

A Wireless Network for Emergency Services: a Multi-Channel Ad-Hoc Approach

Johan Bergs*, Dries Naudts†, Chris Blondia*, Nik Van den Wijngaert*, Ingrid Moerman†, Piet Demeester†

*University of Antwerp - PATS - IBBT

Middelheimlaan 1, 2020 Antwerp, Belgium

e-mail: {firstname.lastname}@ua.ac.be

†Ghent University - INTEC - IBCN - IBBT

Gaston Crommenlaan 8 bus 201, 9050 Ghent, Belgium

e-mail: {firstname.lastname}@intec.ugent.be

Abstract—Deploying ad-hoc wireless mesh networks for emergency services is a popular topic. One of the main challenges in these networks is to overcome the performance hit due to the interference that is inherent to 802.11 wireless technology. A possible solution is to use multiple interfaces and multiple channels throughout the network in order to minimize this interference. In this paper, we will describe the approach used in a project focused on deploying an emergency ad-hoc network.

I. INTRODUCTION

Recent crises all over the world (09/11, tsunami, etc...) have highlighted the importance of the availability of critical up to date information in real time at the place where needed and they have illustrated the need for reliable communication systems to coordinate the emergency operations. Public safety agencies, such as law enforcement, fire departments, ambulance services, and other emergency response services, are using locally dedicated radio frequencies and transmission systems for their (mainly) voice communication needs. Nowadays, many of the public safety communication systems are based on the Terrestrial Trunked Radio (TETRA) [1]. Although TETRA has enjoyed wide acceptance, in particular in Europe, and is evolving (for example through TETRA release 2) to meet the demands of future services (in particular data services), it is not able to offer the required capacity for envisioned services for the next generation public safety systems such as remote patient monitoring, real-time video, 3D positioning, digital emergency plans exchange, etc. Apart from an increased data rate capacity, other requirements of future public safety communication systems are fast deployment, increase of coverage, scalability, robustness, reliability, security and support of Quality of Service (QoS).

Although the use of existing network infrastructures (cellular 3G and beyond, satellite networks, dedicated public safety networks such as TETRA, etc.) is and will remain crucial to connect a disaster site with the outside world (crisis centre, data bases with emergency plans, hospitals, etc), the communication infrastructure at the site itself is often only partially available or completely destroyed. A possible solution for this lack of communication means is the deployment of ad-hoc and wireless mesh network technology as an Incident

Area Network, i.e., a temporary network infrastructure brought to the scene of an incident, for local communication among different public safety end users (fire brigade, police, medics, etc) and their connection with a gateway. To satisfy this need, ETSI and TIA established the MESA project (www.mesa.org), the goal of which is to define specifications for a mobile broadband network for public safety. Up to now, extensive scenario analyses have led to the MESA Statement of Requirements. Designing and developing such a communication system has been and is one of the major goals of the IBBT GeoBIPS project [2] and its follow-up project ADAMO [3].

When a call reporting a disaster is received at an emergency center, multiple teams are dispatched to the disaster site. These teams can be fire fighter teams, police, medical teams, ... In case of a major disaster, a crisis center is set up that coordinates the actions of the different teams. On site, the different teams spread out to perform their tasks. In the GeoBIPS architecture we initially focused on a particular use case, consisting of a single team of fire fighters - the reconnaissance team or RT - entering a building on fire. This reconnaissance team is supervised by a commanding officer (CO) who coordinates the intervention on site. The CO needs to have a direct communication link with the crisis centre in order to inform them of the situation at hand and to receive further instructions.

One of the challenges of the GeoBIPS [2][4] project is to deploy an ad-hoc wireless mesh network [5] to establish reliable and secure communications between the CO and the RT. Today, such communications are often very difficult due to the limitations of TETRA. The Belgian TETRA network, operated by A.S.T.R.I.D. NV (All-round Semi-cellular Trunking Radio communication system with Integrated Dispatchings), is only required to provide outdoor coverage. Indoor coverage is available at some places. At other places, it is non-existent. As mentioned before, the TETRA network is not suited for transferring large amounts of data (other than voice communication) due to its low bandwidth of 28.8 kbps per carrier (7.2 kbps per time slot). During some major interventions, such as large industrial fires or fire inside a ship, the RT is joined by a camera operator. In order to stream the video footage in real time without the hassle of connecting the video camera with a cable, more bandwidth is required.

