

# Wireless Mesh Networks for Public Safety and Disaster Recovery Communications

Marius Portmann

*University of Queensland, Australia and National ICT Australia Limited*

Asad Amir Pirzada

*National ICT Australia Limited*

**ABSTRACT:** Recent events have revealed significant shortcomings in Public Safety and Disaster Recovery (PSDR) communications. A lot of currently deployed PSDR communication technology suffers from lack of interoperability and reliability in disaster scenarios. Furthermore, even the most advanced PSDR communication systems do not provide true broadband capabilities to support bandwidth intensive applications such as high quality real-time video. Wireless Mesh Networks (WMNs) are a promising alternative technology for PSDR communication, providing features such as broadband support, excellent resilience to failures, self-configuration capability, interoperability and low cost. This paper provides a background on WMN technology and discusses its ability to meet the specific requirements of PSDR applications. We specifically address current limitations of WMNs and provide an overview of current research activities that are underway to overcome these shortcomings.

**BIOGRAPHY:** Dr Portmann received his PhD in Electrical Engineering from the Swiss Federal Institute of Technology (ETH) in Zurich in 2002. His research interests are in overlay and Peer-to-peer networks and network security. He is currently a lecturer at the School of ITEE School of ITEE in the University of Queensland. Asad is a researcher in the SAFE Networks work package of the Safeguarding Australia program at NICTA's Queensland Research Laboratory. He is currently working on Wireless Mesh Networks that can be deployed in disaster scenarios. He holds a degree in MSc Computer Science and in MS Information Security. Asad's research interests include data networking and information security.

## 1. Introduction

Reliable and efficient communication is absolutely crucial for Public Safety in general and Emergency Response and Disaster Recovery operations in particular. Recent events such as 9/11 or Hurricane Katrina have dramatically demonstrated that there exist significant inadequacies in current first responder communications. One of the main problems that plagued rescue teams and emergency services during these disasters was the lack of interoperability between communication equipment used by different public safety agencies and jurisdictions. The 9/11 commission report (Kean 2004) noted that a patchwork of incompatible technology and the uncoordinated use of frequency bands was one of the main reasons of non-existing or poor inter-agency communication during emergency response and recovery operations. Shouting, waving signs and runners with hand-written messages often had to be used as a primitive alternative.

Another problem of Public Safety and Disaster Recovery (PSDR) communication is the strong reliance on terrestrial communication infrastructure such as traditional landline and cellular telephony, as well as infrastructure-based Land Mobile Radio (LMR). Hurricane Katrina took out hundreds of wireless base stations, numerous vital communication cables were disconnected and central offices were flooded. The remaining functional parts of the network

were often completely overloaded and unable to provide adequate services in the aftermath of the disaster. First responders were surprised and severely hampered by a near complete breakdown of the fixed terrestrial communication infrastructure. In a number of recent major disasters, communication systems relying on fixed terrestrial infrastructure have proven to be rather unreliable. A strong dependence on point-to-point communication links and a limited degree of redundancy give these systems an insufficient level of resilience and robustness in disaster scenarios.

A further shortcoming of current PSDR communications is the lack of support for broadband data rates. It is widely recognized that data intensive multimedia applications have a great potential to improve the efficiency of disaster recovery operations. Real-time access to critical data such as high resolution maps or floor plans can be extremely valuable for front-line first responders. As another example, being able to send a live video stream from the incident site back to the command post would greatly increase the situational awareness and would allow more efficient decision making and resource allocation. The need for broadband communication capabilities for PSDR agencies is also pointed out by a report by the SAFECOM program of the US Department of Homeland Security (DHS) (Safecom 2004). The document states that "voice communications are critical, but voice communications requirements are not the only issue....public safety agencies are increasingly dependent on sharing of data, images, and video".

