EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Ubiquitous robust communications for emergency response using multi-operator heterogeneous networks

Alexandros G Fragkiadakis[1*], Ioannis G Askoxylakis[1], Elias Z Tragos[1] and Christos V Verikoukis[2]

Abstract

A number of disasters in various places of the planet have caused an extensive loss of lives, severe damages to properties and the environment, as well as a tremendous shock to the survivors. For relief and mitigation operations, emergency responders are immediately dispatched to the disaster areas. Ubiquitous and robust communications during the emergency response operations are of paramount importance. Nevertheless, various reports have highlighted that after many devastating events, the current technologies used, failed to support the mission critical communications, resulting in further loss of lives. Inefficiencies of the current communications used for emergency response include lack of technology inter-operability between different jurisdictions, and high vulnerability due to their centralized infrastructure. In this article, we propose a flexible network architecture that provides a common networking platform for heterogeneous multi-operator networks, for interoperation in case of emergencies. A wireless mesh network is the main part of the proposed architecture and this provides a back-up network in case of emergencies. We first describe the shortcomings and limitations of the current technologies, and then we address issues related to the applications and functionalities a future emergency response network should support. Furthermore, we describe the necessary requirements for a flexible, secure, robust, and QoS-aware emergency response multi-operator architecture, and then we suggest several schemes that can be adopted by our proposed architecture to meet those requirements. In addition, we suggest several methods for the re-tasking of communication means owned by independent individuals to provide support during emergencies. In order to investigate the feasibility of multimedia transmission over a wireless mesh network, we measured the performance of a video streaming application in a real wireless metropolitan multi-radio mesh network, showing that the mesh network can meet the requirements for high quality video transmissions.

Keywords: Wireless mesh networks, Public safety, Emergency response, Inter-operability, Re-tasking, Security, Ubiquitous environments, Heterogeneous networks, 3G, TETRA, WiMAX, Wi-Fi

Introduction

Disasters in various places of the planet have caused an extensive loss of lives, severe damages in properties and a tremendous shock to the survivors and their relatives. Several other serious outcomes are observed after a disaster, like social effects as looting, economic pressures as loss of tourism industry, etc [1]. Natural disasters like the Hurricane Katrina in US, the tsunami in Asia, or man-made attacks like the 9/11 terrorist attack in New York in 2001, and the London bombings in 2005, have shown that the use of communications and network connectivity is of vital importance for saving lives. Immediately after an emergency incident, first responders (e.g., police, fire fighters, medical personnel, etc.) are sent to the disaster area for mitigation and relief operations. As the first minutes (or hours) are vital to save human lives, robust ubiquitous communications should be available to first responders. However, experience has shown that during rescue operations after devastating events, several technology inefficiencies have made communication between the rescuers problematic. For example, during the 9/11 attacks, police issued

* Correspondence: alfrag@ics.forth.gr
[1]Institute of Computer Science of the Foundation for Research and Technology-Hellas (FORTH), P.O. Box 1385, 711 10 Heraklion, Crete, Greece
Full list of author information is available at the end of the article

warnings asking for immediate evacuation of the second building. Unfortunately, the fire department was unable to receive these warnings because the equipment fire fighters used, was not compatible with that of the police [2]. As a result, hundreds of lives were lost. After Hurricane Katrina in US in 2004, communication channels were severely disrupted, causing great difficulties to rescuers, as well as to the victims [3]. In Enschede the Netherlands, a fireworks depot exploded in 2000 destroying a large part of the city. Only a few minutes after the explosion, the GSM network became inoperable [4].

The previous examples show that current technologies impose several limitations and vulnerabilities that can lead to problematic and inefficient performance during emergency situations. Major limitations and vulnerabilities are: lack of technology inter-operability between rescuers' equipment that belongs to different jurisdictions (e.g., police, fire department, army), infrastructure-based operation of the current technologies used (e.g., TETRA [5]) whose parts can be destroyed during a disaster, and the severe overloading of several mobile communication channels (e.g., 3G). This article addresses all those issues and proposes a flexible network architecture that provides a common networking platform for heterogeneous multi-operator networks, for inter-operation in case of emergencies. A wireless mesh network is the main part of the proposed architecture providing a backup network in the case of emergencies. We address issues related to the applications and functionalities a future emergency response network should support, and the shortcomings and limitations of the current technologies. Furthermore, we describe the necessary requirements for a flexible, secure, robust, and QoS-aware emergency response multi-operator architecture, and then we suggest several schemes that can be adopted by our proposed architecture to meet these requirements. In addition, we propose several methods for the re-tasking of communication means owned by independent individuals, in order to provide support during emergencies. Finally, we measure the performance of a video streaming application in a real wireless metropolitan multi-radio mesh network, showing that the mesh network can meet the requirements for high quality video transmission.

The remainder of this article is organized as follows. In Sect. 2 the applications and functionalities a future emergency response communication architecture should support, are described. In Sect. 3 we analyze the various wireless technologies that are used or can be used for emergency response, by focusing on their limitations/shortcomings, as well as on their benefits to meet certain requirements. Sect. 4 includes a survey on research efforts regarding communication networks for public safety and emergency response. In Sect. 5 we propose our communication architecture for emergency response operations. The performance evaluation of a video streaming application in a metropolitan wireless multi-radio mesh networks is presented in Sect. 6. Finally, conclusions appear in Sect. 7.

Required modes of communication for emergency response

After an emergency call has been received, vehicles and personnel belonging to various jurisdictions are sent to the incident scene. Rescuers have to immediately seek for people who need immediate help. At the same time, they have to setup communications for various tasks such as, data transmission to the corresponding headquarter, medical data fetching from hospitals' databases regarding the medical history of the injured persons, etc. In addition, cooperation through communication channels between the rescue teams located in nearby locations may be necessary for the efficient coordination of the emergency operation; thus, the communication system used, is expected to efficiently integrate a plethora of applications with different requirements and performance objectives [6]. Applications and functionalities a future emergency response communication architecture should support, are described in the next sections.

Video

For emergency response operations, first responders often need to share vital information. This may necessitate the transmission of real time video to a control center. Typical scenarios include the transmission of live video footage from a disaster area to the fire department's command center and/or to the nearby located fire fighters. Another scenario is the broadcasting of live video footage from a protest march to the police officers, immediately after violence has broken out.

For video transmission, specific network requirements should be met for an acceptable QoS. The required network throughput depends on the video frame rate, the resolution, and the color. In [7], the authors conducted video quality testing to estimate the quality of video, first responders find acceptable for tactical video applications. The testing shows that: (i) a minimum of 10 frames per second for SIF (360 × 240) or SD (720 × 486) sizes is recommended, and (ii) a minimum of 1 sec video delay (end-to-end transmission) is recommended. Additionally, for MPEG-2 encoding, a minimum of 1.5 Mbps coder bit rate should be used, while for MPEG-4 the minimun coder bit rate should be 768 Kbps.

Audio/voice

Applications that provide voice services between two peers for supporting public safety operations have

become firmly established over the decades [8]. Land mobile radio (LMR) [9] provides half duplex operation requiring the user to "push to talk". However, the public safety communications community is looking towards a future family of full-duplex public safety speech transmission services [8]. Parameters that affect voice quality are [10]: (i) the packet loss correlation (when it is zero, the packet loss process is random), (ii) the packet loss ratio, and (iii) the packet size that can vary depending on the type of the network used (e.g., IP). Of course, voice quality also depends on the compression algorithm used. As an example, in [10] several experiments conducted regarding voice quality, show that 70% of the public safety practitioners judge that voice quality is acceptable if the packet loss ratio is up to 5% and the packet size is either 10 or 40 ms.

The bandwidth requirements can vary depending on the type of voice service. According to [11], for teleconference voice transmission services, 1 Mbps is required with low tolerance on delay, while for voice over the phone, 65 Kbps are required, however, with very low delay tolerance.

Push-to-talk

Push-to-talk (PTT) is a technology that allows half-duplex communication between two users, using a momentary button to switch from voice reception mode to transmit mode. PTT works in a "walkie-talkie" fashion having several features and benefits [12]:

- **instant contact**, as by pressing a button users can instantly connect without the need to dial numbers or having to wait for connection establishment,
- **group talk**, where users can form groups by registering to the PTT group service. One user can talk, while the rest can listen to him at the same time,
- **cost saver** (compared to e.g., SMS with 3G), as PTT messages can be delivered to multiple users at the same time.

The first two features of PTT technology (instant contact, group talk) can be valuable in case of emergencies, as first responders can quickly setup and use this communication mean. PTT over cellular (PoC) is the push-to-talk voice service used in mobile communications. This provides one-to-one and one-to-many communications based on half-duplex VoIP technology.

Real time text messaging (RTT)

Text messaging is an effective and quick solution for sending alerts in case of emergencies. Typical examples of its use can include: (i) individuals reporting suspicious actions to the police, (ii) people affected by a disaster communicating with their relatives, (iii) authorities informing the public about possible disasters (e.g., hurricane, fire, flooding), etc. Types of text messaging can be SMS, email, instant messages, etc. [13]. The requirements of real text messaging are not high, as 28 Kbps can be adequate for this type of application [11].

Location and status information

Location and status information can be of vital importance. During emergency operations, victims' locations can guide first responders to provide immediate medical support. Location information could be obtained through the use of several technologies. For example, 4G networks are expected to provide more accurate location information than the 3G networks that are solely based on GPS technology, which is not very accurate. Simpler devices such as RFID tags can provide location information not only for injured persons but also for the equipment and the medical personnel; thus enhancing the efficiency of the relief operations. At the moment, GPS technology is used for location information in outdoor environments, while RFID tags and Wi-Fi-based location systems are used indoors [14].

