DOCTORATE SCHOOL IN
INFORMATION AND COMMUNICATION TECHNOLOGIES
XXV Cycle

UNIVERSITY OF MODENA AND REGGIO EMILIA
DEPARTMENT OF ENGINEERING "Enzo Ferrari"

Ph.D. DISSERTATION

Security Issues and Performance Analysis of Future Public Safety Systems

Candidate: **Alessandro Paganelli**

Advisor: **Prof. Maurizio Casoni**

The Coordinator of the Doctorate: **Prof. Giorgio M. Vitetta**

The Director of the School: **Prof. Giorgio M. Vitetta**

SCUOLA DI DOTTORATO IN
INFORMATION AND COMMUNICATION TECHNOLOGIES
XXV Cycle

UNIVERSITA' DEGLI STUDI DI MODENA E REGGIO EMILIA
DIPARTIMENTO DI INGEGNERIA "Enzo Ferrari"

TESI PER IL CONSEGUIMENTO DEL TITOLO DI DOTTORE DI RICERCA

Sicurezza e Analisi delle Prestazioni nei Sistemi di Emergenza di Prossima Generazione

Tesi di: **Alessandro Paganelli**

Relatore: **Prof. Maurizio Casoni**

Il Coordinatore del Dottorato: **Prof. Giorgio M. Vitetta**

Il Direttore: **Prof. Giorgio M. Vitetta**

To Milena

Abstract

Today, the evolution of modern communication techniques has deeply changed the way information is globally exchanged. Interoperability, which is guaranteed by the presence of proper communication protocols, such as those forming the TCP/IP stack, and by international standards defined within standardization bodies such as the IEEE and the ITU, has promoted the spread of a large number of network-connected devices that have profoundly changed our current way of living.

One of the most important application of such modern ICT systems regards public safety, mainly because the efficacy of the response to any possible crisis event directly depends on the effectiveness of the available communication infrastructure. The current state of the art in wireless communication technologies provides a large selection of feasible alternatives that can be used, in principle, to support novel telecommunication services for both present and future public safety agencies; however, although several public safety systems based on heterogeneous wireless standards are available today, until now only few have been designed with a special focus on trying to unify the best available technologies from the interoperability perspective.

In this work we present a novel approach to the design of modern ICT systems for emergency response, based on the current state of the art in communication and information processing technologies. This research study has been conduced within a large scale integration project, co-funded by the European Commission, entitled "E-SPONDER: a holistic approach toward the development of the first responder of the future", whose consortium comprises several technical and academic European institutions. At a glance, E-SPONDER's main goals are the study, the design and the implementation of a new and original ICT system, based on heterogeneous and pervasive solutions, able to satisfy all the user requirements of the personnel involved in present crisis events.

First of all a high-level overview of the main issues that can be found in current European public safety deployments is presented; then, a detailed discussion about state of the art technologies exploitable for a possible new implementation is provided.

Since today communication security is of paramount importance in every network-connected system, a careful study of the most important security issues affecting emergency networks has been carried out to define the specific security requirements of a modern public safety system.

Moreover, another vital aspect for the design of a telecommunication infrastructure for supporting emergency response regards the users' perceived quality of experience. To investigate this, at first we have considered quality of service issues from the network perspective and, then, we have moved toward the analysis of users' perceived quality, by means of an open-source software evaluation framework, released under GPL v.2 license, which has been developed to perform objective audio and/or video quality assessments.

Keywords: network, emergency, security, performance, QoE

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Together with traditional computer networks, public safety telecommunication technologies have evolved in the last decades toward integrated solutions, to (possibly) support additional multimedia services, other than voice. However, even state-of-the-art public safety systems, especially those designed before year 2000, still suffer from limited capabilities, in particular regarding the data capacity made available to the network applications.

In addition to the limited diffusion of IP-enabled network devices in the last decade of the past century, bandwidth scarcity has greatly limited the development of data services for those public safety system deployments, whose principal application has remained voice for considerable time.

The need of additional and added-value services in these systems, as well as the need of enhanced system features, has begun since the World Trade Center Attack, in 2001, where the limits of technologies available at that time became evident. This has been confirmed again in the last decade (2000-2010), considering some of the most important crisis situations that happened these years (e.g., terrorist attacks, hurricanes).

In the last few years, the continuous evolution of *traditional* ICT technologies (i.e., consumer ICT products) has led researchers to understand if the same solutions could be adopted for implementing *evolved and new* emergency response systems, that can tackle and, possibly, solve these issues.

1.1 The E-SPONDER project

"E-SPONDER: a holistic approach toward the development of the first responder of the future" [1, 2, 3] is an European Union Seventh Framework Programme (FP7/2007-2013) large-scale integration project, co-funded by the EU under grant agreement n° 242411, whose ultimate goal is to study, design and implement the main concepts of next-generation public safety systems, by employing the most important ICT technologies available today (2012), as well as those that will be available in the next future. The project has been funded in 2010 and will last for 4 years (toward December 2014).

The consortium of the project is composed of several companies, national bodies and Universities:

- Exodus S. A. (Grece) as the project coordinator;
- University of Modena and Reggio Emilia (Italy);
- Crisisplan BV (the Netherlands);
- ProSyst Software GmbH (Germany);
- Immersion S. A. (France);
- Rose Vision (Spain);
- Telcordia (Poland);
- CSEM (Switzerland);
- Smartex (Italy);
- Technische Univesitat Dresden (Germany);
- YellowMap (Germany);
- Panou S. A. (Grece);
- Telcordia (Taiwan);
- Institute for Information Industry (Taiwan);

- Entente pour la Forêt Méditerranéenne (France).

Thanks to the unique expertise of each partner of the project, both technological and non-technological advances over the state-of-the-art have been made possible, together with the steady goal of providing an valuable reference for possible future studies on next-generation public safety systems.

The results that will be described in the next Chapters have been obtained during the research activities our research group at University of Modena and Reggio Emilia has performed within the E-SPONDER project.

1.2 Outline of the thesis

This thesis is organized as follows. In Chapter 2, a detailed introduction to the current state-of-the-art of public safety system technologies is provided, together with an elaborated analysis of most important architectural aspects that have to be considered when implementing a new generation emergency network.

In Chapter 3, a detailed study of security properties and security issues that can be found in modern emergency networks is presented, together with possible technical solutions and protocols exploitable in real deployments.

Chapter 4 begins the description of the quality of service (QoS) analysis we have carried out for the E-SPONDER's network, considering realistic traffic pattern configurations and network settings. Then, Chapter 5 describes the sequel of this activity, which has been focused on the quality of experience (QoE) a user perceives when using the network. In particular, this Chapter describes the efforts we have spent in designing and in developing a new software tool usable to perform objective QoE assessments with *network simulator v. 3* (NS-3).

Finally, Chapter 6 provides some conclusions of this research work and reports some ideas for possible future developments.

Chapter 2

Architectural Aspects of Modern Public Safety Systems

2.1 Introduction

Several public safety systems are deployed around the world, today, adopting different standards and employing diverse technologies. However, the increasing need of high-performance and effective emergency response solutions, also motivated by recent large scale disasters (e.g., world trade center attack), has led both the academia and the industry to research and design new methods and new approaches for implementing interoperable public safety systems.

In this Chapter, a review of the most important standards, used to implement state-of-the-art public safety systems, is presented, and, then, a detailed analysis of modern public safety systems' requirements is provided. To satisfy them, a possible approach based on wireless mesh networks is presented and, finally, our solution for the E-SPONDER project is described in details.

2.2 The state of the art: professional mobile radios

Nowadays (2012) several communication standards are in use worldwide to provide communication support to first responders during emergencies or crisis events. Among them, *professional mobile radios* (PMRs, also known as *private mobile*

radios and *land mobile radios*) play an important role, because of their features, which fit very well the requirements of any public safety system. Two of the most important standards within this family are:

1. TETRA (*TErrestrial TRunked RAdio*, formerly known as *Trans-European TRunked RAdio*), an ETSI standard mainly deployed in Europe;

2. Project 25 (also known as *P25* and *APCO 25*), a North-American standard.

Although both provide similar features to the users, and both are digital standards, there are some important differencies that make the two systems not interoperable.

2.2.1 TETRA

TETRA [4] is an ETSI standard that has born around 1994 to provide a PMR system that could be deployed in Europe. Regarding the communication technology, TETRA is a completely digital system, similar to GSM, that can support different kind of network services, such as voice and data.

The original TETRA release, known today as TETRA Release 1, was primarily designed to support robust voice calls and low bit-rate data transfers (up to 18.8 kbit/s using multiple physical timeslots of a single TDMA frame). Among the possible voice services, we may find [4]:

- group calls, where different users can talk together in a tele-conference;

- simple priority calls and pre-emptive priority calls, where different priority levels (up to 16) can be set up to provide different grade of service (GoS) to the users;

- call retention, in order to protect a given call from being forced off by the system in case of resource scarcity;

Regarding TETRA's architecture (see Figure 2.1), it consists of a radio access network (RAN) and a core network (CN).

The RAN is responsible to support the communications between a radio terminal (RT) and the base station (BS) when trunked mode operation (TMO) is

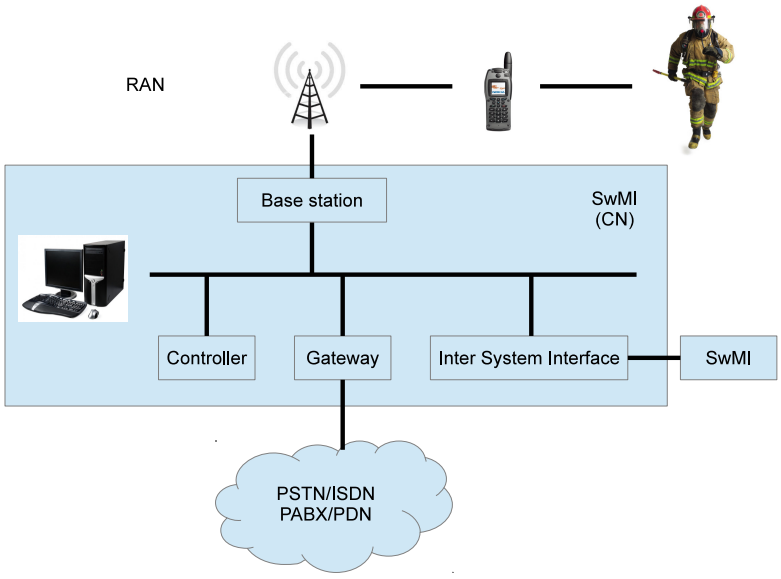


Figure 2.1: TETRA system architecture.

employed. Although TMO is the standard mode of operation of TETRA, which provides wireless conncetivity over a maximum distance of 58 km between the radio terminal and the base station, a very useful additional mode, known as direct mode operation (DMO) is also supported, in order to provide the system with "walkie-talkie" capabilities between two radio terminals. DMO becomes fundamental in case a RAN is not present.

The CN, which in TETRA is typically referred to as the *switching and management infrastructure* (SwMI), is responsible to connect TETRA users with any command and control center using the system; moreover, it can be used to interface the TETRA network with other data networks, e.g., ISDN, PSTN, as well as with any PABX.

The evolution of digital technologies, together with the eveolution of users' requirements, pushed the TETRA Association (which comprises all the companies involved in implementing and deploying TETRA tecnology) to work on several enhancements to the TETRA Release 1 standard. In particular, TETRA Release 2, standardized in 2005, comprises the following [4]:

- TMO range extension, used to increase the initial maximum TMO range from 58 km to up to 83 km;

- support to AMR and MELPe codecs;
- TETRA Enhanced Data Services (TEDS), which greatly increases the overall donwlink throughput by exploiting higher bandwidth channels, if compared with Release 1, together with high order modultations (up to 64 QAM).

In [5] a deep description of TETRA's security features is provided. Among the others, mutual authentication (i.e., between a RT and the CN) and confidentiality (by means of TEA1, TEA2, TEA3 and TEA4 cryptographic algorithms) are supported. Implicit authentication can be used also in DMO, by adopting the same shared key in both RTs. For a more detailed description of TETRA's security featurese, please refer to [5].

2.2.2 Project 25

Project 25 [6] (also known as P25 and APCO 25) is a North-American telecommunication standard for PMR, similar to TETRA but not interoperable with it.

The standard has born around 1990 with the need to upgrade existing analog radios used by most of the agencies in the united states to digital ones. Its main goal was to implement a new interoperable standard among different agencies and among different states of the federation, in order to enhance the effectiveness of any possible emergency response. Indeed, until the beginning of the nineties, several analog system were in place, possibly operating on different frequency bands and/or using different modulation schemes, making it impossible a real cooperation among diverese agencies operating in the same territory. Among the other goals, we may also find the need of an increased spectrum efficiency, compared to legacy standards.

Although Project 25 is focused on adopting digital modulation schemes to support both voice and data, it can also be used to communicate with legacy analog equipments.

Regarding Project 25's architecture (see Figure 2.2), it is very similar to the TETRA's one: it is composed of a RAN and a CN, with the former used to connect a subscriber unit (SU) to the system by means of a base station (also called "repeater" in the P-25 jargon), while the second one is used to convey the traffic

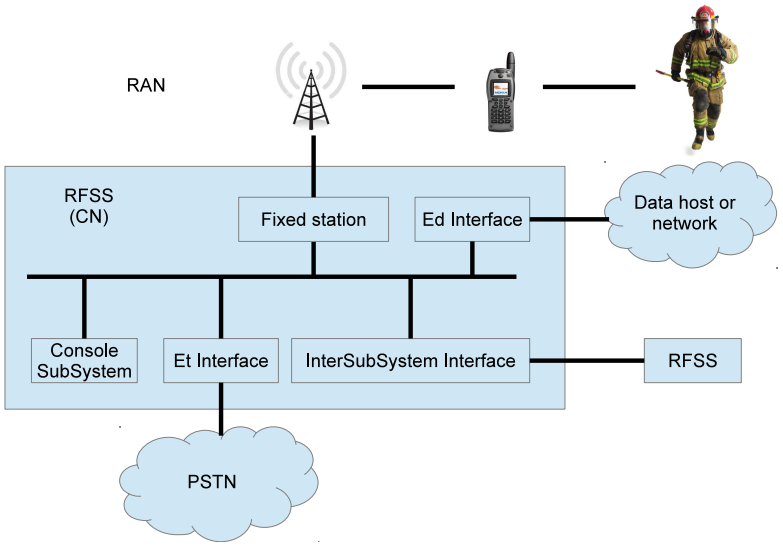


Figure 2.2: Project 25 system architecture.

to the various hosts deployed in the command and control centers. Moreover, the CN can be used also to interface any P-25 network to other systems or to any PSTN network.