Unfortunately, current PSDR communication systems do not provide the necessary broadband capabilities for bandwidth intensive multimedia applications. The mainstay of public safety communication has been and still is Land Mobile Radio (LMR), also known as Professional Mobile Radio or Private Mobile Radio (PMR). Traditional LMR systems provide analog voice communication for closed user groups over dedicated UHF or VHF radio frequency bands. Modern LMR systems are digital and have limited data capabilities. The two most relevant standards are APCO (Association of Public safety Communications Official) Project 25 (P25), standardized by TIA (Telecommunications Industry Association) (TIA 1995), and TETRA (Terrestrial Trunked Radio), developed by ETSI (European Telecommunications Standards Institute) (ETSI 1997). Most versions of LMR systems that are currently being deployed (TETRA release 1 and P25) only support narrowband communication with data rates of 9.6 kbit/s or 28 kbit/s, which is only adequate for non-bandwidth intensive applications such as text messaging and simple database lookups.

Both TIA and ETSI have recently developed new standards (TIA 2002 & ETSI 2001) with support of data rates of up to 473 kbit/s or 690 kbit/s. This is still not sufficient for high quality video and other broadband applications, which require a throughput capacity of multiple Mbit/s. Further standardization efforts (MESA 2000) are currently under way to develop public safety communication systems with true broadband capabilities. However, these efforts are in their very early stages and it is not expected that any standards or products will be available in the short to medium term. For a more detailed overview and discussion of public safety and disaster recovery communications, we refer the reader to Balachandran et al. (2006).

Given the shortcomings of current PSDR communications mentioned above, Wireless Mesh Networks (WMNs) provide an interesting alternative technology. The key features of WMNs are broadband support, wide area coverage, quick deployment, fault tolerance as well as self-configuration and self-healing capabilities. This paper provides an overview of WMN technology and its potential and limitations as a platform for PSDR communication. Section 2 gives a background of the technology and discusses issues such as architecture, implementation and key characteristics. Section 3 considers the specific requirement of PSDR communication and discusses to what degree they can be met by WMNs. Finally, Section 4 concludes the paper.

## 2. Wireless Mesh Network Technology

Today, wireless local area networks (WLANs) are primarily used to provide mobile users access to a fixed network infrastructure. These networks allow users to roam freely throughout the office or any other space within network coverage with untethered broadband network connectivity. This support for mobile broadband connectivity combined with the rapidly decreasing cost of IEEE 802.11-based commodity hardware have resulted in phenomenal success of wireless networking technology in the last few years. Table 1 shows the key characteristics of the most relevant WLAN standards.

*Table 1. Specifications of Wireless LAN standards*

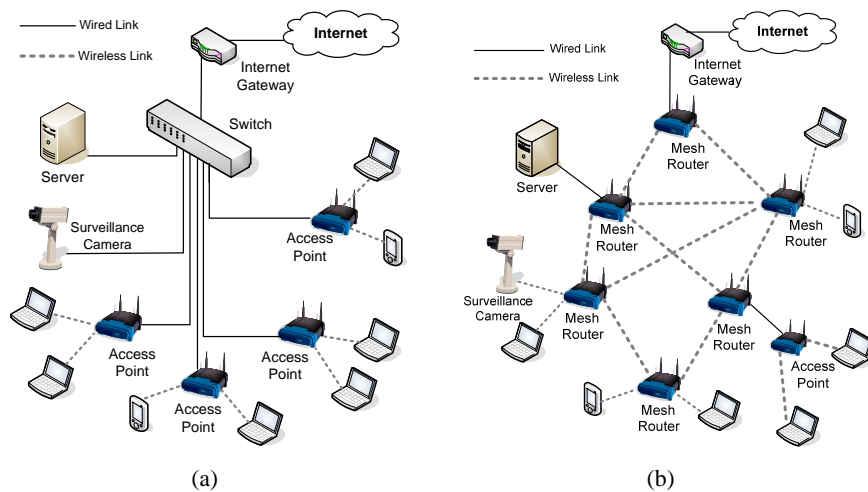
	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a
Theoretical Peak Data Rate	11 Mbit/s	54 Mbit/s	54 Mbit/s
Frequency band	2.4 GHz ISM band	2.4 GHz ISM band	5 GHz ISM band
Modulation	Spread Spectrum	OFDM	OFDM
Number of orthogonal channels	3	3	12
Typical Outdoor Range	100-500m	100-500m	30-300m

The currently most widely deployed standard is 802.11g, which operates in the unlicensed 2.4 GHz ISM band and which is backwards compatible with the older 802.11b standard. Due to the higher frequency band (5 GHz) at which 802.11a equipment operates, the typical outdoor range that can be achieved is significantly smaller than for 802.11b/g networks. However, since the 5 GHz ISM band is less crowded than the 2.4 GHz band, 802.11a networks typically suffer from less interference and achieve higher data rates. Another benefit of 802.11a is its support for more non-overlapping channels, which is useful to minimize interference in dense deployments.