Status information is referred to the status of several types of objects within a jurisdiction area. For example, in public safety operations, a sensor network can broadcast information related to the environmental temperature, the level of water, etc. In emergency operations, RFID tags placed on the injured persons by the medical personnel, can classify them into different levels depending on their criticality (e.g., life threatening, severely injured, etc.).

Broadcasting, multicasting

Broadcasting is referred to the ability to transmit information to all users, while multicasting is the ability to send information to a group of users. Both functionalities, if supported by technology, can enhance public safety and rescue operations. For example, suspicious actions outside a bank can trigger the transmission of live video footage to the nearby police cars (multicasting).

Current technologies and their limitations/ benefits for emergency response communications

This section describes several technologies used for massive communications, focusing on their shortcomings and limitations, as well as on their benefits for emergency communications.

Cellular networks

Cellular network technology was introduced in 1981 with the 1G systems. Since then, almost every a decade, a new generation appears characterized by new frequencies, higher data rates, and backwards compatible

transmission technology. After 1G that was dedicated to analog mobile radio communications, 2.5G offered digital communications with transmissions rates up to 115 Kbps and 2.75G offered up to 236.8 Kbps. Nowadays, 3G technologies can offer slightly more than 2 Mbps of bandwidth for stationary users, while up to 384 Kbps for moving users. They also have high coverage providing high mobility that combined by the rapid proliferation of smart phones (according to [15] smart phones in US will undertake feature phones by 2011), have dominated a significantly large part of the telecommunications market. 3G are all-IP networks; networks that offer integrated enhanced service sets (functionalities over IP) that are independent of the access system used. Universal Mobile Telecommunication System (UMTS) is one of the 3G technologies widely used. Figure 1 shows a 3G (UMTS) network architecture. Newer technologies such as HSPA/3.5G can provide up to 14 Mbps.

Cellular networks can provide valuables services in case of disasters but only if they are available. For example in [16], the authors describe an architecture that based on information it receives from cell phone networks, detects possible emergencies and evaluates possible actions to deal with them. A convenient method for transmission of short messages in case of emergencies in massive scales, is cell broadcasting. Cell broadcasting is an existing feature of GSM and UMTS; however, it is rarely used. It could be of very high value to take advantage of this functionality in emergency situations, as it can be used even if the network is overloaded [17]. Furthermore, the Multimedia Broadcast/Multicast Service (MBMS) could be used in the case of emergencies. MBMS is a relatively new service that supports broadcast and multicast over UMTS networks [18]. The service types provided by MBMS are [19]: (i) continuous media streaming (audio and video), (ii) binary data downloading by multiple receivers, and (iii) carousel: a streaming and download combination with synchronization constraints. The Digital Video Broadcasting-Handheld (DVB-H) and Digital Audio Broadcasting (DAB) that can provide high-speed video and audio services over 3G infrastructures, could also be used in emergencies.

However, in several big disasters, cellular network services have become completely unavailable [20] because their centralized infrastructure makes them vulnerable to threats like power outage, physical damages of the base stations (BSs), etc. As an example, if RNC (Figure

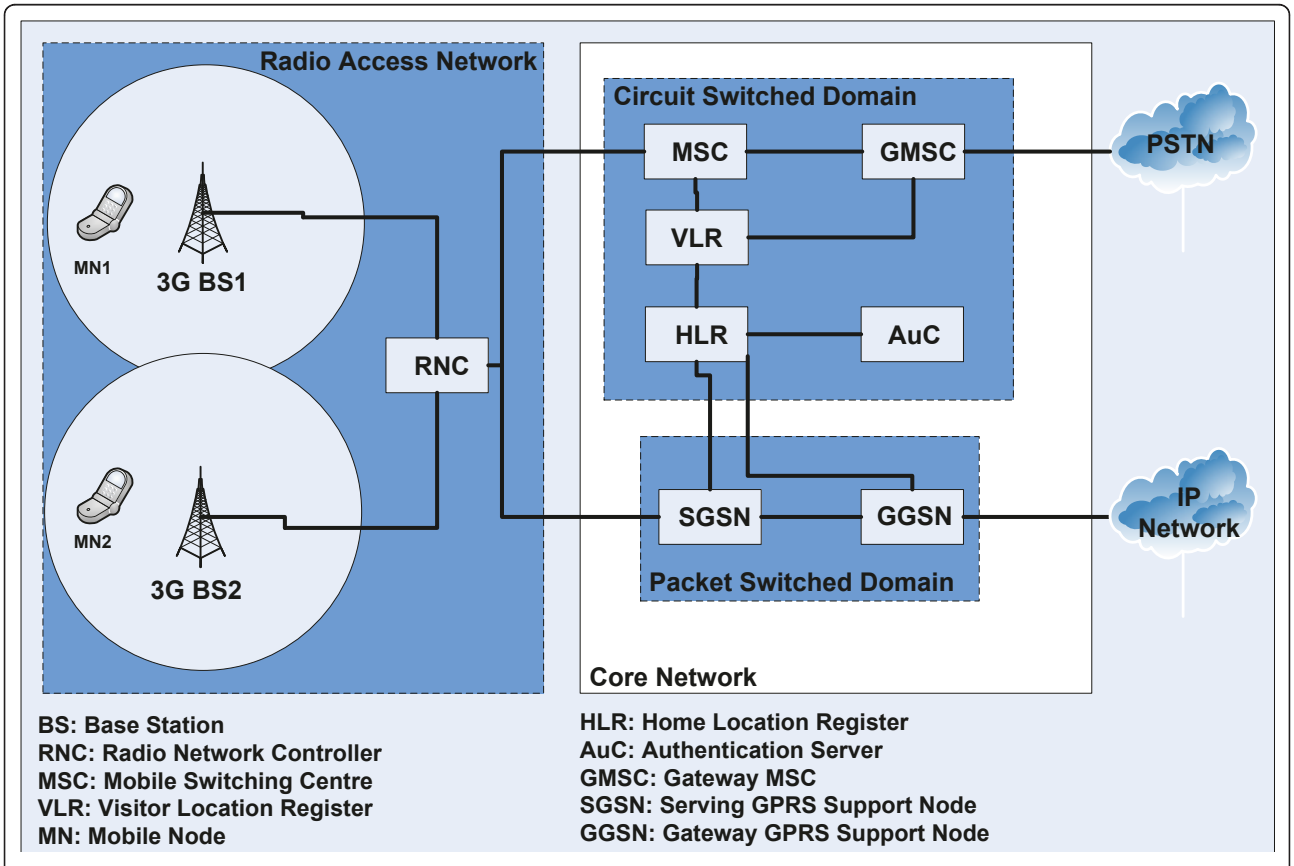

Figure 1 3G network architecture.

1) becomes inoperable, the users associated to either BS1 or BS2 will not be able to communicate with the outside world.

Satellite communications

Satellite are the only infrastructures that are not susceptible to damage from disasters, as the main repeaters for signal transmission and reception are located outside Earth's atmosphere [21]. They are also immune to terrestrial congestion, providing coverage even in sparsely populated areas where no cellular BSs or other means of communication facilities exist. Satellite communications can provide high-speed data transmissions and video conferencing that can be used in case of emergencies (e.g., [22-24]). Very small aperture terminals (VSAT) technology has become very popular for satellite IP services providing interactive real-time data. However, VSAT technology has several shortcomings as asymmetrical transmission rates and weight and cost of equipment [25]. Furthermore, satellite communication equipment can be used only by a limited number of trained personnel; thus not being available for massive use by individuals.

Terrestrial trunked radio (TETRA)

TETRA [5] is one of the most important technologies of the personal mobile radio used in the market, for public safety and emergency response operations. TETRA market has expanded to more than 88 countries worldwide [26]. Its advantages include high spectral efficiency, fast call setup, communication flexibility with one-to-one, one-to-many and many-to-many communication patterns [27]. TETRA has two modes of operation:

- **Trunked Mode Operation (TMO)**. In TMO mode, TETRA operations rely on a fixed private cellular infrastructure with the use of BSs. The network assigns channels and transports radio signals between the users. Similar to the 3G infrastructures, TETRA-TMO due to its centralized nature, can become unable to fulfill its mission in big disasters if any of its key nodes fail (e.g., Controller in Figure 2).
- **Direct Mode Operation (DMO)**. This mode allows the direct communication between the TETRA mobile nodes (TMNs) without the need to use the fixed cellular infrastructure. DMO allows nodes to communicate in an (optionally) encrypted fashion using TDMA and preemption mechanisms. However, TETRA-DMO does not offer multihop capability; thus it provides limited coverage to the users. In addition, the transmission rate of an encoded TETRA data stream varies from 2.4 to 7.2 Kbps [4]. All calls (one-to-many, one-to-one, many-to-many) are half-duplex, supporting only up to two calls per frequency carrier; hence limiting the scalability of the network in terms of the number of users that can be active at the same time [27].

All the above shortcomings make the pure TETRA network functionalities problematic for use in future emergency communications.