P-25 supports also a peer-to-peer communication scheme, dubbed "talk around" mode, where two subscriber units can communicate together without resorting on any existing repeater. This mode of operation is very similar to TETRA's DMO.

The original standard (Phase 1) was designed to operate on 12.5 kHz bandwidth in analog, digital or mixed mode; the channel access scheme was FDMA, while the adopted modulation scheme was *continuous 4-level FM* (C4FM). As for the digital audio codec, P-25 Phase 1 adopted an *improved multi-band excitation* (IMBE) codec operating at 4400 bps.

P-25 Phase 2 [7] is an enhancement of the original P-25 system which mainly aims at improving spectrum efficiency (from one voice channel/12.5 kHz bandwidth, to one voice channel/6.25 kHz bandwidth), by introducing a hybrid TDMA-FDMA channel access scheme, in place of a pure FDMA one, and a more efficient audio codec (AMBE+2 codec).

Project 25 offers *optional* security features that can be used to implement traffic confidentiality [8]. The standard specifies the use of DES, 3DES, AES and the null cypher (used for cleartext). The pre-shared key for these symmetric

cyphers can be manually set up or can be set up by means of *over the air rekeying* protocol (OTAR). Within a group of users, confidential communication can be implemented only if all the radios share the same shared key.

Mainly because of some specific properties of the standard, P-25 systems can be vulnerable to attacks coming from malicious users [8]; in particular, DoS attacks, such as jamming, seem to be very effective [8]. For a detailed analysis of some possible security attacks to P-25 systems, please see [8].

2.2.3 Other systems

In addition to TETRA and Project 25, other systems have been designed and proposed so far to address the needs of public safety agencies. Some of the most important are Tetrapol [9], an early digital PMR standard developed by Matra Communication which must not be confused with TETRA, and Edacs Aegis, a digital system considered outdated, today.

2.3 Modern public safety system requirements

Recent large-scale disasters and crisis events, such as 9/11, have shown several intrinsic weaknesses of current public safety systems. The main issues that have been found are [10]:

1. lack of real interoperability among different agencies (e.g., firefighters, police, paramedics) and among countries, which limits the effectiveness of the emergency response, because other communication means need to be found to synchronize and coordinate all the people involved in the operations;

2. most of the current public safety systems strongly rely on fixed and pre-existent infrastructures, like land mobile networks, that can be easily damaged or can be unavailable during the emergency event (e.g., during hurricanes or earthquakes);

3. lack of broadband communication systems, able to support modern multimedia services, other than voice (e.g., video, image and data sharing), as

pointed out in the *SAFECOM* program report [11] (from the US Department of Homeland Security).

The SAFECOM program published in 2006 a document entitled "Public Safety Statement of Requirements for Communications and Interoperability" (vol. 1 and 2) [11], which contains a very detailed description of the features and the requirements of a modern public safety system. As for the functional requirements [10] we have the following:

- The need of enhanced interoperability between systems, agencies and countries, to speed up the emergency response and to avoid possible issues among them (e.g., radio interference, protocol incompatibility, different data formats);

- Voice and data support, in order to expand the capabilities of current public safety systems toward modern data services, such as file transfer, e-mail; moreover, real-time services, such as video and audio streaming, should be supported as well.

- Mobility support, to allow users to seamless and successfully communicate across jurisdiction boundaries, possibly at high speed (up to the speed of a small aircraft [10]). In this regard, handovers must be as fast as possible, together with all the related procedures (e.g., authentication).

- Security, in order to guarantee a reasonably high level of information and communication security among the parties involved in the emergency response. Authentication issues, as well as availability, have to be guaranteed as well.

As reported in [10], additional *performance* requirements should also be met. The system should be robust and reliable, even in case of harsh environments (e.g., plane crash); moreover, it should be scalable, both horizontally (i.e., in terms of geographical coverage) and vertically (i.e., in terms of the number of users of the system). Finally, a very important requirement concerns *quality of service*, which has to be guaranteed, in terms of traffic differentiation and prioritization, to provide the best possible usage of the available network resources.

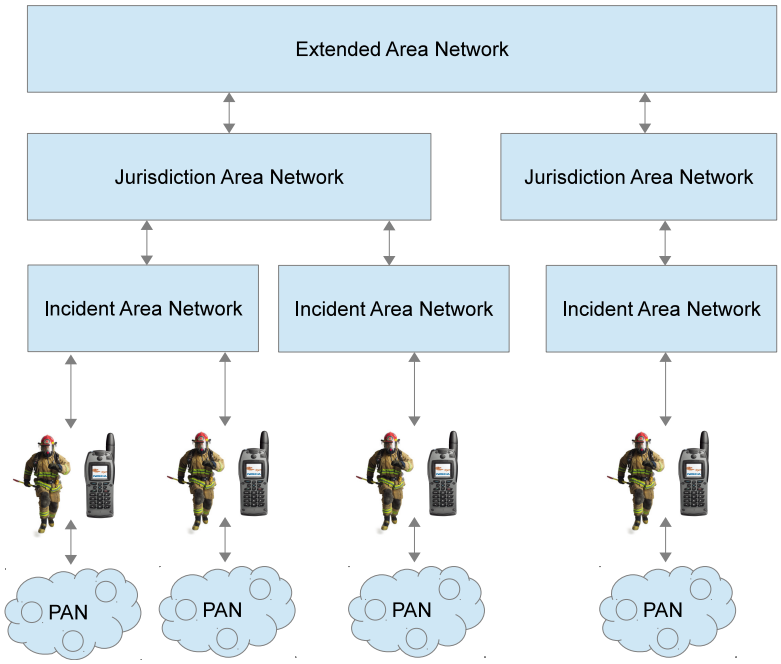


Figure 2.3: A "system of systems" hierarchical architecture.

2.4 A possible approach toward the development of a new-generation public safety system

The set of requirements described in the previous Section poses several constraints and several challenges to the design of a modern public safety system, especially regarding its telecommunication infrastructure, that should be flexible but reliable and robust.

In order to try to meet these requirements, in [11, 10] the concept of "system of systems" is introduced: in this vision, each communication device (e.g., the first responder's unit, FRU) should act as a gateway or a proxy for the data coming from a lower coverage network, that should be forwarded toward the proper gateway of a larger coverage one.

To provide a clearer picture, consider Figure 2.3, where a network as such has been depicted, according to the terms adopted in [11]. In particular, we may find:

- *Proximity area networks* (PANs), mainly composed of small-sized devices (such as sensors) typically deployed over a very small area (e.g., on the first

responder's body, composing a *body area network*, BAN).

- *Incident Area Networks* (IANs), networks implemented to respond to a specific event (e.g., the one composed of a group of first responders involved in the field operations), which is temporary in its nature.

- *Jurisdiction Area Networks* (JANs), which are responsible for all the traffic not related to the IAN (e.g., the communications to/from the command and control center); a JAN typically corresponds to the jurisdiction's telecommunication network (e.g., the network adopted for the firefighters' communications). Moreover, it should allow access to wide area networks (WANs), such as the Internet and/or the EAN (see the next item).

- *Extended Area Networks* (EANs), which have a larger coverage than the previous ones and can be used to interconnect different JANs together, e.g., by exploiting national public safety networks or by means of the Internet.

As suggested in [10], wireless mesh networks (WMNs) represent a very effective solution to address the aforementioned issues, since this approach suits very well the "system of systems" vision. Indeed, several practical technologies are already available in the market, today, for implementing effective heterogeneous WMNs, addressing each communication network type among those previously described.

2.5 The E-SPONDER vision

2.5.1 An interoperable WMN architecture

Within the E-SPONDER project, the WMN-based architecture described in the previous Section has been adopted to design a dependable and interoperable communication network for a new generation public safety system.

Interoperability requires a careful choice of the communication technologies that can be used for a possible implementation, because it is vital to adopt standard and widespread technologies to foster the networking among the users of the system. Furthermore, this choice allows to take advantage of the economies of

scale, which in turn allows the realization of less expensive systems when compared to proprietary and closed solutions.

Another important aspect that must be considered during the design is that every node in the network should be able to communicate over diverse network paths (i.e., a main path and, at least, a backup one) to ensure communication resiliency and redundancy. In particular, it should be possible to route all the traffic originated from a first responder unit (FRU) and directed to the emergency operation center (EOC), or to its local version, the mobile EOC (MEOC), through another FRU, if needed.

In the E-SPONDER project, some of the wireless technologies that have been taken into account are:

- IEEE 802.15 family standards, which comprises IEEE 802.15.1 (best known as Bluetooth) and IEEE 802.15.4 (best known as ZigBee), for the implementation of wireless PANs;
- IEEE 802.11 family standards for the coverage of IANs;
- 3GPP's UMTS and LTE standards, as well as IEEE 802.16 for interconnecting different MEOCs or to interconnect a MEOC with the JAN/EAN;
- ETSI DVB-RCS standard for providing a full-duplex satellite link connecting the MEOC to the EOC.

A general sketch of the proposed architecture for the E-SPONDER telecommunication network, together with possible technologies for its implementation , is depicted in Figure 2.4.

In E-SPONDER the unifying protocol suite for the many different host-to-network technologies is TCP/IP because it is capable to offer a flexible transport mechanism that is independent of the required service typology. This choice, however, share a disadvantage with the internet: IP is a best-effort protocol, i.e., it cannot guarantee the quality of service currently required by network applications. In order to solve this problem it is necessary to adopt proper techniques to manage the QoS and several solutions have been considered:

- at data-link layer: IEEE 802.11e protocols [12] and IEEE 802.11s ones [13];

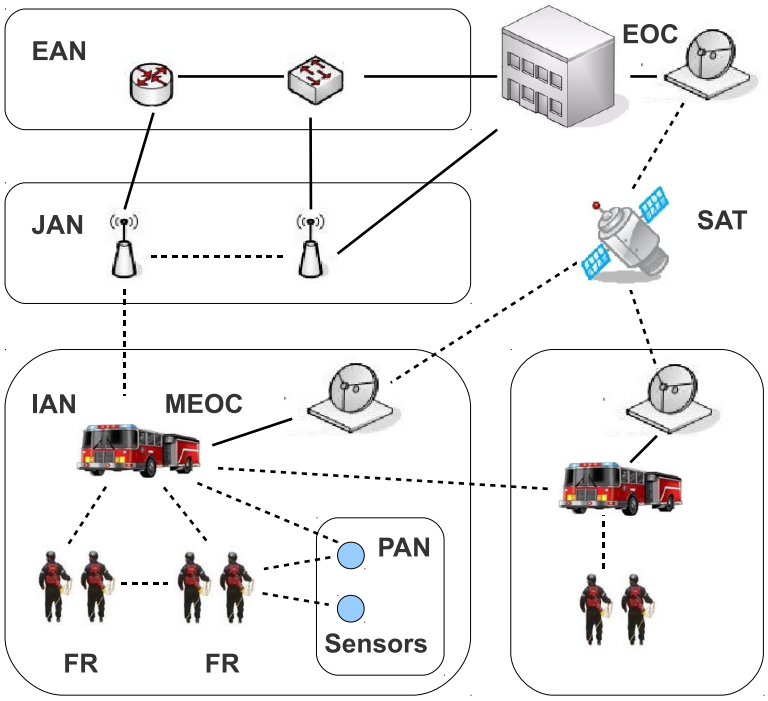


Figure 2.4: E-SPONDER's telecommunication network - a general view.

- at network layer, such as IntServ[1] [14] and DiffServ [15];
- at application level, e.g., by prioritizing specific data flows.

2.5.2 Network services and possible solutions

Regarding the network applications that should be suppported, according to Section 2.3, we may find:

1. Voice calls (between two users and/or to support tele-conferences), which can be implemented by means of voice over IP (VoIP) technology. More specifically, open and interoperable solutions should be adopted, such as *session initiation protocol* (SIP) [16] and *real-time transport protocol* (RTP) [17].

[1]Please note that E-SPONDER focuses on the design of an infrastructure-less network architecture, which should operate independently of any pre-existent network (such as any cellular or wired one). This makes the E-SPONDER network less exposed to scalability issues that arise in traditional IP networks employing IntServ.

2. Video streaming, to provide enhanced situation awareness to the commanders at the EOC or at the MEOC. Again, open technologies similar to those considered for VoIP service should be employed as well.

3. Sensor data transfers, to stream field measurements to the EOC and/or to the MEOCs.

4. Generic data transfers, usable to support database queries, to transfer detailed 2D/3D maps of the crisis scenario, etc.

2.6 Summary

Current state of the art public safety systems suffer from limited interoperability, due to their intrinsic features, and limited support for current broadband multimedia applications. The need of scalable and flexible architectures suggests new ways to design and implement a public safety system, such as adopting emerging wireless mesh network technologies. Thanks to IP connectivity and to widespread digital technologies, real interoperable wireless mesh networks can be effectively designed to match the needs of any emergency response, as in the case of the E-SPONDER project.

Chapter 3

Security Issues in Emergency Networks[1]

3.1 Introduction

This Chapter reviews the most important security properties found in traditional computer systems from the perspective of a possible network architecture for implementing modern public safety systems. The main goal of this research has been to find what properties affect the most the design of an emergency response network, together with the study of the set of the available solutions that can be used to implement these properties in an actual emergency network.

As already described in the previous Chapters, a public safety system is a complex system designed to operate in, virtually, any crisis scenario, with the goal to coordinate the emergency response. Such a system includes a communication infrastructure usable to support (almost) every communication service needed by the first responders (FRs), such as police and firefighters. This network, in the following denoted as an *emergency network*, is vital for the entire public safety system and, thus, needs to be designed carefully.

In [11] a deep analysis has been carried out to formalize and define the operational requirements for such a system, in order to provide a comprehensive

[1] 2011 © IEEE. Reprinted, with permission, from: Casoni, M., Paganelli, A., "Security issues in emergency networks", IEEE 7th International Wireless Communications and Mobile Computing Conference (IWCMC), 2011, pp. 2145-2150.

document usable as an input for the development of technical/technological solutions for interoperable emergency networks. One of the most critical aspects that needs to be carefully addressed regards *information security*.