The paper is structured as follows: in section II, a short overview of the architecture of the GeoBIPS system is given. Section III will discuss the multi-hop ad-hoc wireless mesh network in more detail. Finally, in section IV, we will state our conclusions and further work.

II. ARCHITECTURE OVERVIEW

In the GeoBIPS project, we defined an architecture that tackles both the indoor coverage problem and the available bandwidth problem. The backbone of the deployed infrastructure is an ad-hoc 802.11 network. As can be seen in figure 1, three main parts of the network can be distinguished. The first part (on the left of figure 1) is located in and near the fire truck (FT) connecting it with the disaster site. As central device in this part of the network the project has chosen a Cisco 3200 series *Mobile Access Router* (MAR). It is powered by the fire truck battery and its primary functions are:

- Establish a secure local hot spot around the fire truck;
- Establish a secure Internet uplink using the best available technology;
- Establish a wireless connection with the RT via the WLTP or *Wireless Link Termination Point*.

Another important device located in the FT is the embedded server, that is used to store video and audio streams from the RT. It also serves as local storage of digital intervention plans and GIS data.

At the other end of the network (on the right of figure 1), which is located at the RT, another WLTP is deployed. It has three functions:

- Establish a connection with the wireless mesh network to realize communication with the FT;
- Establish a local hot spot around the RT;
- Establish a connection with the video server.

The members of the RT are equipped with PDAs that can connect to the local hot spot and thus send and receive information to and from the FT through the wireless mesh network (WMN). The function of the video server is to encode the analog video signal originating from the camera to an MPEG4 RTP stream, which is then streamed to the FT.

In order to connect the RT's WLTP with the FT, a WMN is dynamically set up by the RT as they enter the building. Since the GeoBIPS system uses 802.11 technology, the SNR drops with distance. Therefore, the RT drops *Relay Stations* (RS) as they move further away from the FT to maintain connectivity. This results in a dynamically deployed ad-hoc WMN, which we shall refer to as the *Relay Network* or RN. Let us now discuss the three parts in some more detail.

A. Fire Truck

As stated in the overview, the central device at the fire truck is a MAR. The MAR is a powerful device, offering Mobile IP and VPN support, multiple wireless interfaces (802.11, WiMAX, ...) and multiple wired interfaces. One of the 802.11 interfaces is used to set up a secure local hot spot around the fire truck. This hot spot allows authorized devices (e.g. the CO's tablet PC or PDA) to connect with it.

To establish a connection to the Internet, the MAR is equipped with one or more access technologies. These access technologies can be GSM/GPRS/UMTS modems, a WiMAX radio, an 802.11 radio, a satellite uplink, a TETRA uplink, ... Depending on the technologies built in the MAR and their availability on the crisis location, the MAR automatically connects to the access technology that offers the best service. By "best service", we mean the access technology that offers a combination of a stable connection and high bandwidth. The communication between the MAR and the backbone infrastructure in the crisis centre is established by using the Internet. To ensure this communication is always possible without requiring manual configuration of the MAR, a Mobile IP tunnel is set up between the MAR and the backend. Furthermore, this Mobile IP tunnel is encrypted, ensuring no one on the Internet can obtain information that is exchanged between the MAR and the backbone.

The embedded server and the WLTP have a wired connection with the MAR. The function of the WLTP is to connect the Relay Network with the MAR. Since the Relay Network uses a wireless medium, it is important that the information that is exchanged is encrypted as well. Therefore, a VPN tunnel is set up between both WLTP's. The VPN tunnel adds an extra layer of encryption on top of the standard encryption mechanisms of 802.11 such as WEP, WPA or WPA2.

B. Reconnaissance Team

The WLTP deployed at the RT is the endpoint of the VPN tunnel set up at the FT. In addition to realizing this VPN tunnel, the RT's WLTP creates a local hot spot around the RT, offering the same service as the MAR's access point around the fire truck. The WLTP is also connected (using standard ethernet) with the video server.