Wi-Fi

The mandate of FCC [28] in 1985 for the opening of several bands of the wireless spectrum on a non-licence basis, has allowed the evolution of the Wi-Fi (Wireless Fidelity)

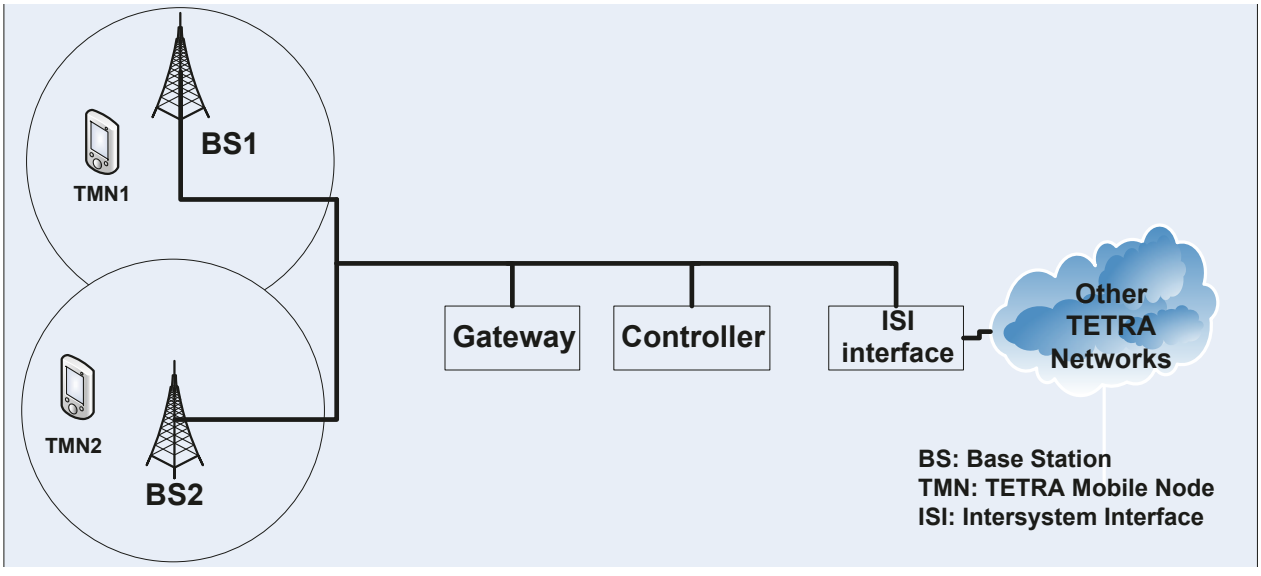

Figure 2 TETRA network architecture.

technology. The so-called Industrial, Scientific and Medical (ISM) band can be used for wireless communication without the need for a licence purchase. The subsequent evolution of the corresponding protocols (IEEE 802.11a/b/g), made Wi-Fi a ubiquitous communications mean for the provision of multi-Mbps internet access. Thousands of IEEE 802.11 hotspots serve millions of users in several public places (e.g., airports, shopping malls, etc.). Regarding transmission rates, IEEE 802.11b can offer up to 11 Mbps while 802.11a/g up to 54 Mbps.

However, as Wi-Fi uses the ISM band for transmissions, and given the proliferation of this technology, interference between devices transmitting on neighboring channels can be present very often (see [29]). For this reason, the transmission power of the antennas are regulated so as Wi-Fi provides short coverage and thus it does not interfere with neighboring wireless networks. Wi-Fi coverage is limited to about 200 m [25]; therefore, such a coverage is not adequate for emergency operations, as disaster areas can span to several hundreds of meters or kilometers.

WiMAX

World Wide Inter-operability for Microwave Access (WiMAX) is the user-friendly name of the IEEE 802.16 protocol [30]. This technology uses licensed parts of the spectrum (e.g., 3.5 GHz) offering broadband wireless access up to 50 km for fixed stations and up to 15 km for mobile stations. Figure 3 shows a typical WiMAX network architecture. The Access and Service Network (ASN) contains the BSs and an ASN gateway (ASN-GW). BSs provide the air interface, serving a number of mobile nodes (MNs) that are further connected to the outside world through the ASN-GW. ASN-GW provides several functionalities such as intra-ASN location management and paging, admission control, authentication, authorization and accounting (AAA) client functionality, etc. The Core Network (CN) contains the necessary hosts/services for AAA, and mobility management through the Home Agent (HA) server. CN also provides connectivity to the internet or other public or corporate networks. WiMAX-enabled devices can achieve transmission rates up to 63 Mbps within a cell radius of 5 km [31]. WiMAX technology is rapidly expanding as newer versions of smart phones are equipped with wireless interfaces that support it. Furthermore, the use of WiMAX-enabled femtocells (small cellular BSs [32]) is continuously spreading, as their use substantially increases WiMAX coverage and performance.

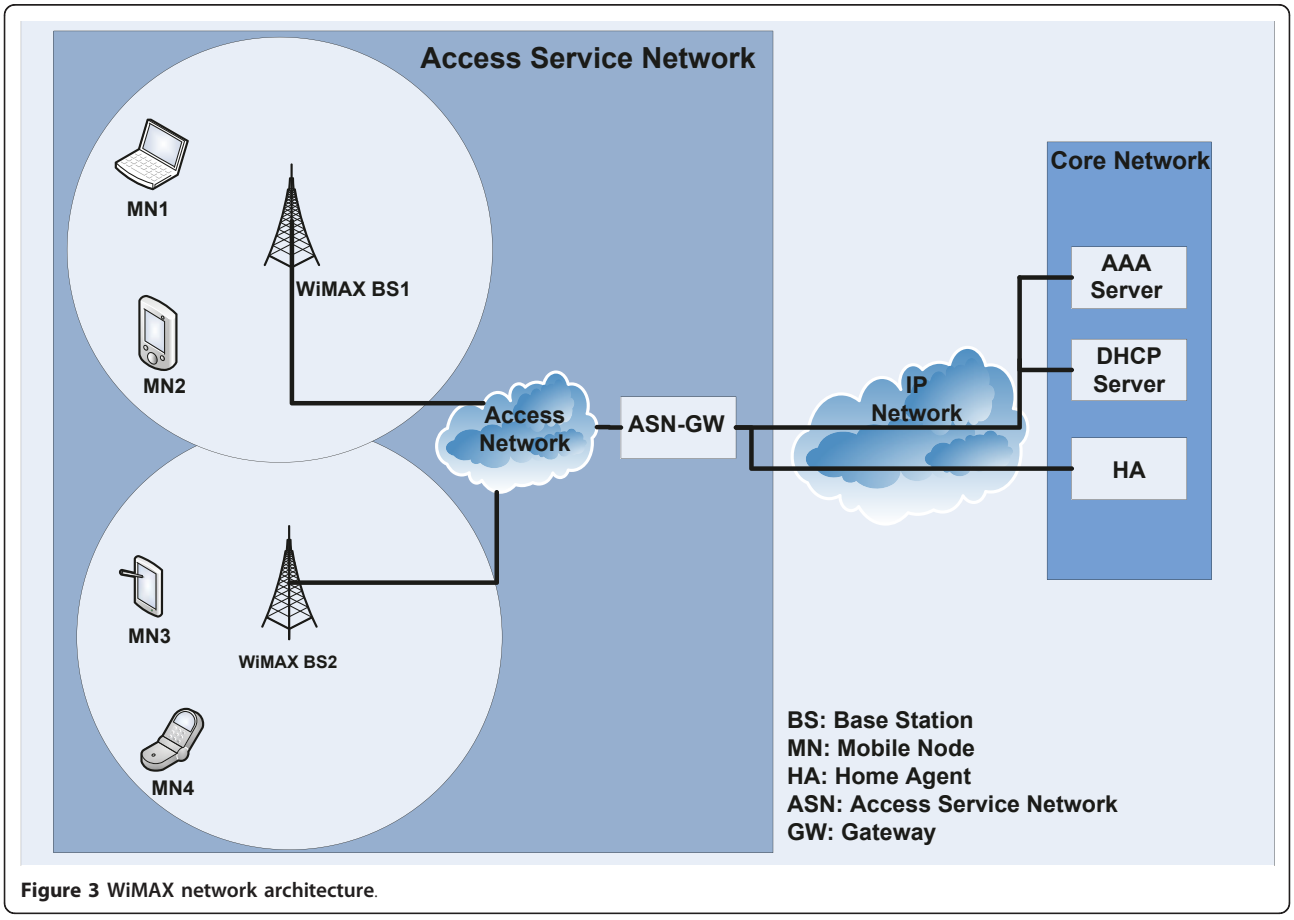

Figure 3 WiMAX network architecture.

Table 1 Limitations/shortcomings and benefits of current technologies for emergency response communications

Technology	Limitations/shortcomings	Benefits
Cellular	low to medium bandwidth, centralized architecture, high cost of infrastructure deployment and maintenance	high mobility, high coverage, high penetration of smart phones, broadcasting mechanisms for audio and video transmission
Satellite	asymmetrical transmission rates, high cost of equipment, heavy weight of equipment	immune to terrestrial congestion, coverage in even sparsely populated areas, high transmission rates
TETRA	centralised architecture, low transmission rates	a good established and mature technology, expansion to many countries
Wi-Fi	limited coverage, intra and inter-channel interference	high transmission rates, use of unlicensed spectrum, rapid proliferation of Wi-Fi-enabled devices
WiMAX	centralised architecture, licensed spectrum use, high cost of infrastructure deployment and maintenance	high transmission rates, proliferation of WiMAX-enabled devices (e.g. smart phones, femtocells)

As Figure 3 shows, WiMAX has a centralized infrastructure; thus in case of big disasters, several major components of its architecture can become single points of failure. For example, if ASN-WG becomes inoperable, the connected MNs will not be able to communicate with the outside world. In addition, newly arrived MNs will not be able to authenticate to the WiMAX network, as they will not be able to reach CN network and the AAA server. Therefore, WiMAX architectures have a high risk to become inoperable in big disasters.