The purpose of this Chapter is to *specialize* the security requirements described in [11] for the E-SPONDER system (see Chapter 1 and Chapter 2), describing the practical issues we have found during design of the emergency network, as well as the security solutions and protocols currently exploitable within the project.

This Chapter is organized as follows. In Section 3.2 we describe in details the functional requirements for an emergency network, while in Section 3.3 we review the most important security properties for a computer network (we refer to these networks with the terms "classical" or "traditional" in the remaining of the Chapter), which will be analyzed under the emergency network point of view in Section 3.4. In particular, in this Section we describe our analysis and our outcomes regarding the security properties that affect the most the design of the system architecture for such a network. In Section 3.5 we sum up with our conclusions and we report some suggestions for possible future work.

3.2 Emergency Networks

3.2.1 Functional requirements for emergency networks

As already described in the previous Chapter, from [11], the main functional requirements for a modern public safety system and for its network architecture can be summarized as follows:

- it should be reliable and available (that is, it should be prompt at, virtually, any time);
- it should be secure and should make use of authentication control and authorization mechanisms;
- it should guarantee the confidentiality of the data travelling across it;
- it should be scalable, both horizontally (i.e. with the spatial extension of the emergency scenario) and vertically (i.e. with the number of the users);

- it should be interoperable, that is, it should adopt standard and open (i.e. with well defined interfaces) technologies, in order to simplify the interconnection with existing systems and to take advantage of the economies of scale;

- it should support quality of service;

- it should support users' mobility;

- it should be characterized by high survivability (i.e. it should survive to, virtually, almost all possible failures).

The design of the system architecture for an emergency network means the "translation" of these requirements into a practical set of technologies, protocols and solutions composing a possible real implementation. This typically requires the designed to find a trade-off solution between conflicting requirements.

3.2.2 A possible attack scenario and emergency network's security requirements

An attacker acting on the emergency field may have the following goals:

1. exploiting the emergency situation for personal gain (e.g., accessing to confidential information related to the people involved in the crisis, such as healthcare data);

2. increase the impact of the disaster or make the disaster response ineffective (e.g., a terrorist attack).

As for the telecommunication network, the first case can stem from an intrusion or from data sniffing, while the second one can be translated into a denial-of-service (DoS) attack. These simple examples suggest that the main security requirements for an emergency network are *confidentiality* and *availability*. Moreover, *authentication*, together with *authorization*, can help in the reduction of DoS attacks from within the network. These properties will be described in Section 3.3.

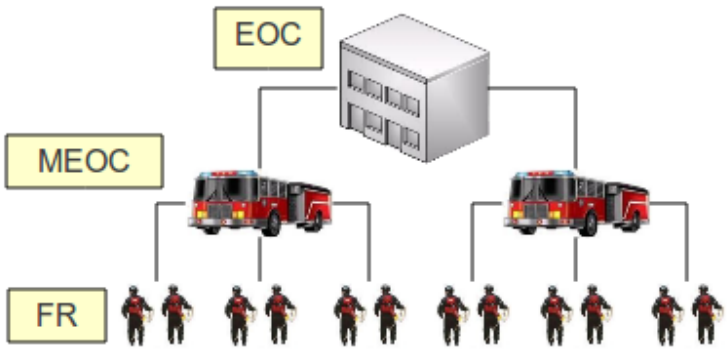


Figure 3.1: High-level E-SPONDER architecure. © 2011 IEEE

3.2.3 The E-SPONDER project's emergency network

For a matter of clarity, here we briefly report the high-level system architecture for the E-SPONDER project's network [3], which is depicted in Figure 3.1. There we can find:

- The emergency operation center (EOC). It is the command and control center for the crisis scenario, often located away from the operation field.
- The mobile EOCs (MEOCs). These are *local* and *mobile* (e.g. they may be implemented over specialized terrain vehicles) command and control centers, that may be deployed close to the crisis scenario. These need to be connected to the EOC for the coordination of the emergency response.
- The first responders (FRs). They are the people involved in the crisis response since the very beginning (such as police, firefighters, etc). They need to be connected with the local MEOC(s) to communicate either with it(them) or with the EOC.

3.3 Generic security properties and issues

In this Section we review the most important security properties that can be found in a "classical" computer network. Please refer to [18] for a more detailed description of these properties and solutions.

3.3.1 Simple and mutual authentication

This property relates to the ability of a host/system to correctly identify another host/system. In particular, with *simple* authentication we mean a "one-way" authentication, that is, the generic host needs to verify only the authenticity of the recipient, but not the converse. With *mutual* authentication we mean a "two-ways" procedure, in which each of the hosts involved in the communication can successfully identify the other.

Obviously, authentication is a very important property in many widespread services, such as e-commerce, in which the identity of the seller's website needs to be verified prior the actual purchase.

Generally speaking, we have three main authentication types:

- solutions based on something known by the user (such as a password);
- solutions based on something the user posses (such as a badge);
- solutions based on something the user is (such as biometric footprint).

These factors are listed in ascending order of importance (in fact, a password can be quite easily stolen or sniffed, while it is more difficult to overtake a biometric authentication system); moreover, these can be combined together to realize a stronger authentication mechanism (e.g., two and/or three factors authentication methods).

Nowadays, the most widespread authentication systems can be classified as:

- systems based on repeatable passwords;
- systems based on one-time-passwords (OTP, which are disposable passwords that can be discarded after their use);
- systems based on OTP with a timestamp (i.e., the disposable password is associated with a lifetime, after which the password must be discarded);
- systems based on symmetric (i.e., with a shared secret) challanges (private key systems);
- systems based on asymmetric challanges (public key systems);

- systems based on a *subscriber identity module* (SIM), which are typically found in cellular systems;
- biometric systems.

Please note that, besides the conceptual differences existing between these systems, an additional aspect that separates them in two distinct classes is related to the use (or not) of a *trusted third party* (TTP), i.e., a third node, other than the two nodes involved in the communication, which can be used to check the correctness of the users' identities. A TTP can be usually found in systems based on asymmetric challanges, such as in the case of a *public key infrastructure* (PKI), in which the TTP coincides with the *certification authority* (CA, the entity responsible for signing the public key of each user), but characterize also those based on SIMs.

It is intersting to cite also the "Open Authentication" (OATH) project [19], which targets "the realization of an open reference architecture for strong authentication by leveraging existing open standards" [19]. This project suggests to adopt the best and most widespread authentication solutions available to implement an integrated "core set" of authentication credentials, which could be possible to integrate together into a single secure authentication device that can be used for authentication purposes with a many networks and services.

Finally, it is important to say, as suggested in [19], that with "authentication" we may refer to two distinct possible situations:

1. Network (or access) authentication, in which a user needs to authenticate with the network provider in order to make use of the communication infrastructure.
2. Application authentication, in which a user who has already accessed the network needs to authenticate with the application server (or directly with the end-user or system) to make use of the service required.

This distinction is very important, mainly because we can classify every authentication method based on which problem it addresses (e.g., a SIM approach for network authentication and a public key one for authenticating with a remote SSH server).

3.3.2 Data confidentiality and secrecy

This property aims at the hiding of the content of a message to unauthorized users. Secrecy is usually implemented with cryptography, both asymmetric (for the initial session key establishment) and symmetric (for the actual data exchange).

Nowadays, almost every communication standard (e.g. IEEE 802.11i, IEEE 802.16, UMTS) implements cryptography. Moreover, cryptography can be found also at higher levels of the stack, such as at layer 3.5 (e.g. with IPSec), at layer 4.5 (e.g. with SSL/TLS) and at application layer (e.g. with SSH).

3.3.3 Data/origin authentication

This property relates to the capability of a system to correctly identify the sender (or the author) of a message. This requirement is particularly felt in those situations in which a message needs to travel across many intermediate nodes, before reaching the recipient: in this case, each of the intermediate node may alter the message by changing the actual sender identifier with a bogus one.

Another similar situation is related to *identity thefts*, in which a malicious user could try to illegally impersonate a legitimate user. Data authentication can be achieved with the use of hash functions and both symmetric and asymmetric cryptographic techniques. By sending the message m together with its (a)symmetrically encrypted digest $K(H(m))$ [18], the recipient can check if the message actually comes from the intended sender or not, by decrypting the digest with the symmetric key (or the sender's public key, in the case of the use of an asymmetric crypto). Nowadays, most of the transmission technologies implement data authentication with *message authentication codes* (MACs).

3.3.4 Authorization/access control and accountability

Authorization is related to the granting of access rights to the resources of the system (or the network) to only specific users. This is typically performed after the authentication procedure, and is related to the accountability property, which is the property of keeping track of some of the users' actions. Authorization can be accomplished by defining specific policies for each user or for each group of users,

while, on the other hand, accounting can be implemented by means of logging the most important activities, in order to find possible misuses of the network or the service.

Because of this relationship, it is possible to implement authentication, authorization and accounting (AAA) by using a single server, called AAA server. The most widespread AAA server currently available is RADIUS (which, in turn, stands for Remote Authentication for Dial-In User Services), although its direct evolution, called Diameter, is gaining popularity.

3.3.5 Data integrity

This is the capability of a user to verify if a message sent over a network, or data stored in a memory, has been modified since its creation. Data integrity can be achieved by using *secure hash functions*, which are a particular sub-class of hash funtions [18].

Data integrity is usually combined with origin authentication in the message authentication codes (MACs), which, nowadays, are widespred in almost every networking standard.

3.3.6 Non repudiation

This property is related to the capability of a system to prevent a user from repudiate the sending (or the reception) of a given message. This, together with data authentication and data integrity provides the basis to the *digital signature*. Non-repudiation is particularly important in e-commerce websites, in which, for instance, the webstore should not be able to repudiate the reception of a payment.

3.3.7 Availability

This is the ability of a system to be prompt and usable when the user needs it. This property is particularly important for those services strictly connected to the preservation of human lives, such as in the case of *emergency networks*.

3.4 Security in emergency networks

3.4.1 Goals

In this Section we discuss the aforementioned properties in the specific context of emergency networks. The main goals of this Section are:

- the review of the properties described before, in ordert to evaluate their relative importance in this new context;
- the review of the "classical" security paradigms and solutions to evaluate if they can be extended to emergency networks;
- the proposal of new research ideas for the properties for which the "classical" security approaches are not well suited.

In the following, the various security properties will be presented in the order of importance that reflects how much the property itself affects the design of the whole system.

3.4.2 Simple and mutual authentication

The authentication issue is one of the most important in emergency networks, because it has a significant effect on the design of the whole system.

Authentication, in this context, should be addressed with a solution that can be performed quickly and in a simple way. It should be possible to execute the authentication procedure even in the case of partially network disconnection; in the worst case, it should be possible for two hosts to authenticate each other without the need of a network connection with other systems. Moreover, some of the most secure approaches, such as the biometric ones, could hardly be used in particular context (e.g. when the first responder wears a protective suit or gloves), preventing them to be used as the only authentication method, because they require (at least) a backup one. Lastly, even if 2/3-factors authentication methods are very robust, they may require additional efforts for the user, with respect to a single-factor one, which could limit their effectiveness in emergency

networks (e.g. what could be done if a first responder loses his/her ID badge during the emergency?).

Even if authentication is one of the most important security aspects even in emergency networks, it should be clear that, as described in Section 3.2, the main goal of this kind of network is to effectively support the activities of the first responders, to help in protecting or saving lives: it would be unacceptable if a security protocol could decrease the effectiveness of the whole emergency response system. For this reason, a tradeoff solution, between security and usability/effectiveness, should be found.

In the following, we describe some possible solutions that can be adopted in emergency networks, depending on the particular context considered.

3.4.2.1 Overview of the alternatives

First of all we can find the *repeatable password* based approach, for which a previously set password can be used as a shared secret (even for cryptographic purposes). This simple approach is, obviously, the least secure one: if a password is re-used for long time, it has high chances to be sniffed or to be guessed. Moreover, with this approach it is not possible to interoperate with different jurisdiction (e.g. police with firefighters), because each password has only a local meaning. This approach can be used, thus, only in limited scenarios, in which interoperability is not an important feature, together with a strict password change policy.

A second approach is represented by *symmetric challange systems*, in which a user can be authenticated successfully only if he/she owns a pre-shared secret, used for symmetric cryptographic purposes. The main drawback for this approach is related to the high number of secrets that need to be shared, which grows as N^2 (where N is the number of the hosts of the network) and make this approach not scalable for large contexts.

A similar approach is represented by *asymmetric challange systems*, very similar to the previous one but with the use of asymmetric cyphers. In order to guarantee the correctness of each user's identity (i.e. his/her public key), we have two possibilities: the first requires that each public key has been previously stored inside each node of the network (which is the same situation of the symmetric challange systems); the second requires the use of a TTP acting as a CA. This

approach makes the network more scalable than the previous case, but requires also that the CA could be accessed at any time, which cannot always be the case in emergency networks (e.g. due to fading, interference, failures, etc).

One possible tradeoff solution is represented by the PGP's *web of trust* model [20], in which user A can "trust" user B by checking if B's public key has been signed by himself, or by a third user C in which A already puts his/her trust in. In this way, the "trust" propagates through the network, by means, for example, of X.509 certificates; each user can trust another one by searching in the certificate chain a path that connects him to his/her counterpart. This approach has the great benefit of being completely de-centralized (i.e. it does not require a CA).

Another class of methods is related to *OTP*, which, as described before, are very simple yet robust. The main problem is related to the counterpart to which the user wish to autenticate: if the authentication process is a related to a network access process, then the procedure involves only the user and the authentication server (AS, typically through a *network access server*, NAS), which limits the setup of the OTP system to only these entities. On the converse, if it is an application authentication process, then the procedure involves the two end-points of the application (depending on the actual system configuration, these may be two users for a VoIP call, a SSH client and a SSH server, etc), which may require a large number of OTP systems to be set up, which, in turn, may require large memory usage. OTP system which are also time-based require network-wide time synchronization too, which may be hard in specific circumstances. Even more significant, this solution cannot be applied to authenticate users who belong to different jurisdictions, without the use of a proper authentication gateway.