In traditional wireless LAN deployments, clients are associated with wireless access points which are interconnected via a wired backbone network. In this case, the wireless network constitutes only a single hop of the end-to-end path. Clients therefore need to be within a single-hop range of a wireless access point to have connectivity. To achieve coverage of a wide area, a large number of fixed access points need to be deployed and the corresponding wiring for the backbone network (or *backhaul*) needs to be installed. Deployment of large scale WLANs is, therefore, typically a very costly and time consuming undertaking.

In contrast, Wireless Mesh Networks (WMNs) can provide wireless network coverage of large areas without relying on a wired backbone infrastructure or dedicated access points. In WMNs, a collection of *wireless mesh routers* provide network access to wireless clients, similar to access points in traditional WLANs. However, communication between these mesh routers is achieved via the wireless network, typically involving multiple wireless hops. One or multiple mesh routers that are connected to the Internet can then serve as gateways for all other nodes and provide Internet connectivity for the entire mesh network.

Figure 1 illustrates the difference between a traditional WLAN deployment and a WMN. Figure 1a shows a WLAN where clients are associated with wireless access points, which are connected to a central switch via a wired backhaul. In the WMN scenario, as shown in Figure 1b, clients can either be directly communicating with a mesh router or they can be associated with an access point that is connected to a mesh router. The key difference here is that the wired backbone network is replaced by a wireless mesh network.



**Figure 1.** Traditional WLAN (a) versus Wireless Mesh Network (b)

One of the key features of WMNs is their ability to dynamically self-organize and self-configure. The nodes in a WMN automatically detect neighbor nodes and establish and maintain network connectivity in an ad-hoc fashion, typically through the use of ad-hoc routing protocols (Royer et al. 1999). The self-configuring nature of WMNs allows easy and rapid network deployment. WMNs also have the ability to dynamically adopt to changing environments and to essentially self-heal in case of node or link failures. If one mesh link becomes obstructed or otherwise unavailable, traffic will automatically be redirected via an alternative path. Unlike in existing point-to-point radio systems, mesh networks are inherently redundant with no single point of failure. The result is that WMNs have a high level of robustness and fault tolerance.

### 3. WMNs for Public Safety Applications

WMNs can be used in a number of ways and for different PSDR communication scenarios. WMNs can be deployed as an Incident Area Network (IAN) which is a temporary network created for a specific incident only (Safecom 2004). An IAN is necessary when fixed infrastructure networks are unavailable at the incident scene, either because they have been destroyed or they simply do not exist (e.g. in rural areas or in a subway tunnel). IANs allow first responders to share mission critical data and to coordinate their recovery efforts. The rapid deployability and self-configuration capability make WMNs a promising solution for IANs.

The second type of PSDR application scenario of WMNs is as Jurisdiction Area Networks (JAN). A JAN is the main communication network for first responders for all data and voice traffic that is not handled by the IAN. It is also responsible for providing connectivity to the Extended Area Network (EAN) which comprises regional, state or national networks. JANs are permanent networks that are typically installed by municipalities or public safety agencies to provide a wide area (e.g. city wide) communication infrastructure for use in emergency and disaster situations. WMNs have a great potential to serve as JANs due to their high level of fault tolerance. A further key benefit is the ability of WMNs to provide wide area broadband coverage very cost effectively, since no backbone cabling infrastructure is required.