Table 1 summarizes the limitations and benefits of the current technologies for use in emergency response mission critical communications.

A survey on network architectures for emergency operations

Given the shortcomings of the current technologies, there are significant efforts by the research community on defining new architectures for effective and reliable public safety and emergency response. This section describes several of those efforts. The related contributions can be broadly classified into three categories: *ad hoc*, mesh, and hybrid mesh and *ad hoc*.

In general, the *ad hoc* and mesh architectures can provide robust and reliable communications, as they do not rely on infrastructure backbones. A mobile *ad hoc* network (MANET) is a group of wireless nodes that dynamically self-organize in arbitrary and temporary network topologies [33]. The advantages of this technology is that communication nodes can be inter-networked (within their radio transmission ranges) without the need of a pre-existing infrastructure.

Mesh networks consist of two fundamental entities: mesh routers and mesh clients. Mesh clients connect to mesh routers that are further connected to other (mesh) routers forming a multihop architecture. Mesh routers can be equipped with multiple antennas and radios; hence, increasing spectral efficiency and providing acceptable QoS, through reduction of the internal and external channel interference. Furthermore, mesh routers can act as gateways and connect to other networks (e.g., IEEE 802.3). Mesh networks have several advantages such as low up-front cost, easy network maintenance, robustness, reliable service provision, high coverage, etc. [34].

In [25], the authors mention wireless mesh networking as a key solution for emergency and rural applications. They describe MITOC, an off-the-shelf commercial system that includes several types of nodes and diverse functionalities, such as satellite communication terminals, radio BSs, IP-based radio inter-operability, a VoIP telephone switch, etc. In [35], a ballooned mesh network for supporting emergency operations is proposed. This is formed by mesh clients placed on balloons, forming a mesh network in the sky. Communication through the balloons is performed using the IEEE 802.11j protocol, while for the communication between the balloons and the ground equipment, the IEEE 802.11b/g protocols are used.

The deployment of high-bandwidth, robust, self-organizing MANETs can enable quicker response during emergency operations [4]. In [36], the authors propose an *ad hoc* architecture for medical emergency coordination. For scheduling doctors to casualties, an algorithm inspired by the behavior of the ants in nature is used. A virtual private *ad hoc* network platform is described in [37]. This consists of a subset of several devices sharing a common trust relationship and providing a secure, transparent and self-administrating networks built on top of heterogeneous networks. In [4], a broadband *ad hoc* networking architecture for emergency services is presented. The authors also describe several optimizations they have performed in various protocols (e.g., OLSR extensions for routing) for supporting critical requirements.

Various other architectures are not purely based on *ad hoc* or mesh networking, rather they combine a number of different technologies. Bouckaert et al. [38], propose GeoBIPS, a mixed mesh and *ad hoc* architecture for emergency services. They use a camera and a video server to send real time video from a disaster site to a headquarter through a mesh network. For security, they

use IPsec and a pre-shared authentication scheme to sign the OLSR routing messages. The authors in [20] describe a hybrid wireless mesh network architecture for emergency situations that can also take advantage of pre-existing technologies, such as cellular, IEEE 802.11, and bluetooth. A hybrid *ad hoc* and satellite IP network operating with conventional terrestrial Internet, called DUMBONET, is presented in [39]. The radio equipment of first responders in each disaster site forms an *ad hoc* network that is further interconnected to a headquarter via satellite access. Karagiannis et al. [40], propose a generalized network architecture (GAN) for supporing ambient intelligent services and emergency services. GAN interconnects several heterogeneous networks (TETRA, UMTS, mesh, etc.). The authors give a high-level description of the GAN architecture emphasizing on several aspects like inter-operability, mobility and network management, and security.

Except the aforementioned proposed architectures, there is a number of related contributions that do not explicitly define the type of the underlying network architecture (e.g., *ad hoc*, etc.). Kurian et al. [41] propose ODON, a large-scale overlay network for mission critical communications. This consists of four entities: users who are pre-authorized by a destination server, overlay nodes deployed across multiple Internet domains, the destination server, and an ODON client that is installed in clients' equipments. In [13], the authors exploit the idea of using a special-purpose network that can be used in emergency situations, enabling individuals to send short messages to friends or relatives. This architecture is based on a special-purpose social network where users use pre-assigned IDs for sending their messages. Among several aspects, authors address issues related to security and storage capacity requirements. Ahmed et al. [42], describe a decentralized cognitive radio based approach for information exchange between first responders. It consists of four core components: a publish/subscribe module, a routing/forwarding engine, a radio module, and a policy module.

An emergency response communication network architecture for missioncritical operations

This section proposes a new Emergency Response Communication Network (ERCN) architecture that is based on public communication networks, and on the re-tasking of the private network infrastructures. ERCN interconnects networking devices based on heterogeneous technologies. The core component of this architecture is a wireless mesh network (WMN) that can be either created on-the-fly upon the event of an emergency, or be a preexisting network used for day-by-day operations that switches to an emergency mode when necessary.

At this point we classify the types of networks, ERCN can interconnect in emergency situations.

Public communication networks

Public communication networks can be broadly classified into two categories. *Operator Interest Networks* (OINs) that are deployed by major private operators, following a specific billing scheme for service provision. OINs are heterogeneous in nature and can include 3G, WiMAX, and Wi-Fi technologies. On the other hand, *Public Interest Networks* (PINs) owned by governmental or municipal authorities, are usually deployed to provide communications between public authorities, as well as to provide ubiquitous broadband wireless access to the general public (e.g., through hotspots). Technologies utilized by PINs are usually Wi-Fi with wireless hotspots, dedicated wired IP backhauls, as well as WMNs in several cities (e.g., [43]).

As mentioned in Sect. 3.3, TETRA has expanded in many countries, used as a major communication mean for public safety and emergency response. TETRA networks can be part of both OPNs and PINs. In both cases, TETRA networks are not used by the general public as they are mainly used for specific operations such as emergency response or day-by-day routine operations (e.g., communication between workers).

Private communication networks

Internet proliferation has been remarkable the last decade. The low subscription costs, the low cost of networking hardware/software equipment, the proliferation of smart phones, the advances in technology (ADSL, IEEE 802.11, etc.), all have contributed to the provision of ubiquitous broadband internet access. Especially in homes, ADSL technology has simplified (in terms of cost and installation) network connectivity, providing multi-Mbps transmission/reception rates, so millions of homes nowadays are online in a 24 h base. Furthermore, in-home Wi-Fi access points provide a convenient mean to connect several devices between them, as well as to the internet through the ADSL line. In addition, recent advances such as the femtocells will provide even more flexibility and enhanced in-home performance by converging several technologies like (3G) mobile traffic over ADSL or WiMAX over ADSL. We name this advanced in-home networking facilities as *Private Communication Network* (PCN), owned and operated by independent individuals. In PCNs we could also include metropolitan WMNs built by volunteers and technologist enthusiasts as the Athens Wireless Metropolitan Network [44] that has more than 1100 nodes, providing internet access to more than 2900 client computers.

PCNs resources will be of high value if utilized during an emergency by ERCN. As parts of the OINs and PINs

are infrastructure-based, they are highly vulnerable in the case of big disasters. PCNs in such cases can become *islands of connectivity*, bridging several parts of OINs and PINs together, as well as providing connectivity with the outside world.

ERCN architecture

ERCN is a network architecture formed on-the-fly in case of emergencies. This interconnects various types of networks through a WMN. Figure 4 shows a high-level view of an example ERCN, consisting of two OINs, a single PIN and two PCNs, interconnected through the WMN. As described in Sect. 3, infrastructure-based networks such as TETRA, 3G, and WiMAX are highly vulnerable in the case of emergencies. It has been observed that 3G networks for example, are often unable to provide communications, either because one or more of its core components fail, or they are unable to cope with sudden increases in users' traffic. ERCN can provide under these conditions an alternative path, routing the traffic of these networks through the WMN. WMN has a vital role within ERCN, providing interconnection between heterogeneous multi-operator networks. It consists of several types of devices:

- **Operator mesh routers and gateways (OMRGs)**. These devices belong to a specific operator, used as a "glue" to the WMN. Their role is to handle traffic between the OINs or PINs, and the WMN. Among their functionalities can be the admission control, QoS regulation, and data translation between protocols.
- **Mesh routers (MRs)** that route traffic within WMN. In general, routing protocols for mesh networks support multipath, QoS, link failure detection, etc. (see [45,46]); thus, they provide robustness and resilience to a number of failures.
- **Mesh routers and gateways (MRGWs)**. These devices do not belong to a specific operator but they are core components of the WMN. Their role is to provide routing, to translate data among heterogeneous protocols, to establish connections with