Another approach is based on *SIM* authenticators, that can be typically found in cellular systems for network authentication. Even in this case, there is the need to use an authentication gateway to allow inter-jurisdiction authentication.

Another different approach is the use of Kerberos [21], a ticket-based single sign on (SSO) system that can be used to authenticate users to many different services over an insecure network. The main problem of using Kerberos in an emergency network is related to its possible disconnection, that make the Kerberos' *key distribution system* (KDS) unreachable for the users.

Next, as cited before, OATH's vision [19] seems to be the most conscious one,

because it suggests the adoption of a *set* of authentication methods, rather than a single one, each one for a specific purpose. The "all-in-one" security device conceptualized within the project [19] could bring together many authentication solutions into a single device, in order to allow the user to authenticate successfully to many networks and services; a similar device could be adopted (or implemented inside the FRU) also in an emergency network.

In [22] the authors review the whole plethora of solutions that can be applied in mobile ad-hoc networks (MANETs), starting from symmetric solutions (such as the Bluetooth and the IEEE 802.11 models) and ending with asymmetric ones. In addition to those solutions, similar to the ones we already described, the authors report asymmetric solutions such as the *identity based cryptography model* and the *self-certified public key model* (which both do not make use of certificates); moreover, they describe also the *self-organization model* and the *trusted subgroup model* (which both do not require a CA).

Finally, *simultaneous authentication of equals* [23] (SAE) is an authentication method developed specifically for wireless mesh networks (WMN) and currently considered within the IEEE 802.11s working group for implementing a secure authentication in 802.11-based mesh networks. This approach, which focuses on the authentication of the node's neighbours, is based on a pre-shared secret, which can be distributed at the network setup phase. This is a very general for mesh networks and it is not bounded to only the IEEE 802.11 technology.

3.4.2.2 Lessons learned and project vision

The above discussion led us to identify the following requirements for an authentication method for emergency networks:

- The method should perform quickly and, possibly, without human intervention.

- The method should work even if the network is partially disconnected; in other words, it should be possible to authenticate with the network or with the recipient if they are reachable, without the involvment of additional systems.

- The method should be scalable.
- The method should be extensible (e.g. programmable to implement different actual solutions) and should allow inter-jurisdiction cooperation.

Under this vision, one of the most promising solution is the adoption of a single device, similar to that envisioned in OATH, which could be programmed accordingly to the requirements of the crisis context (possibly over the air); possible solutions are the development of such a device as a detachable module for the FRU or the implementation inside it.

Moreover, the authentication approach should not require the use of a special system, such a CA, because it could become unreachable in case of network disconnection. Some of the exploitable solutions are, thus, identity-based cryptography and the self certified subgroup model, which both do require the use of a CA, but only at the setup of the network (which may be during the initial briefing of the FR group); other, completely distributed systems are the self organization model and the trusted subgroup model (see [22] for details). In the case of a mesh-based networks, SAE seems a very effective solution (it requires only the sharing of a secret during the setup/briefing phase).

For inter-jurisdiction operation we may have some alternatives:

- For identity-based cryptos it is possible to have the CAs of the two (or more) jurisdictions to communicate together to exchange the actual settings of the id-based system [24], which differ from one jurisdiction to the other; in this way, it would be possible to extend the use of the identity-based crypto outside the original jurisdiction. Although this solution requires that the users could communicate with their own CA, which is not usually the case, it may neverthless be acceptable, because inter-jurisdiction communications, in some specific scenario, are less frequent and may be more delay tolerant than the intra-jurisdiction ones. Moreover, the crypto's settings need to be exchanged only once and, after that, the access to the CA becomes unnecessary.
- For both the self-organization model and the trusted subgroup model, it can be possible to have the first responder chief to act as a guarantee for his/her

FR group, by digitally signing the group's public keys. Prior the actual inter-jurisdiction communication, the two (or more) FR chiefs exchange and sign their respective public keys, allowing their respective groups to "trust" each other.

3.4.3 Data confidentiality and secrecy

In an emergency network, data confidentiality is a mandatory feature, because there are many situations in which it is necessary to hide the content of a communication or a data transfer (e.g. healthcare data transfer for people involved in a terroristic attack, the coordination of a secret strategic plan between the forces acting over the field, etc). This, however, should not be a limiting feature, as stated before for authentication.

3.4.3.1 Lessons learned and project vision

The research perfomed on the technological solutions for data confidentiality led us to state that the choice of the specific confidentiality approach depends on:

- the transmission technologies and standards adopted for implementing the system;
- the *scope* of the cryptographic technique (i.e. is it an end-to-end solution or a hop-by-hop one?);
- the presence of additional specific requirements, such as QoS.

In fact, as stated in Section 3.3.2, almost every transmission technology provides its own cryptographic solutions, which could be used to guarantee data confidentiality over a single-technology network (that is, a *local* cryptographic approach, valid only between the boundaries of the adopted transmission technology); on the converse, higher-layer approaches could be used to increase the scope of the secrecy solution, overcoming the layer 2 network boundaries (e.g. IPSec, SSL/TLS, etc).

The choice between these contrasting methods depends heavily on the network topology and on the whole system architecture; from another point of view, these

considerations would steer the design of the whole system and network architecture.

Within E-SPONDER, we have considered several alternatives:

1. A full layer-2 implementation, where each network segment implements its own cryptographic solution, providing confidentiality on a hop-by-hop basis. This solution allows both routers and network gateways to perform service classification to enforce QoS, by means of packet inspection, which is made possible since no encryption is employed above the MAC layer. Because of this separation between cryptography and QoS functions, this trade-off approach seems to be effective and practical for the E-SPONDER platform.

2. A full layer-3 implementation, based on IPSec and IPv6. Since IPv6 offers more flexibility than IPv6 regarding flow classification (providing up to 28 bits in its header usable to identify the traffic class and the label for each flow) compared to IPv4 (which provides in its header 6 bits only), it is possible to easily exploit this feature with IPSec (employing *encapsulated security payload*, ESP) to enforce both QoS and confidentiality.

3.4.4 Availability

One of the most important features of an emergency network is availability: as described previously, the network should be ready and usable every time a user needs it. Think, for instance, at the need to send an warning signal in response to an extraordinary event, such as the explosion of a bomb or the collapse of a building, in order to alert the people in the surroundings of the danger zone.

3.4.4.1 Lessons learned and project vision

Within the european project, we believe that availability can be enhanced by adopting redundant solutions, thus enhancing the number of alternatives that can be used to serve each incoming request.

As regards computer systems, the main principles that can be applied to enhance availability are replication (i.e. implementing redundant systems) and caching (i.e. store the required data for further access). This could be done, in

principle, with respect to those systems which are vital for the correct operation of the whole network, such as the CA servers.

Regarding the telecommunication networks, the availability can be enhanced by introducing redundant links and redundant technologies (which increases also interoperability).

In order to choose the correct number of redundant systems/technologies that need to be implemented, we have performed careful analysis, whose target has been to identify the weakest part(s) of the entire system. One of the most important link that can affect the most the overall performance of the network is the one connecting FRs to the MEOC, because, depending on the kind of emergency in place, the FRs may operate far away from it, thus increasing the outage probability. On the other hand, we believe that the inter-MEOC links could be more reliable than the previous ones, mainly due to different technologies considered for their implementation (i.e. IEEE 802.16 and DVB-RCS, with respect to IEEE 802.11 for FRs' network) and because of the lesser stringent power requirements than those that characterize the FRs' equipment.

3.4.5 Authorization and accounting

Authorization and accounting are properties that one usually finds together with authentication (implemented, as described before, by means of AAA servers). This holds also for our project, depending on which of the aformentioned authentication solution is considered for the actual implementation. This implies that it is the authentication procedure that actually affects the system design, with respect to authorization and accounting.

However, there are some cases in which these properties can be found separed from authentication. Think, for instance, at the traffic filtering function that a gateway node can perform, or at the logging capabilities provided by the operating system installed on each node/device.

3.4.5.1 Lessons learned and project vision

Within the european project, we believe that there will be more than a single authorization and accounting procedure throughout the whole system. First of

all, this is due to the different authentication mechanisms that one can find in such a system (i.e. network access authentication and application authentication); moreover, it is possible to implement logging and data integrity functions in almost every node of the system (depending, obviously, on the computational capacity required), in order to reduce the risk of node impairment by the action of a malicious user. Finally, it would be possible, in principle, to apply a distributed traffic shaping and filtering method, in order to allow only certain authorized protocols, users and/or systems to access to the network resources and services.

In our view, we believe that these two properties do not affect the design of the system in a deep way; it is possible, thus, to delay the choice of the authorization and accounting solutions after those related to authentication, confidentiality and availability.

3.4.6 Data authentication, data integrity and non repudiation

Even if data authentication, data integrity and non repudiation are very important features for an emergency network, almost every low-layer (e.g. 802.11) and high-layer (e.g. SSL/TLS) technology implements them; this, in turn, limits the effect these properties have on the design of the architecture of the system.

3.4.6.1 Lessons learned and project vision

As introduced before, the choice of the specific method for data authentication, integrity and non repudiation depends on the choice of the communication technologies. Moreover, the low-level implementations can be used only to guarantee the aformentioned properties on the local network, and not in an end-to-end fashion; for this issue, and depending on the service/application requirements, it is possible to adopt IPSec or SSL/TLS.

As stated before for authorization, we believe that also data authentication, data integrity and non repudiation are properties that actually do not affect deeply the whole system design, making the implementation decision about them delayable with respect to the other properties described before.

3.5 Summary

In this Chapter we have presented a careful analysis of the security issues and properties for an emergency network, to find those that most affect the design of the whole crisis response network. During this analysis we found that authentication, confidentiality and availability affect the project in a significant way, starting from topological constraints imposed by some of the authentication method described before, to the difficulties related to the implementation of cryptography together with QoS mechanisms. Conversely, the remaining properties affect the project in a minor way, thus relaxing their actual implementation. Moreover, this analysis suggested some possible research topics that can be studied and evaluated in some future work.

Chapter 4

QoS Performance Evaluation of Multimedia Services in Emergency Networks[1]

4.1 Introduction

As deeply described in previous Chapters, modern public safety systems have to address several issues shared among most of the standards and most of the technologies currently used for their implementation. For instance, the limited use of standard and off-the-shelf technologies poses serious limits regarding interoperability; moreover, many jurisdictions still use outdated equipment or infrastructures (e.g., analog radios, used to provide only voice service), which, nowadays, can't enable an effective emergency response.

Hence, the design of a modern public safety system, and of a cutting edge emergency network architecture, requires to carefully consider the support to several different applications and services, together with state-of-the-art ICT technologies. This can be translated into the finding of the best set of applications and technologies that can provide the most effective response to crisis events. Following a top-down approach, given the set of services required by the end-users

[1]2012 © IEEE. Reprinted, with permission, from: Paganelli, A., Saladino, D., Casoni, M., "QoS Performance Evaluation of Multimedia Services in Emergency Networks", IEEE 8th Wireless Communications and Mobile Computing Conference (IWCMC), 2012, pp. 933-938.

(e.g., police, firefighters) the designer needs to assess whether the underlying ICT infrastructure could properly support them.

One of the main goals of our research activities, that led to the results described in this Chapter, has been the evaluation of the *quality of experience* (QoE) perceived by the end users of the E-SPONDER's emergency network; hence, the first step in this direction has been the assessment of some network-side metrics, representing the *quality of service* (QoS) provided in a reference specific context, which have been easily obtained by means of simulation software.

This Chapter presents our work regarding the study of the performance achievable by an emergency network architecture and by the considered communication technologies, in terms of QoS. More in detail, first of all we have identified the communication services necessary to be provided in any emergency network and we have analyzed them in order to determine their bandwidth requirements. Then, the next step has consisted in simulative tests in order to assess if each network segment composing the proposed architecture, as well as the proposed communication technologies, can effectively support all the considered emergency network services, providing adequate QoS.

This Chapter is organized as follows. In Section II, we give a short presentation of the examined emergency system, whereas Section III provides a general description of the communication services to be supported. Section IV presents the analysis of the services bandwidth requirements of each considered network segment, while, in Section V, some numerical results are presented. Finally, Section VI summarizes the main findings and describes our possible future works.

4.2 System Architecture

4.2.1 Reference network architecture

As briefly depicted in Figure 4.1, and as already described in previous Chapters, a generic emergency network, and, in particular, the E-SPONDER's one, is composed by an Emergency Operations-control Center (EOC), some Mobile Emergency Operations-control Centers (MEOC) and some groups of first responders (FRs), each one equipped with a FR unit (FRU).

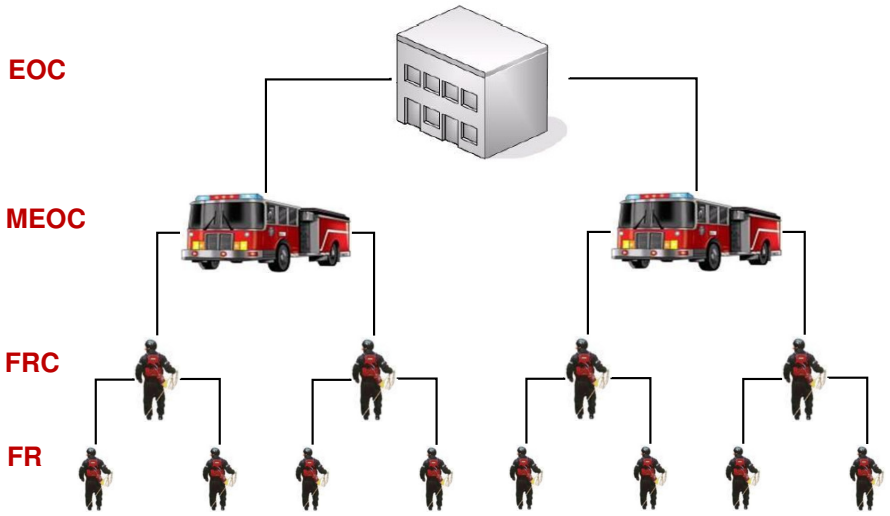


Figure 4.1: Reference emergency network architecture. © 2012 IEEE

A possible way toward the design of such an architecture is represented by a hierarchical wireless mesh network (WMN) approach [10], which provides several benefits over conventional architectures, like modularity, open connectivity (e.g., toward the Internet) and flexibility.

