of broadcasts.

QoS and bandwidth management is still emerging in these technologies. While priority mechanisms have been added to 802.11, it is not clear how to combine them with the forwarding mechanisms of the mesh network.

Security is also difficult to provide in such networks. While users can encrypt their communications, the infrastructure itself is vulnerable to Denial of Service (DoS) attacks.

While large bandwidth can be best provided with a wired gateway to the Internet, it is worth exploring possible benefits of using other technologies to interconnect WMN to an Internet backbone, especially cellular networks. While this may seem paradoxical, because of the more limited bandwidth, there are scenarios, typically for emergencies, where such a combination makes sense, as will be discussed in the next section.

As we discuss below, interconnection with a cellular network, with its extensive infrastructure presence, may also help minimize the above-mentioned path length, and reduce the impact of the density of gateways.

All of these issues have to be addressed in the general case, but they are even more challenging in the case of emergencies which we will consider in the following section.

III. Issues for WMN in Emergency Scenarios

As have appeared in many cases of emergency situations in Lebanon, the need for voice communications between people increases significantly during such situations, and any available telecommunications infrastructure will be needed. The dominant service in this case is usually voice communication, although some urgent data communications may be needed. The main advantage of WMNs is their resilience to link and node failure, and the possibility of self-recovery and reconfiguration. It is of interest to mention that although we have insisted on urban areas as the regions densely covered by WiFi APs, it is also of interest to have these types of APs in all other regions, like rural areas [8] so as to be able to use them as well in emergency situations, while providing rural communities with high speed Internet access. The other type of infrastructure present in all regions is the fixed telephone network, as well as cellular networks, though some of their infrastructure may be damaged by a disaster. While WMN may be sufficient and resilient enough to survive during a disaster, the need for distant communications may be urgent, where WMN usually show great limitations with an ever-increasing length of path between source and destination, especially for voice traffic. Therefore, it may be of interest to have an interconnection between distant MAPs using the fixed or cellular network, even if part of it is not operational. Even if the capacity of such interconnection may be small compared to direct interconnection between mesh routers, the reduction in delay and the few resources needed for voice communication may be enough in such situations. It is to be noted that the use of such a hybrid backhaul network may be subject to priorities and restrictions in the case of emergencies, for example to reserve them for emergency services acting on the sites of a disaster.

The issues that are of interest are derived from the previous ones, but are more related to the specific environment, i.e. emergency situation where voice traffic is predominant and there are some restrictions with the resources available, which quickly reach saturation. We illustrate these issues and we expose in the following section the proposed research to answer a few of them.

- Traffic is primarily generated by VoIP sources, accessing the access links and wishing to reach destination on the fixed network (possibly). Priority must be ensured to these types of traffic.
- Guaranteed bandwidth on the backhaul and the gateways to the fixed/cellular networks must be ensured.
- Proper routing between the already installed APs that have no routing capability (but are directly connected to the fixed network) and newly installed MAPs in their vicinity through the air interface between them. This may be achieved either by installing a router at the premises of the APs (by decision of its owner) or a solution to reroute the packets from the router to which is connected the AP on the fixed network to the MAP of interest. This issue is being investigated at the moment.
- Study of the interference generated and load limits in the access tier, depending on the rate limitations in the backhaul tier due to interference (in the case of similar radio frequencies with the access tier).
- Related to the previous point is the optimal grouping in emergency situations of WiFi hotspots acting as APs with no routing capabilities other than to the MAP acting as a portal to the group, and interconnected either to another MAP for forwarding traffic, or to a cellular network (only, and not a fixed infrastructure) to ensure mobility of the gateways to the fixed telephone system. The issues in this case will be: load limitation due to the interconnection to the cellular system, interference between nodes of the WMN. Harmonization of security aspects between mesh and cellular and other issues.

A transitional phase before the deployment of a WMN in Lebanon is the study of the deployment of mobile MAPs at an emergency location that connects the available WiFi APs through these MAPs, with the interconnection to the rest of the telecommunications network via the cellular network, which ensures the mobility of the mobile MAPs and the possibility of their deployment to a disaster area quickly and efficiently.

There are already products on the market that ensure this type of interconnection with 2G systems.