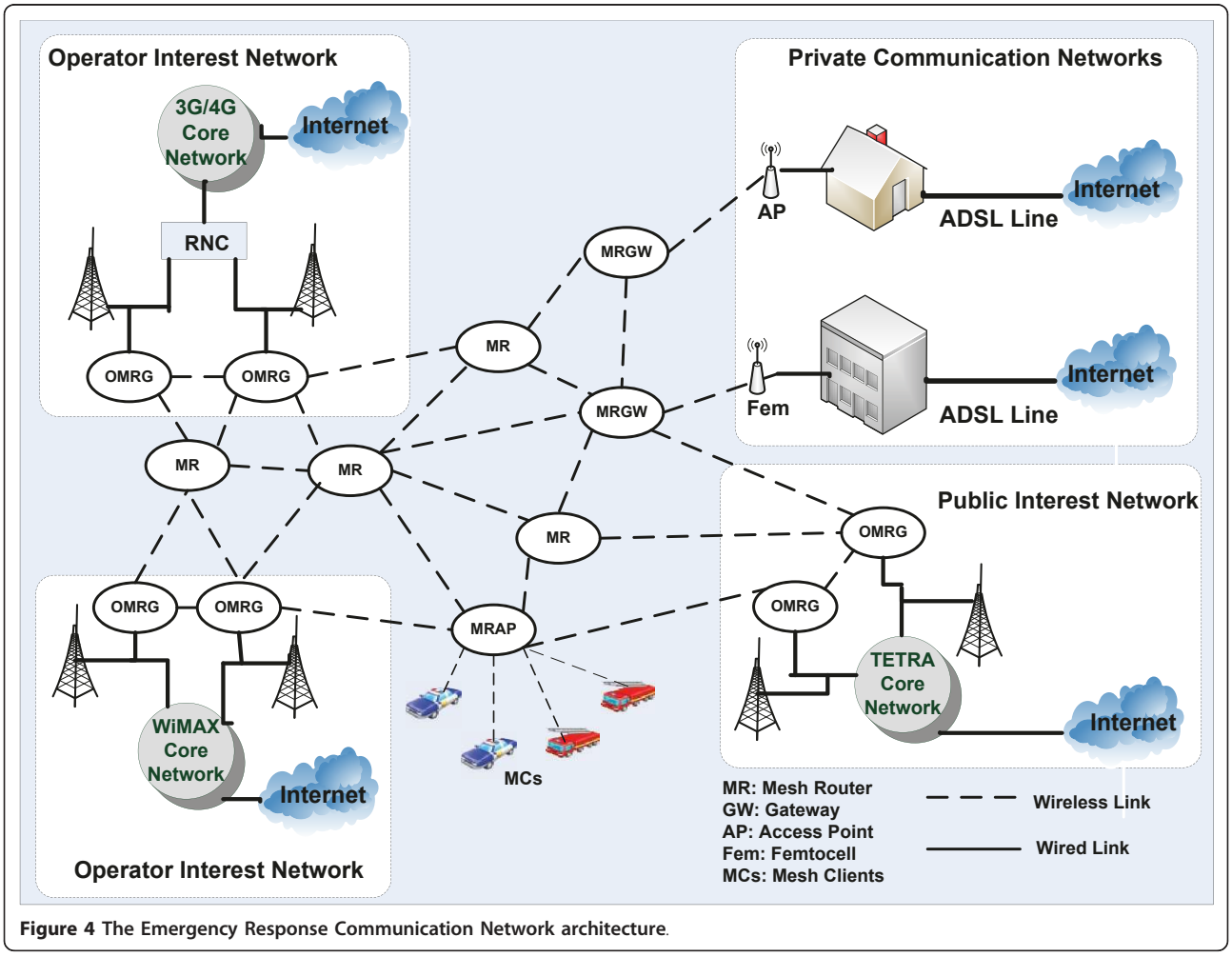

Figure 4 The Emergency Response Communication Network architecture.

OMRGs or other networking devices (e.g., access points, femtocells) that belong to PCNs, and to perform admission control.

• **Mesh routers and access points (MRAPs)**. They perform the same functionalities as MRs but they also provide access point capabilities in order to connect mesh clients (MCs).

WMN is the "heart" of the ERCN that can be designed, deployed, and maintained based on a number of different policies. First of all, the WMN can be a dedicated wireless network for use only in emergencies. The associated costs can be covered by public sector operators, private sector operators or by both based on pre-agreements. However, as big disasters do not happen very frequently, and the cost for the deployment and maintenance of a metropolitan-scale WMN is high, public as well private sector operators would be very reluctant to follow such an approach. We believe that a more appropriate approach would be the deployment of a metropolitan WMN that is initially used for day-by-day operations, and whenever an emergency occurs, it switches on the emergency mode forming the ERCN. Day-by-day operations can cover a very wide area of service provisioning, such as public safety operations (video surveillance, sensors for temperature and water levels recording, etc.), e-governance, e-health, entertainment to the public in large geographical areas, etc. For example, *smart cities*, a recent technology trend, are mainly based on ICT infrastructures for improving quality of life. Therefore, the WMN could be initially part of such an ICT infrastructure (part of a smart city formation), and switch to the emergency mode, whenever it is necessary. This will create incentives for operators coming from both the public and the private sectors. Public sector operators (e.g., authorities) by investing on the deployment of a metropolitan WMN can provide better services to their public and at the same time, they can have a backup network for support in emergencies. Private sector operators by being able to rely on the ERCN in emergencies, can enhance their profile and increase their profits, as they can provide reliable communications even during big disasters. A pre-installed WMN does not necessarily mean that no extra mesh devices can be installed in case of emergencies. Indeed, as WMNs are in general self-adapted networks due to several of their core mechanisms (routing, channel assignment, admission control, etc.), mesh nodes can be deployed and connected to the WMN on demand. For example, mesh nodes in balloons [35] can be easily deployed to expand the WMN's coverage.

Nevertheless, there are several challenges and requirements for the realization of the ECRN architecture, as it must be robust, QoS-aware, secure, and able to provide a common networking platform for different applications and technologies, interconnecting several multi-operator heterogeneous networks.

Emergency detection and notification

By following the approach that the WMN is a pre-installed mesh network used for day-by-day operations, switching to the emergency operation only when necessary, an appropriate mechanism is required for emergency detection and triggering. This should give answers to questions "when, how and by who is an emergency alerted?". There are several approaches to address those questions.

• The WMN can be the alert triggering mechanism. As the WMN is (in its default status) used for public safety, several sensors deployed throughout the network can monitor and report measurements related to temperature, water levels, movements of the public, etc. These measurements can be collected by a fusion command center and then, by using the appropriate algorithms, if one or more thresholds are violated, WMN will change its status to emergency and it will notify all the networks (OINs, PINs), their operators have contractual agreements with it.

• Another approach is the WMN to be triggered by other networks. This can allow public or private operators (that have contractual agreements) owning OINs or PINs to trigger and join WMN, whenever they are in an emergency situation. For example, if a big explosion takes place nearby the CN of a 3G operator (Figure 1), and communication between a number of BSs with the CN becomes infeasible, WMN could be triggered and used as a backup path for the data and signalling of the 3G network.

For both approaches, security mechanisms are required for authentication and encryption of the emergency detection and notification messages.

ERCN deployment

ERCN deployment involves the process of forming its topology by attaching to the core WMN, any available OINs, PINs and PCNs. Here we make a distinction between two classes:

• **Attaching OINs or PINs**. In emergency cases, OINs and PINs join ERCN so they can route traffic through the WMN. In order the joining to become feasible, two requirements have to be met: there must be contractual agreements between the operators of these networks with the operator of the WMN, and parts of their critical infrastructure must have survived from a disaster. After the emergency detection and notification takes place, interested

networks can join ERCN through appropriate authentication and admission control mechanisms. This process can be initiated by the WMN or the other networks, and topology discovery can be based on beaconing transmissions, so interested parties can discover each other.

• **Attaching PCNs**. Attaching PCNs to the ERCN has several challenges. PCNs are owned by individuals, meaning that network devices within these networks (e.g., access points, femtocells) may operate under different policies. Some may be free for use, while other may deploy several security mechanisms (e.g., WPA2), so their use by the ERCN is not straightforward. Furthermore, current legislation does not allow use of private network resources for emergency operations. For these reasons, there are a few requirements for the re-tasking of PCNs. Re-tasking was defined in [47] as the use of the existing networks for emergency response purposes. We extend this definition to include PCNs as well. For the successful re-tasking of the PCNs, legislation issues have to be solved (e.g., if an ERCN can use private communication resources), and technical solutions have to be invented. Supposing legislation has adapted so as PCNs can be retasked, technical approaches can include: (i) the network equipment been equipped with credentials (e.g., long-term keys) that can be used to generate connection keys, (ii) the network equipment been reset by its owners in emergency situations so no access control is enforced for its use (however, this can make ERCN very vulnerable to attacks), and (iii) the authorities can re-task the network equipment using "technology requisition", a process similar to police requisition. The last option can be performed with the appropriate software for hacking into the network equipment. Of course, this would require additional legislation adaptations to become legal.

Inter-operability

As ERCN provides a common platform interconnecting several heterogeneous networks, interoperability is of high importance. Inter-operability can be defined as the capability of "gluing" together several heterogeneous technologies, referring to two main mechanisms:

• **Transparent communication**. This is the ability to send traffic between networks based on different technologies. As Figure 4 shows, gateways (OMRGs) exist between the WMN and the interconnected networks. One of their roles is to provide "translation" between different communication protocols. In general, interworking between heterogenous networks can be applied using four architectures: very tight coupling, tight coupling, loose coupling, and open coupling. Each method has its own advantages and disadvantages (see [48,49]). We suggest the very tight coupling approach where OMRGs (that belong to the corresponding operators and not to WMN) are "glued" to the backbone that connects the various BSs to their corresponding CN. Using this type of coupling, any failures to the highly vulnerable CNs will not affect the operation of the OMRGs that will still be able to route traffic through the WMN. Of course, redundant OMRGs could be placed in several other places such as between the RNC and the 3 G CN (Figure 4), so if any failures occur in one of the BSs or the RNC, communications will not be severely disrupted, as the redundant OMRGs will handle the traffic through the mesh network. The number of the deployed OMRGs within a network depends on the trade-off between cost and robustness, as the more devices of this type are available, the more robust the network is but at the same time deployment and maintenance cost increase.