C. Wireless Mesh Network

The Relay Network is set up dynamically as the RT enters a building and moves further away from the FT. In the GeoBIPS solution, the Relay Stations are using battery powered devices with a relatively small form factor. Each node has two wireless (802.11) interfaces. The use of multiple radios allows multiple channels to be used throughout the network, theoretically reducing the overall interference in the relay network. The WMN will be treated more in-depth in section III.

D. ADAMO Improvements

As can be seen on figure 1, the WMN deployed in GeoBIPS is more a "wireless cable" than a true mesh network. In the GeoBIPS follow-up project ADAMO, we will be extending this indoor network to a full mesh network. Also, while in GeoBIPS we focused on a single team entering a building, in ADAMO we explicitly take into account that multiple teams may be present in the building. All the teams will share the deployed WMN, routing over each others nodes to avoid that every team should have to set up their own network.

In ADAMO, the outdoor network is also more complex than the GeoBIPS network, which is concentrated around the fire

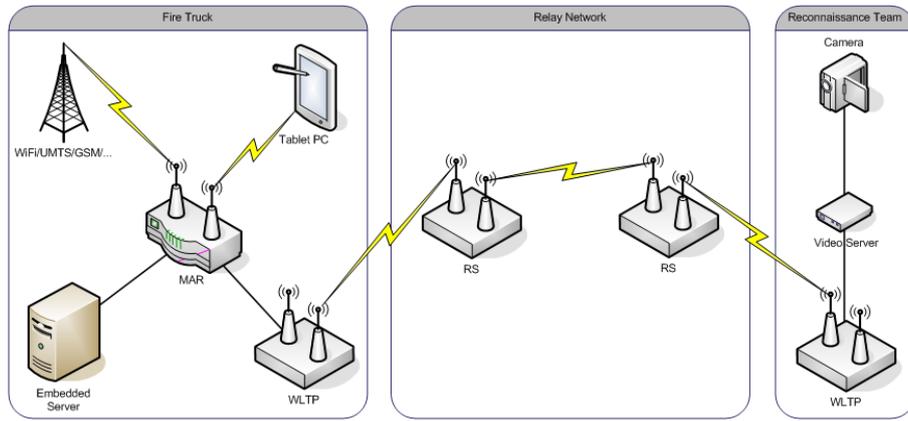


Fig. 1. GeoBIPS Network Setup

truck. In ADAMO multiple vehicles will be on-site. These vehicles will each be equipped with WiMAX technology, creating an outdoor mesh network that will be used as a backbone network at the crisis site. One of the vehicles, the CP-Ops (Command Post Operations), will establish the Internet uplink, using the same technology as used in the GeoBIPS FT, to allow Internet access to all devices connected to the backbone network.

Another important difference between GeoBIPS and ADAMO is the fact that GeoBIPS was targeted at the fire department, while ADAMO takes a much more multi-disciplinary approach. This implies that logical groups should be created, so that each logical group (e.g. a specific team of fire fighters or the police) have their own “private” communication channel on the shared network.

III. AD-HOC WIRELESS MESH NETWORK

While the local networks around the reconnaissance team and the fire truck are an important integral part of the GeoBIPS system, this paper focuses mainly on the relay network. As explained in section II, the relay network is deployed as the fire fighters enter the building. This means that there are some challenges that needed to be resolved in order to make the system work. The most important of these challenges are:

- **Connectivity:** the fire fighters need an indication when they have to introduce a new relay station in the network.
- **Capacity:** because of the nature of 802.11, the channels on which the relay stations operate need to be carefully chosen.
- **Robustness:** the failure of one node should not bring down the entire network.

A. Routing Protocol

We chose the OLSR[6] (Optimized Link State Routing) routing protocol on our WMN. OLSR is a proactive, table-driven routing protocol, implicating that each node in the network knows routes to any other node in the network. We made this decision because each node needs to have a complete overview of the topology for our network monitoring tool, which is further explained in III-B. Furthermore, the

HELLO and TC (Topology Control) messages, which are used to spread topology information in the network, could easily be extended to support our monitoring extensions.