A careful analysis of the user requirements is a fundamental step to extract the main needs of any public safety agency and, correspondingly, to define the best network configuration to provide efficient rescue operations. Therefore, in what follows, we have considered FR teams composed by up to 8 FRs and one FR chief (FRC), which is the most common configuration of a typical FR team in most of the European countries. The FR chief coordinates the on-field emergency response activities and rescue operations of his/her corresponding FRs team. From the network point of view, he/she is a special node, acting as a bridge between the FRs team and the MEOC, and as a hub for any kind of FR communication[2], as depicted in the reference network architecture of Figure 4.2.

The EOC is located at the headquarters of the public safety agency, it is responsible for the coordination of the rescues and communicates with the MEOC or the first responder chief, if the MEOC is not deployed on the field yet. The MEOC acts as a virtual bridge between the FRs and the EOC (see Figure 4.2).

[2]As the FR chief may represent a single point of failure, it is possible to contemplate the adoption of backup solutions to improve the network availability.

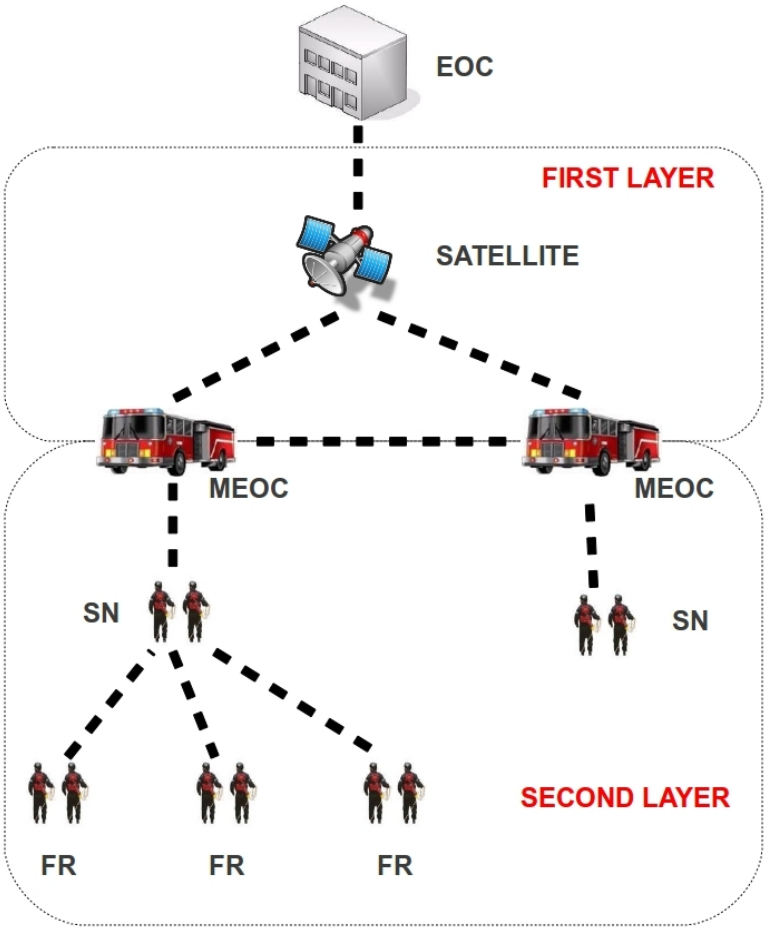


Figure 4.2: Reference network architecture.

Moreover, possible MEOC-to-MEOC communication links can be established, in order to improve the overall availability of the system, as described in the previous Chapter.

4.2.2 Enabling technologies

Modern conventional wireless transmission technologies and standards can be effectively implemented in emergency scenarios as well, to provide enhanced situation awareness (e.g., by offering video capabilities, as well as high data-rate Internet connectivity) with respect to the technologies currently employed.

As described in Chapter 2, in order to support FR-to-FR communications in E-SPONDER, the technology we have taken into account is IEEE 802.11-based WLAN technology; more in details, we have considered a star-based, infrastructure-mode 802.11 architecture, where the access-point node is implemented in the FR chief's FRU. The main reason for this choice has been to provide communication capabilities to the FRs even if the group is partially disconnected from the rest of the network, by allowing them to make use of a subset of the services supported by the system.

As for the link between the FR chief and the MEOC, we have considered IEEE 802.16-based WMAN technology, which provides longer-range connectivity than IEEE 802.11 (with maximum theoretical range of about 50 km) and QoS support by means of traffic differentiation.

Finally, as the distance between a MEOC and the EOC can span from few to, maybe, hundreds of kilometers, one of the most suitable communication solutions exploitable for the MEOC-to-EOC link appears to be satellite, as described in [3], which is capable to provide connectivity even if any ground-based telecommunication infrastructure (e.g., 3G or IEEE 802.16) is unavailable or destroyed; more in detail, we have taken into account Digital Video Broadcasting - Return Channel via Satellite (DVB-RCS) technology [25].

The proposed architecture offers high scalability, thanks to its hierarchical structure, which can be tailored to the specific requirements imposed by the crisis event, at the price of a light increase in the overall network complexity, if compared with other non-hierarchical solutions. However, it is important to underline

that the benefits coming from this approach greatly outweigh the drawbacks, and provide us with a real and practical approach toward the implementation of next-generation emergency networks.

4.3 Communication Services

In order to allow the rescuers to communicate each other, one of the most important services that has to be provided in any emergency system is represented by voice calls among the FRs and MEOC/EOC. This kind of service can be implemented by means of Voice over IP (VoIP).

Some of the most widespread audio codecs, usable for a VoIP service implementation, as reported in [26], are:

- IS-127, that is a very high compression ratio codec and requires a bit-rate of 4.2 kbit/s;
- G.729, that operates at a bit-rate equal to 8 kbit/s and is mostly used in VoIP services thanks to its low bandwidth requirements;
- G.726, that requires a bit-rate of 32 kbit/s; (iv) G.711, that operates at a bit-rate of 64 kbit/s.

Furthermore, in order to have a clear and precise vision of the emergency scenario, a second valuable service that has to be provided to the FRs is real-time video, implementable by means of Video over IP (VIP); this way, it is possible to provide better awareness of the disaster scenario to the MEOC/EOC and to consequently organize effective rescue operations. In E-SPONDER, we consider that only the FR chief is equipped with a proper designed video camera and, therefore, he/she is the only FR that can make use of this service. In addition, two commonly used video codecs we considered for a possible VIP implementation are MPEG-4 (Moving Picture Experts Group-4) and H.264/AVC (Advanced Video Coding).

The garment of each FR is equipped with several sensors (which are used to monitor, for instance, temperature, heartbeat, breath, and so forth), whose information have to be transmitted by the FRU toward the MEOC/EOC. Hence, since the transmission of sensor data requires approximately a bit-rate of the order

of $1 \div 2$ kbit/s, we suppose to adopt either ZigBee standard, also known as IEEE 802.15.4, or ANT.

Finally, also generic data transfer service may be of significant importance in specific crisis scenarios (e.g., the transfer of a picture or the map of the incident area) and has to be supported as well.

In conclusion, please note that even if each described service has specific bandwidth requirements, time-sensitive applications, such as VoIP and VIP, impose delay and jitter constraints too, as will be described next.

4.4 Theoretical Bandwidth Requirements

This Section presents the aggregate bandwidth requirements for each of the services described so far.

Regarding VoIP service, we assume that all the FRs communicate through a VoIP teleconference, which can be implemented in several ways. In what follows, we take into account different implementation approaches, namely:

- the employment of a *conference bridge* and *media mixing server* on the FR chief [27], that has to provide SIP signaling, to merge all the voice streams and to work as a relay. Here, each node has to contact the conference bridge in order to communicate with every other node;

- *multi-unicast*, that corresponds to a full mesh overlay, where every node communicates directly with all the other nodes;

- *multicast*, where data are sent simultaneously to a group of nodes belonging to the same multicast group in a single transmission.

Even if the most suitable approach to VoIP teleconference is based on multicast, here we consider the previous approaches, too, for the sake of completeness.

In order to compute the theoretical bandwidth requirements, as described in Section 4.2, we consider a team composed by eight FRs ($N_{FR} = 8$), one FR chief ($N_{FRC} = 1$); moreover, we have one bidirectional VoIP stream between the MEOC/EOC and the FR chief ($\tilde{N} = 1$).

As for the protocol stack overhead, we consider the use of *real-time transport protocol* (RTP) and UDP to convey VoIP and VIP, while we adopt UDP only to transfer sensors data; we consider TCP to support only the data-transfer service (the size of each TCP segment is 1024 byte). The overall protocol overhead at IP layer is, thus, 40 byte for VoIP and VIP (12 byte for uncompressed RTP header + 8 byte for uncompressed UDP header + 20 byte of uncompressed IP header), 28 byte for sensors (8 byte for UDP header + 20 byte for IP header) and 40 byte for data-transfer (20 byte of TCP header + 20 byte of IP header).

4.4.1 FRs Network

As for the network of the FRs, we assume that the predominant services are VoIP communications and sensor data to be transmitted.

More in detail, the number of VoIP streams (N_{VoIP}) is:

- $N_{VoIP} = 2 \cdot (N_{FR} + \tilde{N} + N_{FRC})$ for conference bridge implementation;
- $N_{VoIP} = (N_{FR} + \tilde{N} + N_{FRC}) \cdot (N_{FR} + \tilde{N})$ for multi-unicast implementation;
- $N_{VoIP} = (N_{FR} + \tilde{N} + N_{FRC})$ for multicast implementation.

Thus, by using the previous relations and by considering also sensor data service (from any FR to the FR chief), the maximum bandwidth requirement is of about 8 Mbit/s, if we adopt the G.711 codec with 10 ms long frames and employing the multi-unicast approach, whereas the minimum bandwidth requirement is of about 200 kbit/s, if we adopt the IS-127 codec with 20 ms long frames and using the multicast approach.

In our view, a possible acceptable configuration is the one employing the G.726 codec, with 10 ms long frames and adopting a conference bridge on the FR chief, which requires just 1.2 Mbit/s.

4.4.2 FR chief - MEOC link

As for the link between the FR chief and the MEOC, we suppose to support VoIP, VIP and sensor data in uplink and data transfer service in downlink.

Thus, the number of VoIP streams (N_{VoIP}) is[3]:

- $N_{VoIP} = 2$ for conference bridge implementation;
- $N_{VoIP} = 2\tilde{N} \cdot (N_{FR} + N_{FRC})$ for multi-unicast implementation.

Again, it is straightforward to compute the maximum bandwidth requirement, which is about 0.9 Mbit/s for VoIP, if we adopt the G.711 codec with frame of 10 ms and employing the multi-unicast approach, and about 630 kbit/s for VIP service, if we adopt a codec of 400 kbit/s with 70 bytes long packets. The overall bit-rate requested is around 2 Mbit/s, considering also the data transfer service and sensors data transmissions.

On the other hand, the minimum bandwidth requirement is about 20 kbit/s for VoIP, if we adopt the IS-127 codec with frame of 20 ms and employing a conference bridge on the FR chief, and about 67 kbit/s for VIP service, if we adopt a codec of 64 kbit/s and 1000 bytes long packets. The overall bit-rate requested is around 110 kbit/s.

In our vision, one of the most acceptable case of bandwidth requirement is of 64 kbit/s for VoIP, if we adopt the G.726 codec with 10 ms long frames and employing a conference bridge on the FR chief, and about 400 kbit/s for VIP service, if we adopt a codec of 256 kbit/s and 70 bytes long packets. The overall bit-rate requested is around 550 kbit/s.

4.4.3 MEOC - EOC network

Since the MEOC acts as a local relay to the EOC, for the link between the MEOC and the EOC, we make the same assumptions made for the FR chief - MEOC link, and therefore, we have the same theoretical bandwidth requirements.

4.4.4 Performance boundaries

The *quality of experience* (QoE) perceived by any FR can be related to one or more of the following *network-oriented* (or QoS-oriented) metrics: per-packet delay, inter-packet jitter, packet-loss ratio and achievable bit-rate. Then, in order

[3]As for the FR chief - MEOC link we do not present the multicast case for a matter of brevity.

to correctly evaluate these QoS metrics, it has been necessary to find a proper mapping with the quality perceived by each user, as will be described below.

As for the VoIP service, Goode [26] provides a detailed overview of the main issues that can be found in its implementation. Being a delay-sensitive service, VoIP needs a carefully studied end-to-end delay-budget; to be more specific, a maximum end-to-end delay of about 150 ms is generally accepted, while a delay between 150 ms and 400 ms can be accepted for international VoIP calls; a delay of more than 400 ms has to be avoided during the service planning. Being related to the delay, also jitter needs to be bounded, to avoid the use of a large jitter buffer at the receiver. Finally, also packet loss contribute to the QoE degradation; in particular, the QoE degradation depends on the specific codec adopted for the VoIP service. Perkins et al. [28] show an appreciable *mean opinion score* (MOS) degradation for G.729 codec (from 4.0 to as low as 2.4) when packet loss reaches the 3% threshold. Hence, in what follows we consider the approximate 3% threshold for VoIP packet loss.

The delay budget for VIP is very similar to that described for VoIP. Therefore, those delay thresholds can be applied for VIP, too. The same applies to jitter as well, which needs to be kept as low as possible. As for packet-loss ratio, in [29] the authors consider the use of H.264/AVC codec in wireless environments, suggesting to consider 10^{-2} as the maximum packet-loss ratio value for conversational services, while 10^{-1} as the maximum packet-loss ratio value for streaming ones. Here, we consider 10^{-2} as the performance threshold value.

Because of the large number of sensors that can be implemented on a FRU, it is not possible to define in an objective way the performance thresholds for sensors service; therefore, we assume 0.5s as the maximum delay and 10^{-1} as the maximum packet-loss ratio.

Similarly, it is not easy to define objective thresholds for the data service; hence, we assume 100 kbit/s as the minimum throughput and 10^{-2} as the maximum packet-loss ratio.