• **Handover** is the mechanism for seamless handoff between different networks. Horizontal handover is the handoff between networks of the same technology, while vertical handover is the handoff between networks with different technologies. In emergencies, MCs may need to perform handover as several networks or parts of them can become inoperable. Major challenges for successful seamless handover is QoS and admission control. QoS should be guaranteed even if a MC performs handoff to a different network using the same or different technology. Admission control for interworking refers to the appropriate security mechanisms that must exist to provide authentication and authorization for MCs during handovers.

User/traffic classification and prioritization

Depending on a user/traffic classification, different trade-offs regarding security, cost, traffic prioritization, and general performance requirements could exist within the ERCN. For example, first responders could be assigned higher bandwidth for their communications than individuals. Additionally, depending on the criticality, different types of traffic could have higher priority than others. As an example, video and voice transmitted from a disaster area by an injured person in a life threatening situation, could have higher priority than routine communications performed by first responders. Therefore, user and traffic classification should be performed in both a proactive, as well as in a reactive manner.

In a typical disaster scenario, as soon as a call has been received by an emergency operator (e.g., police,

Table 2 User/traffic classification

Users	Traffic
Authorities	Video
Incident commanders	Audio/voice
First responders	Push-to-talk
Individuals	RTT

fire department), first responders are immediately dispatched in the disaster area. In such situations, a large number of users like authorities, first responders and individuals are involved and communication resources are heavily used by them. Table 2 shows a possible classification of users and applications within the ERCN (incident commanders are the persons in charge among the first responders personnel).

During emergency operations, requirements and QoS may dynamically need to change as different user/traffic combinations request more bandwidth in, for example, life threatening situations. A reactive scheme could dynamically compute and assign new priority values depending on a multi-objective optimization function F_o as $P_{i,\ j} = F_o(I_1, I_2, \ldots I_j)$, where P is a priority metric, i is referred to users, j to applications, and I refers to several input parameters that can include: (i) the monitored data from the network (e.g., throughput, delay, etc.), (ii) input from users (e.g., commands from the authorities), (iii) location-based information that for example shows that a person is located in a disaster area and needs to be assigned a higher communication priority.

Security requirements

For the ERCN to become feasible, security mechanisms have to be present to provide authentication, authorization, admission control and message integrity between all networking devices and applications. A security framework is necessary to protect against several types of attackers (external, dishonest clients, dishonest operators, etc.) with different objectives (unauthorized access to the provided services, unauthorized access to client data and meta-data, denial of service, operators gaining advantage of their competitors, etc.) (see [50]).

In this section, we focus on the security requirements regarding the WMN and its interactions with the rest of the networks. Security requirements specific to different technologies (e.g TETRA, 3G) are out of the scope of this article.

- **Authentication and access control enforcement**. This can be performed distributed or centralized, using authentication servers located remotely or locally. As the ERCN is used in emergencies, several networking devices may become inoperable, so any centralized-based authentication mechanisms will be very vulnerable to failures because of several potential single point of failures. On the other hand, a highly distributed mechanism may introduce a significant overhead to the communication parties, reducing the overall QoS. We believe that an appropriate mechanism should follow a hybrid approach. Devices that are less vulnerable to failures (e.g., better physically protected) located in strategic locations can serve as secondary authentication servers (SUSs). The primary authentication servers (PUSs) can be located at the CNs of each operator's network. Through an efficient authentication mechanism, interested communication parties will decide which authentication server to contact, based upon parameters such as server and network connectivity, server load, delay, etc. As OMRGs are placed in strategic locations in the ERCN (Figure 4), they could also play the role of the SUSs.
In extremely big disasters, there is always the danger that no authentication can be supported because no SUSs or PUSs are available. However, parts of the associated networks may still operate. In such conditions, a traffic/user classification scheme (Sect. 5.3.4) could allow special MCs (e.g., first responders, etc.) to access network resources based on pre-defined credentials. For example, MCs carrying mobile phones whose International Mobile Subscriber Identity (IMSI) numbers (see [51]) are prestored into a database, can be granted access to the ERCN using an authentication scheme based on long term keys stored in each device. The challenges here are related to the selection of the nodes storing the IMSI database and how often this is updated.
- **Key management for user handover**. In the ERCN, MCs may traverse from network to network; thus specific requirements have to be addressed for secure and QoS-aware user handover. Requirements include fast authentication, long term keys independent from connection keys, frequent update of the keys, etc. [50].
- **Secure routing**. As WMNs are multi-hop networks, packets flow through several paths to reach their destinations. Routing algorithms play a significant role in the performance of a WMN, therefore secure routing is of vital importance. General requirements of the routing protocols include: adaptation to changes in the network topology, robustness to cope with link and node failures, and efficiency not to over consume computation and network resources [52]. Efficient secure routing algorithms should satisfy requirements related to authentication between the packet sources and the intermediate nodes, integrity of routing information to prevent tampering or corruption of the routing data, and confidentiality to prevent eavesdropping.

• **Data integrity and confidentiality**. A multihop WMN, such the one proposed in the ERCN, is susceptible to several attacks like passive eavesdropping, man-in-the-middle attacks, byzantine attacks, etc., that threaten both the network itself, as well as its interconnected networks. General countermeasures against those types of attacks include: (i) end-to-end protection using TLS [53], SSH [54], IPsec [55], VPN [56], (ii) link-by-link protection using algorithms like HMAC [57,58], AES [59], WPA2 [60], and (iii) route segment protection where only part of the routing path is protected.

• **Intrusion detection**. The previous security requirements address issues related to intrusion prevention. However, there is always the possibility that adversaries manage to bypass part of the protection mechanisms; therefore a second line of defense is of paramount importance. Intrusion detection algorithms make this feasible by protecting against intrusions/attacks in several layers. Several attacks can target the physical layer through jamming, generating interference and severely disrupting the network operations [61]. Usually, the MAC protocol used in WMNs is based on carrier sense (CSMA/CA), as the widely used IEEE 802.11 protocol. Attacks in this layer can include MAC address spoofing, transmission of spurious MAC frames (e.g., RTS, CTS, ACK) [62], as well as greedy behaviors by cheating on backoff rules [63,64]. Furthermore, there are attacks targeting the network layer such as spurious routing messages, as well as several attacks targeting higher layers like port scanning attacks [65] and SYN attacks [66]. An effective and robust intrusion detection system should include probes for measurement collection and combination from different layers (cross-layer), as well as to fuse measurements provided by different monitoring nodes. For example, monitors placed into different locations can collect SNR (signal-to-noise) values informing a fusion center that takes the ultimate decision about the presence of an attacker and triggers the appropriate mitigation mechanisms.

• **Mitigation** that involves the actions taken when an attack is detected and classified. Several techniques can be used to mitigate different types of attacks. For example, jamming attacks can be mitigated using channel switching [67]. Other mechanisms can provide general attack recovery as multi-path routing that can bypass routes which have been attacked, power and rate control that adapts power and rate to increase the energy received per information bit, and mechanism hoping that combines channel hoping and power and rate control [50].

The security mechanisms of the ERCN, both intrusion detection and intrusion prevention will aim to protect not only the core WMN but the other networks that are attached to it as well. Attacks originating from the WMN could severely disrupt the operation of an attached network. For example, a compromised node in the WMN (Figure 4) can severely disrupt the attached 3G network, by sending IP packets in pre-defined intervals to one of its connected IP clients (see [68]).

Signalling

ERCN, as a future emergency network should extend the functionalities of the current voice-centric emergency networks to include applications such as VoIP, real time video, etc. For the support of these types of applications, except the bandwidth requirements for data transmission, a signalling protocol is required. This protocol handles the creation, modification and termination of the sessions between the participants. The Session Initiation Protocol (SIP) [69], is a widely used application-layer signalling protocol that allows participants to agree on a set of supported media types. This follows a client/server model with several servers and related proxies. However, SIP is centralized in nature, so highly vulnerable to failures. Therefore, a distributed signaling protocol is required for the ERCN. Through a carefully designed mechanism, SIP proxies' duties could be assigned to several nodes of the WMN or to nodes belonging to OINs (or PINs), providing SIP functionality when there is no connectivity to the default SIP servers. The main requirements of such a scheme is load balancing and secure authentication (see [70]).

Video streaming performance evaluation in a multi-radio metropolitan wireless mesh network

As ERCN's scope is the provision of ubiquitous communications, including video transmission; in this section we investigate the video streaming performance, in terms of delay, throughput and packet loss, in a multi-radio metropolitan WMN. The metropolitan WMN we use for the measurements is deployed in Heraklion, Crete-Greece by FORTH [71]. The network covers an area of 60 km^2 containing 14 mesh nodes, equipped with directional antennas. We use static IP addressing, OLSR [72] for routing, and IEEE 802.11 as the MAC protocol. Figure 5 shows the topology of the mesh network. The two gateways of the mesh network are the nodes K1 and K4, denoted also with the letter 'G' on their side. Node K1 is connected to the global internet via FORTH, as the line drawn from K1 to M1-FORTH shows. Node K4 is located at the University of Crete and it is connected to the global internet via the GRNET network, a network that connects the universities and research centers of Greece to the global Internet.