B. Introducing New Nodes

Because the end-to-end throughput is highly dependent on the placement of the RSs (if they are placed too far away from each other, throughput automatically drops), it is very important that the RT introduces new nodes in the relay network at the correct locations. However, in crisis situations it is unknown in advance which route a RT will take when they enter the building. Sometimes, even the internal structure of the building is not known in advance. We therefore developed a network monitoring and planning tool, called the *On-The-Go Coverage Indicator* or OTG-CI, which is further described in section III-E.

When the OTG-CI indicates that a new node should be inserted in the network to maintain a path between the FT and the RT that has sufficient bandwidth to stream the video, it is of the utmost importance that the newly inserted node takes part in the routing algorithm immediately. While OLSR will discover the new node quickly, it is designed to choose the shortest path between source and destination, measured in number of hops. Since end-to-end connectivity was still there when the new node was activated, standard OLSR would never choose to route any packets via this new node, since that would introduce one more hop in the path from RT to FT. In order to keep our modified version of OLSR compatible with standard OLSR nodes, we implemented a simple yet effective scheme to enable the newly inserted node to participate in the routing of packets immediately after it is inserted in the network.

C. Channel Selection and Route Optimization

Traditional ad-hoc networks, in which the nodes use a single frequency throughout the network, are known for their lack of scalability[7]. One of the possible solutions to this problem is to equip each node in the network with more than one radio, and to use multiple frequencies throughout the network to reduce interference[8].

To enable the use of multiple channels in the WMN, it is obvious that the nodes in the network should be equipped

with more than one wireless interface. In the GeoBIPS project, we assume that each node had two wireless interfaces. One interface is used to communicate with the “previous” hop, i.e. the hop closer to the FT. The other interface is used to communicate with the “next” hop, i.e. the hop closer to the RT. In order to make it easy for (new) nodes to discover the WMN when they are powered on, and to allow quick recovery (see section III-D), we introduced the notion of a *default channel*. The default channel is a fixed, pre-defined channel known by all nodes. Communication between the RT’s WLTP and the “previous” hop always uses this default channel. When a new node is powered on, it automatically switches one of its wireless interfaces to the default channel. Since a new node is always powered on by a member of the RT, it is automatically in range of the RT’s WLTP. Because of the default channel, the new node can discover the WLTP and the “previous” hop very quickly.

As soon as the newly inserted node has discovered the WLTP and the “previous” hop, it notifies them of its presence. We modified the OLSR algorithm so that it now starts routing all packets via the new node, even though this introduces an additional hop.

Immediately after that, the new node powers up its second 802.11 radio and initiates a scanning phase. During this scanning phase, it discovers other wireless networks in the vicinity. With this information, it can calculate what of the available channels will be the least subject to interference from those other networks. Once the new node knows this channel, it notifies the previous hop that it would like to communicate with it on that channel. The previous hop then acknowledges this information, after which both nodes tune their radios to the new channel and resume normal OLSR operation. A graphical representation of this process can be found in figure 2. On the top, the new node is integrated in the network, and is initiating its scanning phase. On the bottom, the new node is fully integrated in the network.

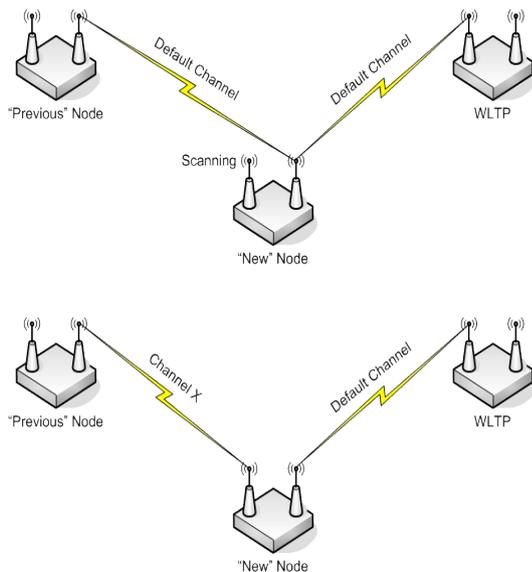


Fig. 2. Inserting a new Node

D. Reliability and Robustness

It is necessary that the GeoBIPS network is reliable and robust. In case a node fails, this should be detected quickly and a new route between the FT and the RT should be established. In the GeoBIPS system, these failures are detected and resolved quickly: as soon as a node discovers it has lost a link with one of its neighbors, it automatically switches the interface on which that link was lost to the default channel. If a node dies, its two neighbors will perform this operation, and will see each other if they are in each others reach, effectively restoring the end-to-end connectivity.