#### 3.1 Functional Requirements

Reliable and efficient communication is mission critical for any PSDR application or communication technology. The SAFECOM program of the US Department of Homeland Security recently issued a Statement of Requirements (SoR) for Public Safety Wireless

communication (Safecom 2004). The following list comprises the most important functional requirements for public safety communication mentioned in the SoR report:

- Support of Voice and Data Services
- Support for Mobility
- Standards-based design
- Use of COTS-based equipment where possible
- Support for unicast, multicast and broadcast communication
- Security (Privacy, Integrity, Access Control)
- Network Management (Command and Control, Maintenance, and Operation)
- Scalability, Extensibility
- User Location

WMNs meet a large proportion of these demands. Any data and multimedia service (including voice) can easily be implemented by WMNs via the IP protocol. User mobility can also be readily supported. Most current WMNs are built on standards-based radio technology using COTS hardware leveraging their low cost, but commercial implementations typically use proprietary protocols and mesh software. However, efforts are under way to define mesh standards, with the ultimate goal of inter-vendor interoperability. WMNs also support a wide range of communication modes, including unicast, multicast and broadcast.

Even though initial attempts to implement security for WLANs failed miserably (Borisov et al. 2001), more recent security standards (802.11i, 802.1X) are considered secure and provide services such as data encryption, integrity and access control. However, these services rely on centralized, trusted entities for key management and access control (e.g. RADIUS server). Introducing such a centralized entity to an otherwise highly distributed WMN would create a single point of failure and would therefore reduce its fault tolerance and resilience capability. On the other hand, implementing security services in a distributed fashion for highly dynamic scenarios such as disaster recovery operations is a very complex problem. This problem has been addressed by the ad-hoc network research community for some time (Hubaux et al. 2003), but a lot more work is required to find practical and mature solutions.

Under the heading *Command and Control, Maintenance, and Operation*, the SoR report lists a number of requirements that can be summarized as Network Management requirements. Current commercial WMN products already support a subset of these required Network Management features but more efforts are necessary. There also exist a wide range of Network Management solutions for IP-based networks and some of these can be applied for WMNs. However, most of these solutions rely heavily on centralized infrastructure. One of the main research challenges in this context is to implement the required management functionality in a distributed manner to preserve the robustness and fault tolerance characteristics of WMNs.

The SoR document specifies two types of scalability requirements. *Horizontal scalability* refers to the ability of the network to grow in terms of geographical coverage, whereas *vertical scalability* allows increasing the number of users. The coverage area of a WMN can very easily be increased by simply deploying additional mesh routers. However, it has been shown that the throughput of a wireless mesh network degrades rapidly with the number of hops involved in the end-to-end path (Gupta et al. 1999 & Li et al. 2001). This severely limits the scalability of WMNs in terms of diameter and size of the network. One of the reasons for this phenomenon is the limitations of the 802.11 Medium Access Control (MAC) mechanism, which was not designed for a multi-hop architecture. However, the main cause of the limited capacity and scalability of WMNs is the radio interference that results in collisions and reduced throughput and increased delay. In contrast to WLANs, the spectrum in WMNs is shared not only by the traffic from clients to the access points, but also with the backbone traffic between mesh routers.

The issue of vertical scalability is also very much an open research problem for WMNs. It is difficult to determine how many users can be supported by a WMN, since this depends on a number of parameters such as network topology, type of applications and traffic characteristics.

The fact that most WMNs operate in unlicensed ISM frequency bands and, therefore, have to share the spectrum with other WLANs as well as a range of other wireless devices further aggravates the scalability problem. A lot of public safety and emergency response practitioners are therefore very skeptical to use any unlicensed frequency bands. It is interesting to note in this context that the US FCC has recently made the licensed 4.9 GHz band available for public safety and homeland security applications, and first commercial WMN products using this band have already been announced by companies such as Firetide and Proxim.

The SoR also specifies that the communication system needs to provide a mechanism to determine the geographical location of a user devices with an accuracy of 1 meter. Even though there have been efforts to implement location services on 802.11 networks using triangulation methods (Bahl et al. 2000), the results are far from satisfactory and a lot more research is required. Multi-path signal propagation effects represent the major obstacle to achieve exact location information.