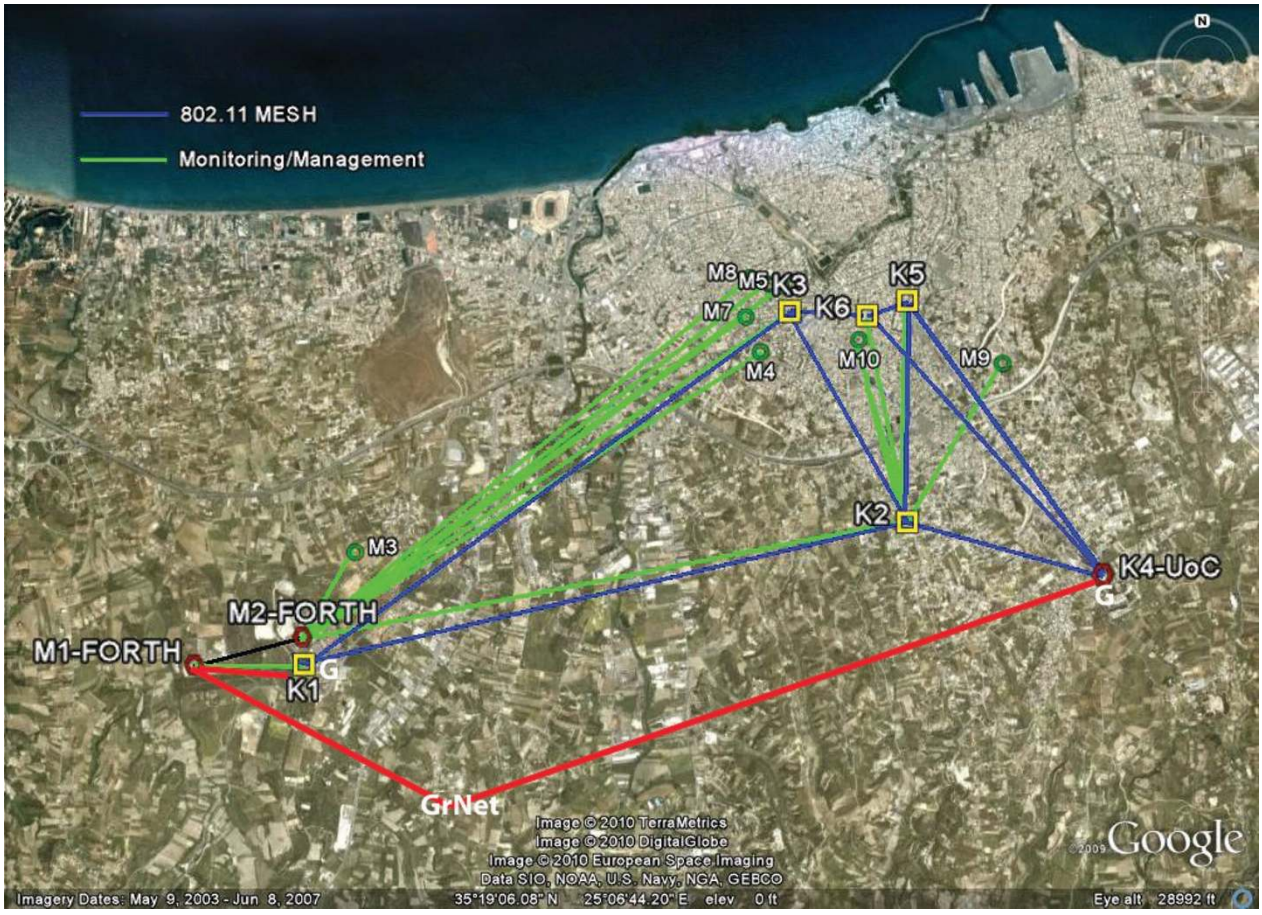

Figure 5 FORTH's Metropolitan Wireless Mesh Network [76].

The setup of the trial nodes include a server, located at FORTH's premises, playing the role of an Internet server and a client computer located at the node K3 of the metropolitan mesh network. In the server, we installed the Darwin Server [73] for streaming video. On the client side at node K3, we use the openRTSP client [74] for receiving video streams. Prior to running any experiments, we used a channel assignment algorithm (see [75]) that automatically assigned channels to the mesh nodes by taking into account both intra-network and external interferences.

We ran the experiment several times. For each experiment the traffic flows from M1 to K3 through the gateway K1 (Figure 5). In order to perform realistic measurements, we added background traffic to the mesh network. This was performed to create intra-network interference to the links. Each node of the mesh network transmitted background traffic by sending ICMP packets of size 1400 bytes every 100 ms to all of its one-hop neighbors. Note that the measurements refer to the end-to-end performance.

Table 3 shows the mean values of the evaluation metrics. The packet delay is much lower than the minimum recommended delay of 1 sec defined in [7] (mentioned in Sect. 2.1). Regarding throughput, the 2.023 Mbps shows that the network can support traffic generated by both MPEG4 and MPEG2 coders (the minimum bit rates of the coders are given in Sect. 2.1). For the packet loss, according to [7] a maximum packet loss of 0.1% is recommended when MPEG4 coding is used without error concealment and/or correction to be necessary. Our measured packet loss is much lower than this limit.

Conclusions

Current technologies used for emergency response operations mainly provide voice-centric services. These

Table 3 Video streaming performance evaluation

Throughput	Delay	Packet loss
2.023 Mbps	6.137 ms	0.003%

networks are mainly infrastructure based; thus highly vulnerable to big disasters, as many reports have highlighted. Future emergency networks are envisioned as architectures that provide more advanced applications such as live video streaming, voice-over-IP, location information, status, etc. All these applications require high bandwidth demands that current networks cannot provide.

This work, after identifying the applications and functionalities a future emergency network should support, proposed an architecture than can, through a wireless mesh network, provide a common platform in the case of emergencies by interconnecting several heterogeneous multi-operator networks. We also described several requirements regarding security, network deployment, and traffic/user prioritization and then, we proposed several approaches that be used to meet those requirements. In addition, we described several approaches that can be adapted to re-task communication resources owned by independent individuals, for use by an emergency response network.

Finally, we measured the performance of a video streaming application in a real metropolitan wireless multi-radio mesh network, showing that it can support high quality video transmissions.

Abbreviations

AAA: authentication, authorization, and accounting; ASN: Access and Service Network; ASN-GW: ASN gateway; BSs: base stations; CN: Core Network; DAB: Digital Audio Broadcasting; DVB-H: Digital Video Broadcasting-Handheld; DMO: Direct Mode Operation; ERCN: Emergency Response Communication Network; GAN: generalized network architecture; HA: Home Agent; ISM: Industrial, Scientific, and Medical; IMSI: International Mobile Subscriber Identity; LMR: Land mobile radio; MANET: mobile *ad hoc* network; MBMS: Multimedia Broadcast/Multicast Service; MRs: Mesh routers; MRGWs: Mesh routers and gateways; MRAPs: Mesh routers and access points; MCs: mesh clients; MNs: mobile nodes; OINs: Operator Interest Networks; OMRGs: Operator mesh routers and gateways; PINs: Public Interest Networks; PCN: Private Communication Network; PUSs: primary authentication servers; PTT: Push-to-talk; PoC: PTT over cellular; RTT: Real time text messaging; SUSs: secondary authentication servers; SIP: Session Initiation Protocol; TETRA: Terrestrial Trunked Radio; TMO: Trunked Mode Operation; TMNs: TETRA mobile nodes; UMTS: Universal Mobile Telecommunication System; VSAT: very small aperture terminals; Wi-Fi: Wireless Fidelity; WiMAX: World Wide Inter-operability for Microwave Access; WMN: wireless mesh network.

Author details

[1]Institute of Computer Science of the Foundation for Research and Technology-Hellas (FORTH), P.O. Box 1385, 711 10 Heraklion, Crete, Greece
[2]Telecommunications Technological Center of Catalonia (CTTC), Barcelona, Spain

Competing interests

The authors declare that they have no competing interests.