IV. Current Work

The current work on the research project at the faculty of engineering (ESIB), St-Joseph University is divided in two phases: simulation studies on the issues related to capacity, different emergency scenarios, interference evaluation, backhaul tier types, etc.; tests on a prototype network on the site of ESIB, with a large number of APs (based on the IEEE 802.11b) with a single radio connected to the LAN wired infrastructure on the campus, that will be switched to be connected to 3 MAP (MSM335 mesh access point from HP ProCurve) with three radios each forming an interconnected WMN, and we will test an emergency scenario with VoIP services over the entire campus, with only the three MAPs acting as the backhaul tier for this prototype network. At a later phase, interconnection to a 3G-prototype network that may be deployed on the site of ESIB will be considered.

V. Conclusion

This article has presented the issues to investigate for the migration of independent WiFi hotspots in high-density areas of Lebanon towards a WMN composed of two-tier architecture, with an access tier servicing the users, and a backhaul tier enabling the connectivity to the rest of the world. The application to emergency situations has been discussed, and the current work on the subject has been presented, consisting of simulation studies of various scenarios and real test on a prototype WMN that will be installed at ESIB. This work is undertaken with researchers from ESIB, faculty of engineering of St-Joseph University, Beirut, Lebanon, and INRS-EMT from the University of Quebec, Montreal, Canada, and is financed by the research council of St-Joseph University, Lebanon.

References

[1] www.darpa.mil

[2] C. Siva Rammurthy & B. S. Manoj, “Ad Hoc Wireless Networks: Architecture & Protocols”, Prentice Hall PTR, 2004.

[3] Y. D. Lin & Y. C. Hou: “Multi-Hop Cellular Networks: New Architecture for Wireless Communications”, IEEE INFOCOM2000, pp. 1273-1282, March 2000.

[4] A. N. Zadeh *et al.*, “Self-Organizing Packet Radio Ad hoc Network with Overlay”, IEEE Communications Magazine, vol. 40, no. 6, pp. 140-151, June 2002.

[5] S. M. Faccin, C. Wijting, J. Kneckt & Ameya Damle, “Mesh WLAN Networks: Concept and System Design”, IEEE Wireless Communications, p.10-17, April 2006.

[6] J.D. Camp & E. W. Knightly, “The IEEE 802.11s Extended Service Set Mesh Networking Standard”, IEEE Communications Magazine, August 2008.

[7] G. R. Hiertz, Y. Zang, S. Max, T. Junge, E. Weiss, B. Wolz, D. Denteneer, L. Berlemann & S. Mongold, “IEEE 802.11s: WLAN Mesh Standardization and High Performance Extensions”, IEEE Network Magazine, p.12-19, May/June 2008.

[8] J. Ishmael, S. Bury, D. Pezaros & N. Race, “Deploying Rural Community Wireless Mesh Networks”, IEEE Internet Computing, p.22-29, July/August 2008.

[9] G. Hiertz, S. Max, R. Zhao, D. Denteneer & L. Berlemann, “Principles of IEEE 802.11s”, IEEE 1-4244-1251-X, 2007.

[10] M. Bahr, “Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s”, IEEE ICCCN,August 2007.

[11] R. de C. Paschoalino, E. R. M. Madeira, “A Scalable Link Quality Routing Protocol for Multi-radio Wireless Mesh Networks”, IEEE ICCCN,August 2007.

[12] M.X. Hu & G.S. Kuo, “ Delay and Throughput Analysis of IEEE 802.11s Networks”, IEEE ICC’2008 workshops, May 2008.

[13] J. Chen, Y.-Z. Lee, D. Maniezzo, M. Gerla, “Performance Comparison of AODV and OFLSR in Wireless Mesh Networks”, Proceedings of the IFIP Fifth Annual Mediterranean Ad Hoc Networking Workshop, 2006.

[14] Q. Shen & X. Fang, “A Multi-metric AODV Routing in IEEE 802.11s”, ICCT’06, November 2006.

[15] N. S. Nandiraju, D. S. Nandiraju & D. P. Agrawal, “Multipath Routing in Wireless Mesh Networks”, IEEE MASS’06, October 2006.

[16] S. Zhao & D. Raychaudhuri, “On the Scalability of Hierarchical Hybrid Wireless Networks”, 40th Annual Conference on Information Science and Systems, March 2006.

[17] J. del Prado Pavon & S. Choi, “Link Adaptation for IEEE 802.11 WLAN via Received Signal Strength Measurement”, ICC’2003.