### **3.2 Performance Requirements**

In addition to the above mentioned functional requirements, the SoR document also lists performance requirements of Public Safety communication systems in the following areas:

- Availability, Reliability
- Survivability, Restorability
- Quality of Service
- Service guarantees
- Support for prioritization of traffic

WMNs systems are excellent at meeting the first two requirements. WMNs are highly reliable, robust and fault tolerant through their implicit redundancy and self-healing mechanisms. However, current systems fail to provide adequate quality of service (QoS) guarantees. The Media Access Control (MAC) mechanism of 802.11 networks is based on a randomized algorithm (CSMA/CA). It is therefore very difficult to give service guarantees regarding delay, throughput or jitter, which is important for real-time applications. Furthermore, with current 802.11 networks it is not possible to provide prioritization of important traffic. In a disaster scenario where the network is likely to be congested, it is crucial to be able to give precedence to high priority messages. IEEE 802.11e (IEEE WG 2005) is a recent extension to the 802.11 standard that supports QoS and differentiation of traffic classes for single-hop wireless networks. However, the issue of QoS in wireless mesh networks is still very much an open research problem.

## **4. Conclusions**

Wireless mesh networks based on low cost commodity hardware have a great potential for PSDR applications. The key characteristics of WMNs are a good match for the requirements of public safety communication as outlined in Safecom (2004). In particular, the robustness and fault-tolerance combined with the rapid deployment and self-configuration capability are crucial features for PSDR communication.

However, WMN technology is still relatively immature and has some serious limitations that need to be addressed. The main inadequacies of current WMN systems are in regards to scalability and quality of service. Given the current research efforts that are under way, we are quite optimistic that these hurdles can be overcome and that WMN technology will play a vital role in future PSDR communications.

## Acknowledgements

National ICT Australia is funded by the Australian Government's Department of Communications, Information Technology, and the Arts and the Australian Research Council through Backing Australia's Ability and the ICT Research Centre of Excellence programs and the Queensland Government.

## References

- Bahl, P. & Padmanabhan, V. N. 2000. RADAR: An In-Building RF based user location and tracking system, in Proceedings of IEEE Infocom: 775–784. Tel-Aviv: Israel.
- Balachandran, K. et al. 2006. Mobile Responder Communication Networks for Public Safety, IEEE Communications Magazine, 44(1): 56 - 64.
- Borisov, N., Goldberg, I. & Wagner, D. 2001. Intercepting mobile communications: The insecurity of 802.11. In Proceedings of ACM/IEEE Mobicom:180-189. Rome: Italy.
- ETSI. 1997. European Telecommunications Standards Institute (ETSI), Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' Guide; Part 1: Overview, Technical Description and Radio, ETR 300-1.
- ETSI. 2001. European Telecommunications Standards Institute (ETSI), Terrestrial Trunked Radio (TETRA): TETRA Advanced Packet Service (TAPS), ES 201-962.
- Gupta, P. & Kumar, P.R. 1999. Capacity of wireless networks, Technical report, University of Illinois, Urbana-Champaign.
- Hubaux, J-P., Buttyan, L. & Capkun, S. 2003. Self-Organized Public-Key Management for Mobile Ad Hoc Networks, In Transactions on Mobile Computing, 2(1): 52-64.
- IEEE WG 2005. IEEE 802.11e/D13.0, Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS).
- Kean, T. H., et al. 2004. The 9-11 Commission Report. <http://www.9-11commission.gov/report/911Report.pdf>, (accessed January 2006).
- Li J., Blake, C., De Couto, D. S. J., Lee, H. I. & Morris, R. 2001. Capacity of ad hoc wireless networks. In Proceedings of ACM/IEEE Mobicom:61-69. Rome: Italy.
- MESA. 2000. Project MESA (Mobility for Emergency and Safety Applications), <http://www.projectmesa.org>, accessed January 2006
- Royer, E. M. & Toh, C. K. 1999. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications magazine, 6(2): 46 - 55.
- Safecom. 2004. The SAFECOM Program, US Department of Homeland Security, Statement of Requirements for Public Safety Wireless Communication & Interoperability, Version 1.0. <http://www.safecomprogram.gov/SAFECOM/> (accessed January 2006)
- TIA. 1995. Telecommunications Industry Association (TIA), APCO Project 25 System and Standards Definition, TIA/EIA Telecomm. Sys. Bull. TSB102-A.
- TIA. 2002. Telecommunications Industry Association (TIA), Wideband Air Interface – (SAM) Radio Channel Coding Specification – Public Safety Wideband Standards Project – Digital Radio Technical Standards, TIA-902 BAAD.