Scenario	Metric	VoIP	VIP	Sensors	Data-transfer
	delay $[ms]$	3.30 ± 0.02	-	4.2 ± 0.1	-
FRs (indoor)	jitter $[ms]$	2.46 ± 0.02	-	4.0 ± 0.1	-
(IEEE 802.11g)	loss	$\simeq 0$	-	$\simeq 0$	-
	bit-rate $[kbit/s]$	$\simeq 64$	-	$\simeq 2.4$	-
	delay $[ms]$	2.55 ± 0.01	-	3.32 ± 0.08	-
FRs (outdoor)	jitter $[ms]$	1.71 ± 0.01	-	2.62 ± 0.07	-
(IEEE 802.11g)	loss	$(1.0 \pm 0.7) \cdot 10^{-5}$	-	$(5 \pm 3) \cdot 10^{-5}$	-
	bit-rate $[kbit/s]$	$\simeq 64$	-	$\simeq 2.4$	-
	delay $[ms]$	6.63 ± 0.02	6.63 ± 0.01	7.78 ± 0.03	123 ± 1
Chief–MEOC	jitter $[ms]$	1.25 ± 0.02	3.220 ± 0.008	2.73 ± 0.03	37.7 ± 0.2
(IEEE 802.16)	loss	$(3.8 \pm 0.1) \cdot 10^{-3}$	$(3.27 \pm 0.09) \cdot 10^{-3}$	$(41 \pm 1) \cdot 10^{-3}$	$(3 \pm 1) \cdot 10^{-3}$
	bit-rate $[kbit/s]$	$\simeq 64$	$\simeq 402$	$\simeq 2.3$	270 ± 20
MEOC–EOC	delay $[ms]$	$\simeq 240$	$\simeq 240$	$\simeq 240$	$\simeq 242$
(DVB–RCS)	loss	$\simeq 2 \cdot 10^{-3}$	$\simeq 2 \cdot 10^{-3}$	$\simeq 2 \cdot 10^{-3}$	$\simeq 2 \cdot 10^{-3}$
	bit-rate $[kbit/s]$	$\simeq 64$	$\simeq 403$	$\simeq 2.4$	$\simeq 480$

Table 4.1: Delay, jitter, packet-loss ratio and received bit-rate per network segment. © 2012 IEEE

4.5 Numerical Results

The goal of this Section is to present the numerical results, about the services described in the previous Sections, that we have obtained by means of the network simulator 3 (NS-3) [30], an open source, discrete-event simulator that is of widespread use in the scientific community. In particular, we focus on each network segment composing the whole emergency network, to ensure if the previous data budgets are actually sustainable. In what follows we consider only the so-called acceptable data-rate configurations; moreover, because of length constraints, we present only results obtained on each single link, leaving end-to-end outcomes to a future work.

Each simulation run has lasted 20 minutes of "simulated" time, during which we have sampled delay, jitter, packet-loss ratio and achievable bit-rate, at IP layer[4].

As for delay and jitter (which are per-packet metrics) we have computed the statistical mean over the whole set of received packets belonging to a given flow, during a single run. In any case, the size of the sample used to calculate delay and jitter has been always greater than 7000 packets.

As for packet-loss ratio and received bit rate (which are per-flow metrics) we have made at least 100 runs (in some cases we have increased the size of the sample to obtain more precise results).

In order to provide reliable results, for the most relevant metrics we have calculated also their 99% confidence interval by using the t-distribution (negligible uncertainties have been omitted).

The simulation results, that will be discussed in the following Subsections, are reported in Table 4.1, which summarizes all the metric mean values for the three network segments. Only the MEOC-EOC network lacks the confidence intervals on time measures, because of the approximate model we have adopted for the experiment (that will be described next).

[4]Since this work concerns with *application* QoS, we neglect other possible metrics, mostly related to lower layers of the protocol stack, such as power consumption of each device employed in the envisaged network.

4.5.1 FRs network

As for the FRs network, we have considered only static nodes deployed on a circle, centered with the chief with a fixed radius[5]. Moreover, the IEEE 802.11g physical layer has been configured to provide both enough data capacity for the network services and adequate transmission range; more specifically, we have adopted the ERP-OFDM physical layer at 6 Mbit/s.

We have considered two different wireless propagation environments, i.e., indoor and outdoor, with both path-loss and small-scale fading. More specifically, the path-loss can be expressed in dB as:

$$L = L_0 + 10n \log\left(\frac{d}{d_0}\right) \tag{4.1}$$

where L_0 is the loss, in dB, at the reference distance d_0, n is the path-loss exponent (e.g., $n = 2$ represents the classical Friis free space propagation model) and d is the actual distance.

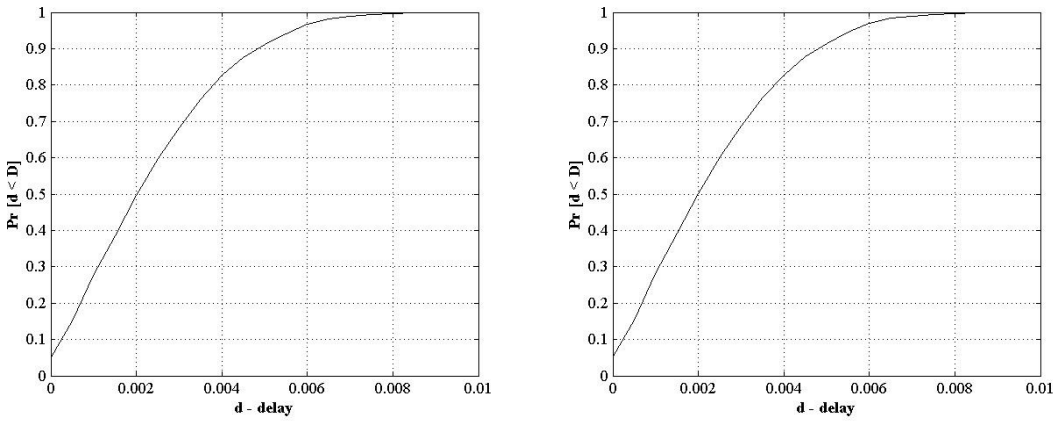
As for the indoor propagation environment, we have modeled a non line-of-sight (NLOS) wireless channel with a path-loss exponent $n = 3$ and Nakagami-m fading with $m = 1$ [31]. Regarding the outdoor propagation environment, we have considered the model proposed in [32], which is a line-of-sight (LOS) path-loss model that considers also the terrain diffraction effects, by taking into account the heights of both the transmitter and the receiver antenna.

Before the actual simulations, we have performed several preliminary runs to identify reasonable separation distances between any FR and his/her respective FR chief; as results of these runs, we have considered $d_{indoor} = 25$m and $d_{outdoor} = 300$m, respectively for the indoor and the outdoor case. In each case we have adopted a transmission power of 20 dBm (100 mW).

The network services considered for the FRs network are full-duplex VoIP (with a conference bridge and a centralized media mixing bridge, co-located at the FR chief) together with unidirectional sensors (toward the chief).

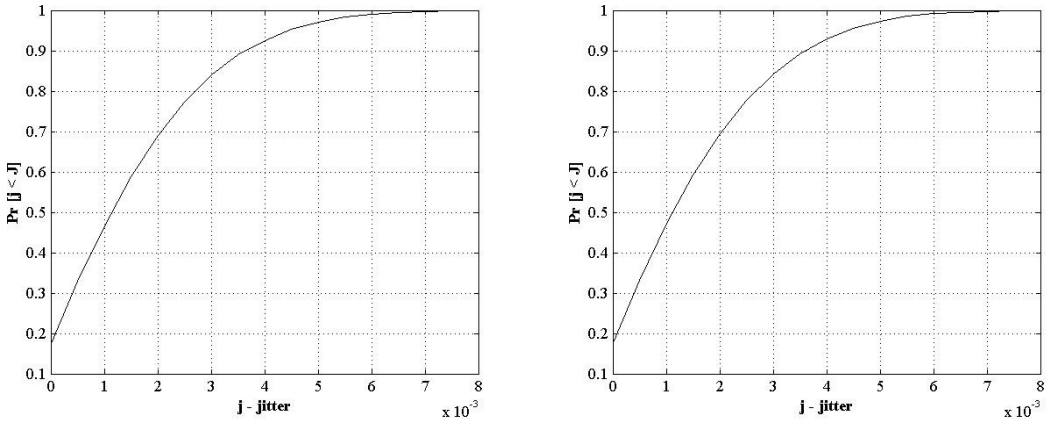
Considering Table I, by comparing the indoor case with the outdoor one, it is evident that the results are quite similar. There are minor differences between

[5]Even if this assumption is not realistic, it is used to guarantee that all FRs evenly experience the same average channel conditions.



(a) Indoor case. (b) Outdoor case.

Figure 4.3: VoIP - per-packet delay CDF.



(a) Indoor case. (b) Outdoor case.

Figure 4.4: VoIP - inter-packet jitter CDF.

the delay and jitter values, from one case to the other, with slightly higher values for the indoor case.

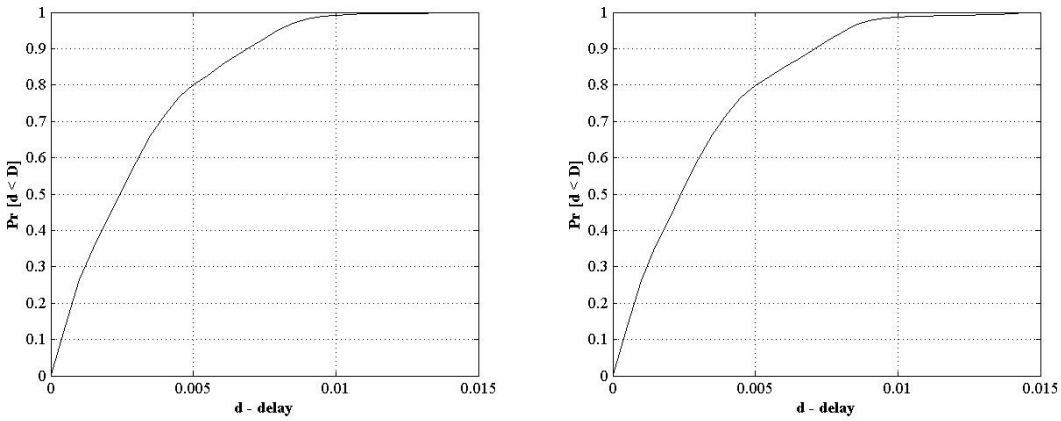
As VoIP is one of the most important delay-sensitive services that has to be supported, delay performance has to be carefully analyzed. More in details, to provide a deeper understanding of its achievable performance, we have computed the cumulative distribution function (CDF) of the delay, for both the indoor and the outdoor case; the two CDFs are depicted in Figure 4.3. As can be seen, there is a very high probability that the delay is lower than 10 ms, which clearly shows the entity of the maximum delay that can be experienced by the VoIP service in the FRs network. Considering Figure 4.4, where the jitter CDF is depicted for VoIP service, it is possible to appreciate a very low maximum jitter value (about 8 ms for both indoor and outdoor cases), while a slightly greater value can be appreciated from Figure 4.5 for sensor service.

4.5.2 FR Chief - MEOC network

The FR chief-MEOC link has been implemented with the IEEE 802.16-WiMAX module included in NS-3 (see [33] for further details). We have used a transmission power of 30 dBm (1 W) and a path-loss exponent $n = 3$. Here we have considered a separation distance between the FR chief and the MEOC of 8 km.

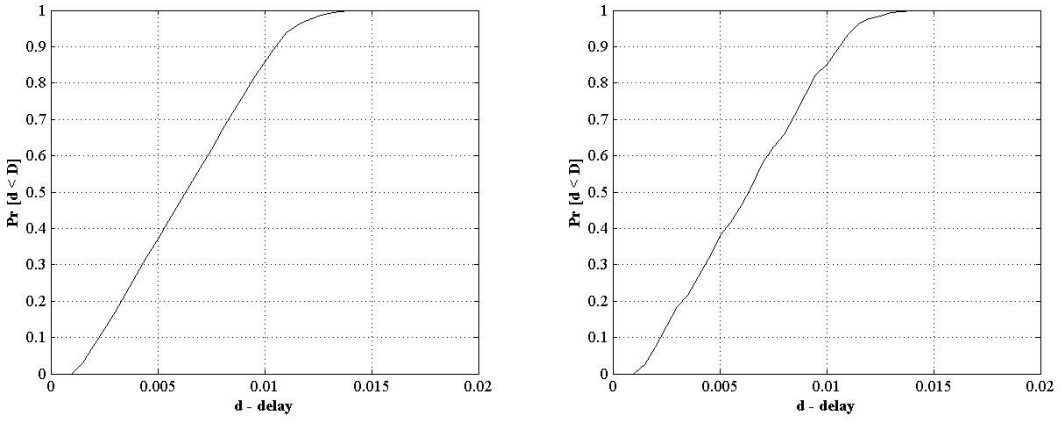
The network services considered for the chief-MEOC link are full-duplex VoIP (between the chief and the MEOC) together with unidirectional VIP (from the chief to the MEOC), unidirectional sensors (i.e., $N_{FR} + N_{FRC}$ sensor flows toward the MEOC) and a bulk data transfer (from the MEOC to the chief). To provide QoS differentiation, we have classified these services according to different IEEE 802.16 service classes; more specifically, we have assigned VoIP, VIP and sensors to the *unsolicited-grant service* (UGS) class, while the data-transfer service has been assigned to the *non real-time polling service* (nrtPS) class. However, please note that other different classifications are possible, too.

Considering again Table I, as for the VoIP service, it is possible to state that, even at the remarkable distance of 8 km, its performance metrics are always within the quality boundaries described previously. This is also true for the VIP service and for the sensors service; note that the uplink H.264 flow can be effectively



(a) Indoor case. (b) Outdoor case.

Figure 4.5: Sensors - per-packet delay CDF.



(a) VoIP service. (b) VIP service.

Figure 4.6: Per-packet delay CDF.

supported, together with all other services, even if its IP bit-rate is of about 400 kbit/s.

Again, to provide a better understanding of the performance experienced by the packets transmitted through the FR chief to MEOC link, consider Figures from 4.6 to 4.8.

Figure 4.6, which depicts per-packet delay CDFs for real-time services, clearly shows that there is a very high probability (more than 95%) that the packet delay is less than 13 ms.

Considering Figure 4.7, which reports the inter-packet jitter CDFs regarding VoIP and VIP, it is possible to appreaciate a very tight upper bound for delay variations (up to 12 ms).

As for packet loss, Figure 4.8 reports its CDF for each service deployed. Regarding real-time services (VoIP and VIP) the loss probability is bounded at about $5 \cdot 10^{-3}$, which is acceptable for the considered link.