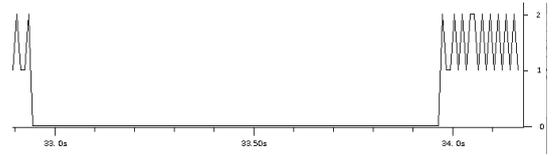


Fig. 3. Recovery from Node Failure

All this happens quite fast, in less than one second, as can be seen on figure 3. The x axis on this figure denotes the time (in seconds) the end-to-end link was up, and the y axis denotes the number of RTP frames that was sent from the video camera to the FT. At about 33 seconds after the video started to run, a node was removed from the end-to-end link, and it can be seen that this link has recovered in less than one second.

However, there are many improvements that can be implemented to further increase the robustness of the network, such as moving from a relay network to a “real” mesh network, which has superior fail-over capabilities. This and many other improvements are currently being implemented in the GeoBIPS follow-up project called ADAMO (Advanced Disaster Architecture with Mobility Optimizations)[3].

E. Monitoring and Planning Tool

In order to easily deploy a mesh network during an intervention, there is need for some kind of tool, called the On The Go Coverage Indicator (OTG-CI), that assist the fire fighters in placing the nodes. As they have neither technical knowledge nor the time to calculate the best location, the OTG-CI should automatically give an indication when a new node should be placed, ensuring an optimal connection between them and the outdoor network. Furthermore, this tool provides feedback to the members of the rescue team about the status of the network. When there is a failure or link degradation, they can act appropriately.

The planning tool is based on the concept of monitoring the RSSI (Received Signal Strength Indicator) values to the nearest nodes. This information can be retrieved by the wireless driver. When the RSSI to the nearest node drops several times below a certain threshold in a certain window, an alert is generated and the fire fighter is encouraged to deploy a new node. This threshold is hardware dependent and is well-considered by experiment. While determining this threshold we accounted for redundancy in the network, so, in case of a node failure, connectivity will be guaranteed.

To monitor the state of the mesh network, we modified the OLSR routing protocol. Each node will estimate link capacity to each of his neighbors by using the Packet Pair Probing method. By sending probes, measuring time difference on arrival and reporting this information back to sender, each node makes an estimation of the capacity of each link to his neighbors. This technique is used because of the minimal extra load on the network. Although the technique is not always very accurate, it gives a good indication of the link status [9] [10].

To have an overview of whole mesh network status, this information should be disseminated throughout the network. Channel information will be spread over the network as well. The OTG-CI will gather and analyze this data and makes an estimation of the end-to-end bandwidth toward the outdoor network, by identifying the bottleneck on the route. This information will be presented by the OTG-CI to the fire fighters in a very simple and clear manner. To minimize the overhead of the link status and channel data dissemination, this information will be piggybacked on the existing OLSR messages. As OLSR is proactive, each node has knowledge of the whole topology of the mesh network.

A more detailed description of the monitoring and planning tool can be found in [11].

F. Challenges in Multi-Channel Networks

While a multi-channel approach seems to be very promising, it still has some drawbacks when it is deployed in the field.

First of all, it is necessary to minimize channel overlap in the network. Even when there are 11 or 13 channels available in 802.11g[12], only three of them are theoretically non-overlapping. Channels are considered to be non-overlapping when the spacing between them is at least 5 channels. In large networks, it is impossible to use only these three non-overlapping channels so that no interference is present. The only solution is to use more channels, but the cost of this approach is that more interference is introduced in the network. Therefore, when deploying a relatively large network, one must try to find a channel distribution that generates the least overall interference. In 802.11a, on the other hand, each channel is orthogonal, but the tradeoff is a higher fading characteristic, and thus shorter range.