Received: 15 January 2011 Accepted: 15 June 2011
Published: 15 June 2011

References

1. R Dilmaghani, R Rao, Hybrid wireless mesh network with application to emergency scenarios. Journal of Software. **3**, 52–60 (2008)
2. The 9-11 commission report, july 2004. http://origin.www.gpoaccess.gov/911/
3. L Comfort, T Haase, 2006, communication, coherence, and collective action: The impact of Hurricane Katrina on communications infrastructure. Public Works Management and Policy
4. M Islam, C Koh, S Oh, X Qing, Y Lai, C Wang, Y Liang, B Toh, F Chin, G Tan, W Toh, Easy wireless: broadband ad-hoc networking for emergency services. *Proc of the 6th Med-Hoc-Net*. 32–39 (2007)
5. Terrestrial trunked radio (tetra). http://www.tetramou.com/
6. D Hinton, T Klein, M Haner, An architectural proposal for future wireless emergency response networks with broadband services. Bell Labs Technical Journal. **2**, 121–138 (2005)
7. M Pinson, S Wolf, R Stafford, Video performance requirements for tactical video applications. *Proc of IEEE HST*. 1–6 (2007)
8. Public safety statement of requirements, Quantitative, version 1.2. **ii** (2008)
9. G Hess, *Land-Mobile Radio System Engineering*. (Norwood, MA: Artech House, 1993)
10. Department of homeland security, public safety communications technical report, measurement of speech transmission suitability, dhs-tr-psc-07-01, october 2007. http://www.safecomprogram.gov/SAFECOM/
11. Transition networks, technical report, quality of service (qos) in high-priority applications. http://www.transition.com/transitionnetworks/Resources/en/PDF/qos_wp.pdf
12. Push to talk technology, white paper, october 2003. http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/whitepaper_pushtotalk_technology.pdf
13. M Allman, On building special-purpose social networks for emergency communication. ACM SIGCOMM Computer Communication Review. **40**, 27–34 (2010)
14. R Togt, E Beinat, S Zlatanova, H Scholten, *Location interoperability services for medical emergency operations during disasters*. (Springer-Verlag Heidelberg, 2006)
15. Nielsen wire. http://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011/
16. T Shoenharl, R Bravo, G Madey, Wiper: Leveraging the cell phone network for emergency response. International Journal of Intelligent Control and Systems. **11**, 209–216 (2006)
17. M Wood, Cellalert, for government-to-citizen mass communications in emergencies. *Proc of ISCRAM*. 323–326 (2005)
18. G Xylomenos, V Vogkas, G Thanos, The multimedia broadcast/multicast service. Wireless Communications and Mobile Computing. **8**, 255–265 (2008)
19. 3gpp. multimedia broadcast/multicast service (mbms) user services; stage 1. ts 22.246; v6.2.0 2004,
20. R Dilmaghani, R Rao, On designing communication networks for emergency situations. *Proc of ISTAS*. 1–8 (2006)
21. Futron corporation and gvf, white paper, why satellite communications are an essential tool for emergency. http://www.iaem.com/resources/links/documents/satellitewhitepaper060906.pdf (2005)
22. V Garshnek, F Burkle, Applications of telemedicine and telecommunications to disaster medicine: historical and future perspectives. Journal of the American Medical Informatics. **6**, 26–37 (1999)
23. T Miyashita, Telemedicine of the heart-real-time tele-screening of echocardiography using satellite telecommunication. Circulation Journal. **67**, 562–564 (2003)
24. J Corry, Interoperable satellite communications. in *Proc of IEEE Conference on Technologies for Homeland Security*. 400–403 (2008)
25. A Yarali, B Ahsant, S Rahman, Wireless mesh networking: A key solution for emergency & rural applications. *Proc of MESH 2009*. 143–149 (2009)
26. M Mikulic, B Modlic, General system architecture of tetra network for public safety services. *Proc of ELMAR '08*. 207–210 (2008)
27. L Adamo, R Fantaci, M Rosi, D Tarchi, F Frosali, Analysis and design of a tetra-dmo and ieee 802.11 integrated network. *Proc of IWCMC '10*. 774–778 (2010)
28. Federal communications commission. http://www.fcc.gov
29. V Angelakis, A Traganitis, V Siris, Adjacent channel interference in a multi-radio wireless mesh node with 802.11a/g interfaces. *Proc of Infocom '07*. 6–12 (2007)
30. The ieee 802.16 working group on broadband wireless access standards. http://www.ieee802.org/16/

31. N Dawod, R Hafez, Enhancement of wimax downlink data rate using sdma. *Proc of AccessNets '07*. 1–4 (2007)
32. V Chandrasekhar, J Andrews, A Gatherer, Femtocell networks: A survey. IEEE Communications Magazine. **46**, 59–67 (2008)
33. W Li, A Joshi, Security issues in mobile ad hoc networks - a survey.
34. I Akyildiz, A survey on wireless mesh networks. IEEE Radio Communications. **47**, 445–487 (2005)
35. Y Shibata, Y Sato, N Ogasawara, G Chiba, K Takahata, A new ballooned wireless mesh network system for disaster use. Proc of AINA '09. 816–821 (2009)
36. B Tatomir, P Klapwijk, L Rothkrantz, Topology based infrastructure for medical emergency coordination. International Journal of Intelligent Control and Systems. **11**, 228–237 (2006)
37. P Dedecker, J Hoebeke, D Naudts, I Moerman, J Moreau, P Demeester, Fast and safe emergency communication through network virtualization. *Proc of IWCMC '09*. 42–46 (2009)
38. S Bouckaert, J Bergs, D Naudts, A mobile crisis management system for emergency services: from concept to field test. *Proc of QShine '06*. 1–5 (2006)
39. K Kanchanasut, A Tunpan, M Aval, D Das, T Wongsaardsakul, Y Tsuchimoto, Dumbonet: a multimedia communication system for collaborative emergency response operations in disaster-affected areas. International Journal of Emergency Management. **4**, 670–681 (2007)
40. G Karagiannis, V Jones, S de Groot, Support of future disaster response using generalized access networks. *Proc of ITAB '06*, 2006, Technical Report.1–6
41. J Kurian, A Kulkarni, H Vu, K Sarac, Odon: an on-demand security overlay for mission-critical applications. *Proc of ICCCN '09*. 1–6 (2009)
42. N Ahmed, K Jamshaid, O Khan, Safire: A self-organizing architecture for information exchange between first responders. *Proc of SECON '07*. 25–31 (2007)
43. City of austin wireless mesh network. http://www.ci.austin.tx.us/help/mesh/
44. Athens wireless metropolitan network. http://en.wikipedia.org/wiki/Athens_Wireless_Metropolitan_Network
45. R Bruno, M Nurchis, Survey on diversity-based routing in wireless mesh networks: Challenges and solutions. Elsevier Computer Communications Journal. **33**, 269–282 (2010)
46. F Kaabi, S Ghannay, F Filali, Channel allocation and routing in wireless mesh networks: A survey and qualitative comparison between schemes. International Journal of Wireless and Mobile Networks. **2**, 132–150 (2010)
47. M LeMay, C Gunter, Supporting emergency-response by retasking network infrastructures. *Proc of HotNet '07*. 1–7 (2007)
48. P Dini, J Bafalluy, M Suriol, On the interworking among heterogeneous wireless networks for seamless user mobility. IEEE Buran Journal. (2007)
49. S Velentzas, T Dagiuklas, 4G Cellular/WLAN Interworking. HET-NET's '05. 3rd International Working Conference, July 2005
50. I Askoxylakis, B Bencsath, L Dora, V Siris, D Szili, I Vajda, Securing multi-operator based qos-aware mesh networks: Requirements and design options. Wireless Communications and Mobile Computing. **10**, 622–646 (2010)
51. G Koien, An introduction to access security in umts. IEEE Wireless Communications. **11**, 8–18 (2004)
52. S Asherson, A Hutchison, secure Routing in Wireless Mesh Networks. http://pubs.cs.uct.ac.za/archive/00000318/01/SATNAC2006WIP.pdf. accessed Jan 2011
53. Transport layer security. http://datatracker.ietf.org/wg/tls/charter/
54. T Ylonen, C Lonvick, The secure shell (ssh) protocol architecture, rfc 4251. (2006)
55. S Kent, K Seo, Security architecture for the internet protocol, rfc 4301. (2005)
56. Z Zhang, Y Zhang, X Chu, B Li, An overview of virtual private network (vpn): Ip vpn and optical vpn. Photonic Network Communications. **7**, 213–225 (2004)
57. The keyed-hash message authentication code (hmac). http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
58. H Krawczyk, M Bellare, R Canetti, Hmac: Keyedhashing for message authentication, rfc 2104. (1997)
59. J Blomer, J Seifert, Fault based cryptanalysis of the advanced encryption standard (aes). *Proc of Financial Cryptography '03*. 162–181 (2003)
60. A Lashkari, M Danesh, B Samadi, A survey on wireless security protocols (wep, wpa and wpa2/802.11i). *Proc of ICCSIT '09*. 48–52 (2009)
61. A Fragkiadakis, V Siris, A Traganitis, Effective and robust detection of jamming attacks. *Proc of the Future Network and Mobile Summit '10*. 1–8 (2010)
62. M Thamilarasu, S Mishra, R Sridhar, A cross-layer approach to detect jamming attacks in wireless ad hoc networks. *Proc of Milcom '06*. 1–7 (2006)
63. M Raya, J Hubaux, I Aad, Domino: A system to detect greedy behavior in ieee 802.11 hotspots. *Proc of MobiSys '04*. 1–8 (2010)
64. A Cardenas, S Radosavac, J Baras, Evaluation of detection algorithms for mac layer misbehavior: Theory and experiments. IEEE/ACM Transactions on Networking. **17**, 605–617 (2009)
65. W El-Hazz, F Aloul, Z Trabelsi, N Zaki, On detecting port scanning using fuzzy based intrusion detection system. *Proc of IWCMC '08*. 105–110 (2008)
66. V Siris, F Papagalou, Application of anomaly detection algorithms for detecting syn flooding attacks. Elsevier Computer Communications. **29**, 1433–1442 (2006)
67. V Navda, A Bohra, S Ganguly, D Rubenstein, Using channel hopping to increase 802.11 resilience to jamming attacks. *Proc of Infocom '07*. 2526–2530 (2007)
68. F Ricciato, A Coluccia, A D'Alconzo, A review of dos attack models for 3g cellular networks from a system-design perspective. Elsevier Computer Communications. **33**, 551–558 (2010)
69. J Rosenberg, Sip: Session initiation protocol, rfc 3261. (2002)
70. I Dacosta, V Balasubramaniyan, M Ahamad, P Traynor, Improving authentication performance of distributed sip proxies. *Proc of IPTComm '09*. 1–11 (2009)
71. Foundation for research and technology-hellas (forth). http://www.forth.gr
72. T Clausen, P Jacquet, Optimized link state routing protocol (olsr), rfc 3626. (2003)
73. Open source darwin streaming server. http://dss.macosforge.org/
74. A command-line rtsp client. http://www.live555.com/openRTSP/
75. M Delakis, V Siris, Channel assignment in a metropolitan wireless multi-radio mesh network. *Proc of BroadNets '08*. 610–617 (2008)
76. M Delakis, K Mathioudakis, N Petroulakis, V Siris, Experiences and investigations with heraklion mesh: An experimental metropolitan multi-radio mesh network. *Proc of Tridentcom '08*. 1–6 (2008)

doi:10.1186/1687-1499-2011-13
Cite this article as: Fragkiadakis *et al.*: **Ubiquitous robust communications for emergency response using multi-operator heterogeneous networks.** *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:13.