Considering the data-transfer service, from Table 4.1 it is possible to see that its mean delay and its mean jitter are considerably higher than those measured for the other services, which is related to the QoS classification adopted. Nevertheless, its average throughput, approximately equal to 270 kbit/s, is sufficiently high for the service requirements.

4.5.3 MEOC - EOC network

Here, we have modeled the MEOC-EOC network by means of asymmetric point-to-point links with realistic values for capacity, delay and packet-loss ratio. We have considered a geostationary earth orbit (GEO) satellite link (one-way delay of about 120 ms), with a 5 Mbit/s in the uplink and 20 Mbit/s in the downlink, while the packet-loss ratio has been set equal to 10^{-3} for both. Finally, we have taken into account the so-called mesh mode configuration, where the satellite can directly interconnect each pair of ground stations without the need of a terrestrial hub. Thus, the overall one-way delay measured between two ground stations is about 240 ms.

The network services for this network segment are the same of the chief-MEOC link (see the previous Subsection).

Considering again Table I, the received bit-rate values are quite similar for VoIP, VIP and sensor services, while the data-transfer service experienced a substantial improvement (from approximately 270 kbit/s to about 480 kbit/s), mainly due to the higher capacity offered by the satellite link, as can be seen in Figure 4.9, where the CDF regarding the data service throuhgput is depicted. Finally, the end-to-end, one-way delay is always about 240 ms, as expected.

4.5.4 Final Remarks

By analyzing the obtained numerical results, we can assert that every considered network technology provides enough bandwidth for the set of services specific to a given network segment. Moreover, the end-to-end delay budget for both VoIP and VIP is always satisfied, even if the satellite link introduces a huge delay bottleneck.

As for the loss budget, the packet-loss ratio of each network segment is always below the required threshold (typically lower than $4 \cdot 10^{-3}$, except for the sensor service on the IEEE 802.16 link). If we consider the end-to-end (i.e., from each FR to the EOC) packet-loss budget, we can find that it is always bounded by about $5 \cdot 10^{-2}$, which is adequate for any of the services taken into account.

Finally, as for the MEOC-EOC network, it is possible to determine the minimum bandwidth requirement for the EOC satellite link. In particular, considering only VoIP, VIP and sensors, the overall minimum bandwidth required in the downlink to support a single FRs team is:

$$C_{down} = C_{VoIP} + C_{VIP} + (N_{FR} + N_{FRC})\, C_{sensors} \tag{4.2}$$

while the overall bandwidth required in the uplink is given by:

$$C_{up} = C_{VoIP} \tag{4.3}$$

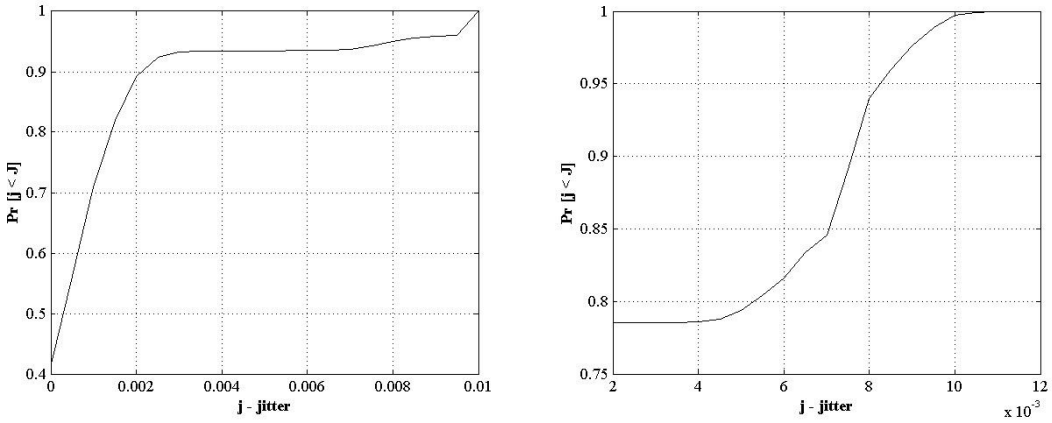
Hence, the required downlink capacity is about $C_{down} \simeq 500$ kbit/s, while the uplink capacity is $C_{up} = 64$ kbit/s, for each FRs group.

In order to consider also the impact of the data-transfer service, these minimum requirements need to be increased accordingly. However, by comparing these requirements with the capacity provided nowadays by satellite service providers,

it is already clear that satellite communications can be used effectively to provide connectivity to public safety systems.

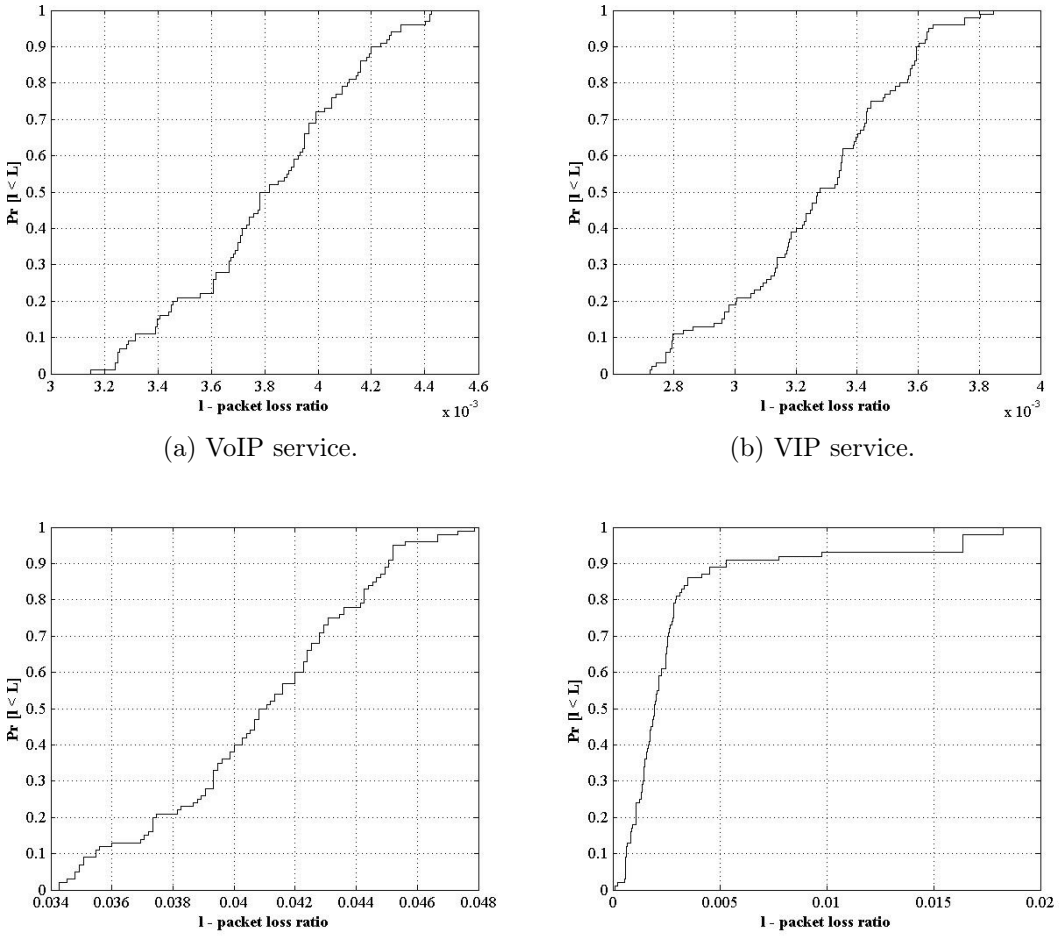
4.6 Summary

In this Chapter, the analysis of the communication services for an emergency network has been described. More in detail, we have determined the theoretical bandwidth requirements considering a particular network configuration. Then, we have evaluated the performance of the considered services by means of NS-3. The obtained results showed that the considered network architecture, together with the technologies employed for its implementation, can provide satisfactory QoS for the required services.



(a) VoIP service. (b) VIP service.

Figure 4.7: Inter-packet jitter CDF.



(a) VoIP service.

(b) VIP service.

(c) Sensors service.

(d) Data transfer service.

Figure 4.8: Packet-loss CDF.

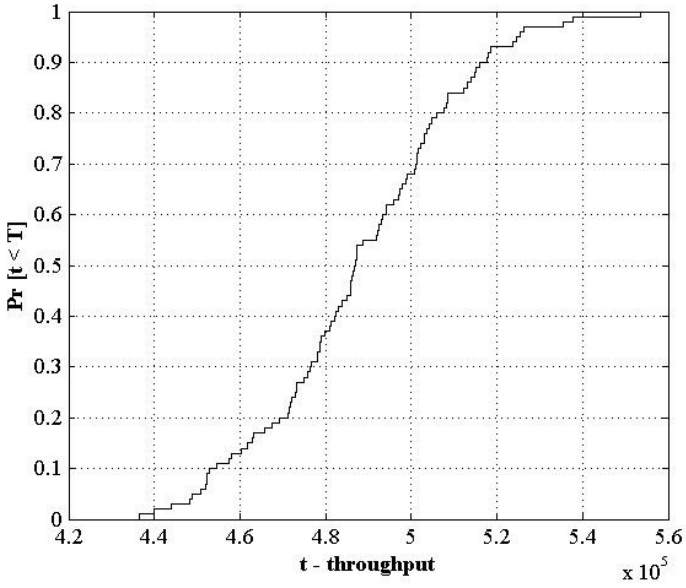


Figure 4.9: Throughput CDF - data service.

Chapter 5

QoE Monitor: a New Tool for QoE Assessments[1]

5.1 Introduction

In the previous Chapter, a detailed QoS analysis of the E-SPONDER network has been described, showing that the proposed architecture can be effectively used to support the network services required for public safety operations. However, although QoS assessments (i.e., network-oriented measurements and/or simulations) are of paramount importance during the design of a networking system (because they are relatively quick to implement) the designer should not forget the ultimate goal of the final implementation: provide the user with a service whose quality corresponds to his/her expectation. This is typically referred to as providing a sufficiently high *quality of experience* (QoE).

At a glance, QoE corresponds to the quality perceived by an end user of the considered system, and typically it is not expressed in technical terms (e.g., delay, jitter, in case of network assessments) but, instead, in terms of a satisfaction grade, e.g., "bad", "fair", "good", "excellent". QoE can be assessed in almost every system (and not just in communication networks) and requires the investigator to directly access what users perceive as system output.

[1]Reprinted from Simulation Modelling Practice and Theory, Volume 32, March 2013, pp. 30-41, D. Saladino, A. Paganelli and M. Casoni, "A Tool for Multimedia Quality Assessment in NS3: QoE Monitor", Copyright 2013, with permission from Elsevier.

With this motivation in mind, our research activity within the E-SPONDER project has moved toward the analysis of the quality of experience a user perceives when using the system. To provide such an analysis, the first step has been to find a suitable assessment tool. Several possible candidates have been found (see Section 5.2 and the references therein) but none of them was available for the NS-3 [30] platform we adopted for our previous analysis. This motivated us to design and develop a new software tool for NS-3 usable to perform QoE assessments in any arbitrary network: *QoE Monitor*.

The current stable version of our software (which is an open-source software released under GPL v.2 license, and can be freely downloaded from [34]) is very general and is by no means dedicated to E-SPONDER's network, only. Currently, it focuses mainly on the QoE evaluation of a video stream transmitted through a given network, by performing the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity (SSIM) metrics, which are both objective (i.e., they are implemented by means of algorithms and do not rely on human evaluations) and full-reference (i.e., they require both the transmitted video file and the received one to predict the perceived quality). During the design of *QoE Monitor*, we have taken into account an existing tool, called EvalVid [35], as an effective starting point and reference: we have carefully analyzed it and completely re-implemented its main features and modules, in order to have a software module that can be directly integrated with the NS-3 simulator.

Since this project is quite young, some advanced and specific features (e.g., application level FEC, reduced and no-reference quality assessments, *universal image quality index*), as well as those related to audio assessments, are still under development and will be part of future works. However, the present version of *QoE Monitor* is already usable and can provide helpful insights to the research community for the evaluation of video streaming services in any network implementable with NS-3.

The rest of this Chapter is organized as follows. Firstly, in Section 2 we describe the state-of-the-art of the currently available tools for the assessment of the video quality experienced by a viewer. Section 3 gives a short description of our reference framework and, then, describes in detail the proposed *QoE Monitor* architecture, together with its integration with NS-3; an overview of the main

C++ classes composing the tool is provided, too. Section 4 presents the analyzed network scenarios and discusses the obtained simulative results, that demonstrate the validity of our tool, whereas Section 5 describes the first validation results we have obtained comparing our tool with EvalVid. Then, in Section 6 we suggest possible future works that could make this tool more efficient and usable in different contexts. Finally, Section 7 reports our main conclusions and highlights our final remarks.

5.2 Related Works

As previously stated, the reference tool we have considered to steer our development is EvalVid, a modular tool-set, written in C, that allows to assess the perceived quality of a video stream transmitted through a network, which could be both realistically reproduced and/or experimentally simulated. The goal of this tool is not only to evaluate network parameters like jitter, loss and delay, which are typically referred to as quality-of-service (QoS) parameters, but also to assess the video quality really achieved through the computation of frame-by-frame PSNR. Moreover, it gives the possibility to change some configuration parameters like the video coding scheme or the adopted error model as well as the network parameters or the error correction strategy employed for the video reconstruction at the receiver side.

In [36], the authors describe a method to integrate EvalVid with the widespread Network Simulator 2 (NS-2) [37], to carry out realistic video QoE evaluations in arbitrarily simulated networks.

In [38], the "Research Group on Computer and Networks and Multimedia Communications - UFPA" implemented a successful port of the code-base of the original EvalVid project, to the NS-3 framework, to replicate the same functionalities provided to the NS-2 platform by [36]. However, it is important to underline that this tool makes use of trace-based evaluations (similarly to what EvalVid does), which means that only offline assessments are possible.

Furthermore, a widespread tool for video quality evaluation is MSU VQMT (Video Quality Management Tool) [39]. This tool supports different input formats, like AVI, YUV, MP4, WMV, VOB, and makes available different metrics to com-

pare up to three video files, like PSNR, SSIM and Video Quality Measurement (VQM), and metrics for blurring and blocking measurement, too. It provides both full-reference (which requires both the sent and the received videos) and no-reference (which requires only the received video) comparisons.