During field tests with the GeoBIPS equipment, we encountered some problems using our multi-channel approach. Even when using only a limited number of hops, and carefully configuring the network so that no overlapping channels were used, the performance of the system was less than expected. We discovered that even when using theoretically non-overlapping channels, radios that are physically close to each other, like the two radios present in each RS, do actually interfere each other due to signal power leakage. This phenomenon has been observed by other researchers as well[13][14].

IV. CONCLUSION

Ad-hoc wireless mesh networks can be used in emergency situations to cover the area emergency services are working in, providing them with a means of communicating efficiently.

Single channel mesh networks are not suitable for large scale deployment, due to the interference issues involved. Therefore, one of the approaches is to deploy a multi-channel mesh network. The channels used in such networks should be chosen to minimize channel overlap and thus minimize overall interference.

In the GeoBIPS project, an ad-hoc network architecture was developed to create indoor 802.11 coverage for a single team of fire fighters entering a building. In the follow-up project ADAMO, the GeoBIPS concept is expanded by providing large-area outdoor coverage and by deploying a full mesh network indoor, instead of the “wireless cable” deployed in GeoBIPS, effectively improving the robustness and reliability of the network.

ACKNOWLEDGEMENT

This research is partly funded by the Flemish Interdisciplinary institute for BroadBand Technology (IBBT) through the GeoBIPS and Adamo projects. The authors would like to thank all academic and industrial partners of these projects.

REFERENCES

- [1] *Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)*, European Telecommunications Standards Institute Std. EN 300 392-2, Rev. 2.5.2, Nov. 2005, work item reference: REN/TETRA-03129.
- [2] IBBT. (2006, Dec.) Geographical broadband integration for public services. [Online]. Available: <https://projects.ibbt.be/geobips/>
- [3] ——. (2007, Jan.) Advanced disaster architecture with mobility optimizations. [Online]. Available: <https://projects.ibbt.be/adamo/>
- [4] S. Bouckaert, J. Bergs, D. Naudts, E. De Kegel, J. Baekelmans, N. Van den Wijngaert, C. Blondia, I. Moerman, and P. Demeester, “A mobile crisis management system for emergency services: from concept to field test,” in *Proc. First International Workshop on “Wireless mesh: moving towards applications” (WiMeshNets2006)*, Aug. 2006.
- [5] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey,” *Computer Networks*, vol. 47, no. 4, pp. 445–487, Mar. 2005.
- [6] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” RFC 3626, experimental. [Online]. Available: <http://hipercom.inria.fr/olsr/>
- [7] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Transactions on Information Theory*, vol. IT-46, no. 2, pp. 388–404, Mar. 2000.
- [8] A. Raniwala, K. Gopalan, and T. Chiueh, “Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks,” *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, vol. 8, no. 2, pp. 50–65, Apr. 2004.
- [9] K.-H. Kim and K. G. Shin, “On accurate measurement of link quality in multi-hop wireless mesh networks,” in *MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2006, pp. 38–49.
- [10] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, “Link-level measurements from an 802.11b mesh network,” *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, pp. 121–132, 2004.
- [11] D. Naudts, S. Bouckaert, J. Bergs, A. Schoutteet, C. Blondia, I. Moerman, and P. Demeester, “A wireless mesh monitoring and planning tool for emergency services,” in *Proc. Fifth IEEE Workshop on End-to-End Monitoring Techniques and Services*, May 2007.
- [12] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4GHz band*, IEEE Computer Society Std., June 2003.
- [13] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, “A multi-radio unification protocol for ieee 802.11 wireless networks,” in *Proc. First International Conference on Broadband Networks (BROADNETS'04)*. IEEE Computer Society, Oct. 2004, pp. 344–354.
- [14] J. Robinson, K. Papagiannaki, C. Diot, X. Guo, and L. Krishnamurthy, “Experimenting with a multi-radio mesh networking testbed,” in *Proc. First Workshop on Wireless Network Measurements*, Apr. 2005.