A very promising tool that brings together a network simulator and a proper multimedia evaluation module is Open Evaluation Framework for Multimedia Over Networks (OEFMON) [40]. Some of the most important features of this tool, which is based on QualNet (a commercial network simulator originally derived from GloMoSim [41]), are: modularity, which allows the system to be extended with novel codecs and/or network standards; real-time operation, which allows the simulation of realistic multimedia communications (e.g., real-time adaptation of coding parameters, usage of scalable video coding, etc.); real-time monitoring, i.e., the multimedia content at the output of the network setup can be monitored in real-time, thus allowing direct subjective quality assessment by the researcher.

Finally, another couple of proprietary and commercial tools is also available, i.e., Q-Master Video System [42] and Video Quality Analyzer [43]. The former measures the perceptual quality of both audio and video streaming, providing information about jerkiness, blurring, noise, besides the traditional Mean Opinion Score (MOS) values. The Video Quality Analyzer tool allows to analyze the perceived video degradation by employing an evaluation model very similar to the Human Visual System.

5.3 QoE Monitor: Architecture and Design

As already previously stated, our purpose is the evaluation of the video quality experienced by a viewer, by adopting objective metrics based on the detection of the differences (or variations) between the original (reference) video and the received and/or coded one. Consequently, our work consisted in designing and implementing a complete framework, whose principle of operation is reported in Figure 5.1, consisting of a new NS-3 module, written in C++, that reproduces the main components and the functions of the existing EvalVid tool[2].

[2]Please note that *QoE Monitor* is not based on EvalVid or part of its source code: it has been designed from scratch, to provide to the NS-3 framework the same capabilities provided

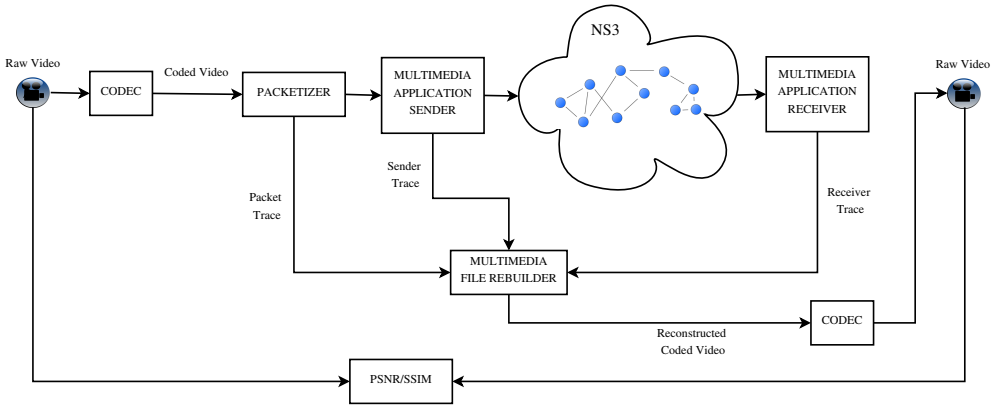


Figure 5.1: The proposed evaluation framework.

First of all, since one of the main goals we have considered at the very beginning of this project was to provide a freely available tool for both research and industrial applications, we have adopted an open-source design approach. Among the others, a great benefit of this approach is that it guarantees that any user can freely verify its code base, then promoting a solid software development and evolution. Moreover, our design is based on well-known and well-tested open-source software, namely, Ffmpeg [44], Avconv [45] and their core libraries (libavcodec, libavformat, etc), for what concerns with the multimedia data manipulation.

By referring to Figure 5.1, here we provide a brief sketch of the working principle behind *QoE Monitor*. Since our final goal is to predict how the video frames, transmitted through a simulated network, are perceived by a viewer, a reference raw (i.e., uncompressed) video is coded using a particular codec (with the adoption of Ffmpeg).

Then, the coded video file is packetized by the *Packetizer* component that, in addition to the packets, produces a packet trace containing some information like the packet ID, its size and its timestamps. The produced packets are transmitted through a network, simulated with NS-3, by the *MultimediaApplicationSender* component. Its task is to create the Real-time Transmission Protocol (RTP) [17] packets, to transmit them within an UDP datagram flow and to produce a sender trace, which contains the packet ID and its timestamp.

At the receiver side, the packets are received by the *MultimediaApplication-*

by EvalVid to the NS-2 one.

Receiver component, that extracts the header information of each packet and reproduces the receiver trace, containing packet ID and timestamp.

Packet trace, sender trace and receiver trace are used by the *MultimediaFileRebuilder* component to reconstruct the video, reporting a possibly corrupted video file. The quality of the reconstructed video depends on how many packets have been received and, therefore, on network parameters like packet delay, jitter and error rate, that affect the QoS.

At this point, the reconstructed video is decoded, in order to obtain another raw video file to be displayed and played out at the receiver side. Now, the received video can be compared to the reference one employing PSNR and SSIM metrics (that will be described next), in order to provide a prediction of the perceived video quality and thus to determine the effects of the video transmission over the simulated network.

Finally, our tool allows to perform a lot of kinds of comparison, e.g., the transmission effects only, the adopted codec effects only, or both, as presented in Figure 5.1 and carried out in our numerical results, that will be presented afterwards in Section 4.

5.3.1 NS-3 QoE Monitor Classes Design

In this subsection, an overview of the main classes composing the proposed NS-3 *QoE Monitor* is presented, with the help of an Unified Modeling Language (UML) class diagram reporting the classes developed so far and the associations and relationships among them (Figure 5.2). For each class the most important methods have been reported only, omitting their complete signature (i.e., the complete formal parameter set); moreover, simple getter and setter methods, as well as class' attributes, have been neglected to provide a clearer view of the overall design of the proposed tool.

One of the most important classes is *SimulationDataset*, which includes all the state variables required to perform the QoE evaluation process. At a glance, it stores all the multimedia file names required for the evaluation, together with all the traces generated by the events related to the actual transmission, as described before. Moreover, it provides the user with a set of getter and setter methods

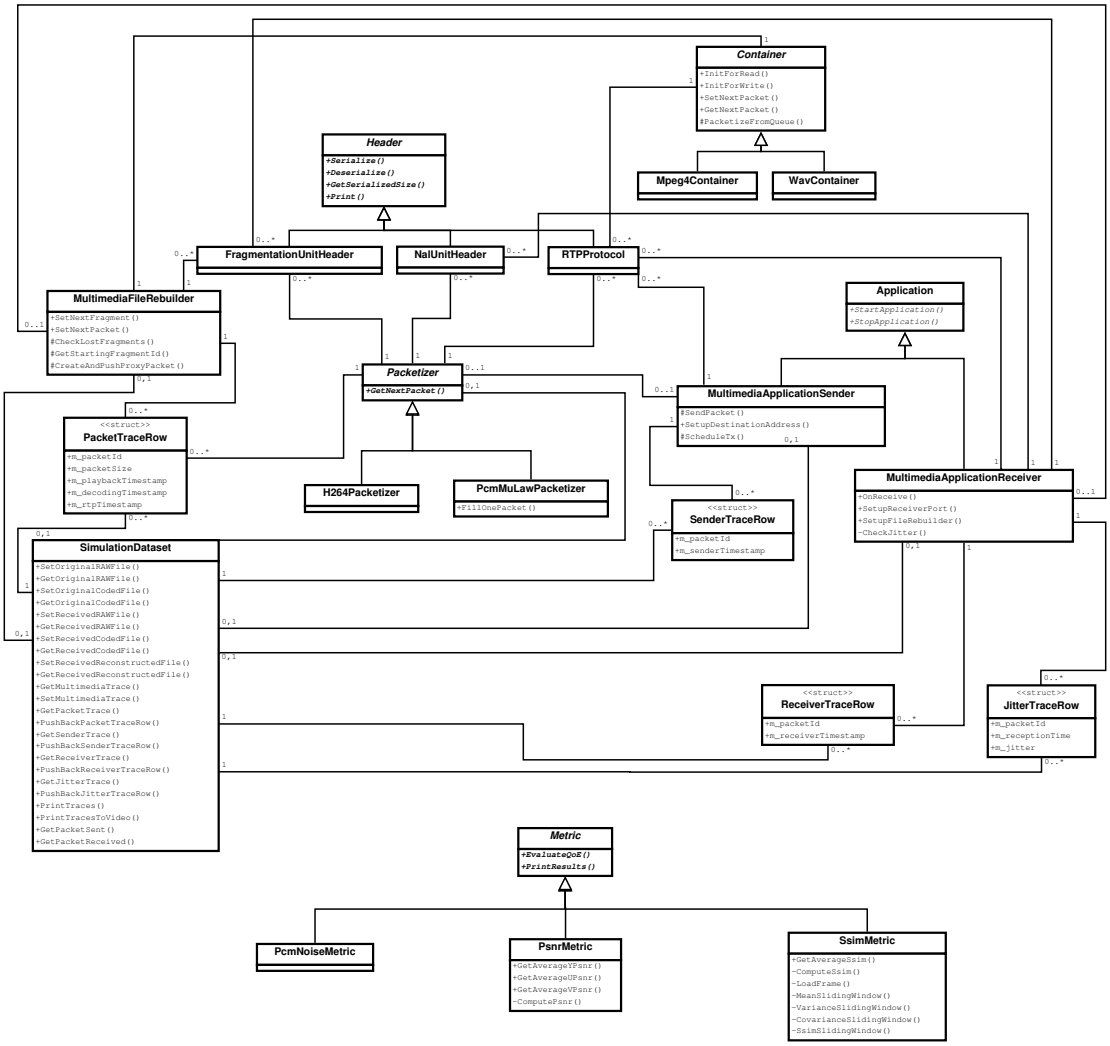


Figure 5.2: *QoE Monitor* simplified class diagram.

that simplify the simulation setup.

Since the proposed *QoE Monitor* module works with multimedia content, there are several classes designed to manipulate video and audio files. More specifically, the pure virtual *Container* class and all the classes derived from it (e.g., *Mpeg4Container* and *WavContainer*) are responsible for working with the specific chosen file container (e.g., Mpeg4, Wave). For instance, these classes provide the caller with capabilities such as writing a coded frame to the output container (with SetNextPacket()) or reading a coded frame from the input one (with GetNextPacket()).

The actual multimedia content transmission over a generic simulated network is performed by the *MultimediaApplicationSender* class, which has been derived from the *Application* class provided by the NS-3 framework. In order to have a generic sender, exploitable with any possible codec, we have created a pure virtual class named *Packetizer*, which hides the actual packetization process to the application. By deriving specific packetizers (e.g., *H264Packetizer*, *PcmMuLawPacketizer*), it is possible to implement different packetization rules, according to the considered multimedia content.

Since our goal has been to support RTP-based multimedia communications, in the proposed NS-3 module we have implemented the most basic RTP features through the *RTPProtocol* class. With this class we have simply provided a packet header that conveys packet ID and timestamp information to the receiver[3], as discussed before.

Since one among the first codecs we have considered in our design is H.264, we have implemented the *Network Abstraction Layer* (NAL) packet header, too, with the *NALUnitHeader* class, according to [46]. Moreover, because NALs could be larger than the network's MTU, we have created an additional class, which is exploitable to report to the receiver that the current packet is actually a single *fragment* of a longer packet, according to [46]: *FragmentationUnitHeader*.

The most useful information about each packet produced by a packetizer is stored in a proper packet trace provided by the *SimulationDataset* class. In more details, for each filled packet a *PacketTraceRow* structure is created and filled with the packet ID, its size, its playback timestamp, its decoding timestamp and

[3]Further capabilities (e.g., RTCP and the like) have not been implemented yet.

its RTP timestamp; finally, the filled row is pushed to the packet trace structure.

Once the application has obtained a complete RTP packet from the packetizer, it transmits it through the network. The information related to each sent packet (i.e., packet ID and sending time) composes a *SenderTraceRow* structure, that is pushed to the sender trace structure located within *SimulationDataset*.

The receiver is implemented by the *MultimediaApplicationReceiver* class. Upon each packet reception, it performs a jitter estimation and check the current packet, according to RFC 3550 [17], to assess whether it is arrived on time or not. For each successfully received packet, jitter information is saved in a *JitterTraceRow* structure containing the corresponding packet ID, the reception time and the current estimated jitter value. Then, the *JitterTraceRow* structure is pushed in the proper jitter trace stored within *SimulationDataset*.

Finally, the receiver passes each correctly received packet to a *MultimediaFileRebuilder*, which rebuilds the transmitted file. Please note that the rebuilt file could be possibly corrupted, if compared to the transmitted one, because of possible packet losses due to the transmission and the coding process. Since our QoE evaluation process makes use of both the received and the transmitted file (e.g., to compute the difference between the transmitted and the received frame of a given video file), it has been necessary to *align* the received file to the transmitted one, because the received data can be significantly *less* than that composing the file at the sender side (e.g., in case of high packet loss rate). To accomplish this, for each lost packet we have chosen to embed the corresponding amount of dummy data to the output file. With this approach, possible future additional modules could make use of transmission-related information (e.g., the ID of each lost packet) to implement application-level error-correction techniques.

5.3.2 Currently Available Metrics

Regarding the video quality evaluation metrics, we have considered PSNR [47] and SSIM [48], that are the most widespread QoE video objective metrics found in the scientific literature. These metrics are both full reference as they require the complete availability of the two video files to be compared.

The class *PsnrMetric*, as the name suggests, has the purpose to compute the

PSNR value between a reference video and a received, and then reconstructed, one. Its values can vary from 0 to infinite (in this work we have considered 99 as the maximum value): bigger values correspond to better quality.

Given each frame of both video files, this component compares them by simply computing the signal-to-noise ratio in order to extract the differences between the two images [47]. This implies that PSNR index analyzes all the image regions in the same way, without taking into account that each one has different visual importance. Indeed, in the Human Visual System (HVS), not all of the image areas receive the same perceptual attention. Generally, in a given scene, the human eye is more attracted by the presence of distinct objects and the core areas than the background ones, as they have perceptually more information and, therefore, more importance. We can conclude that PSNR simply detects the errors between two images (equally analyzing the overall pixels), without approximating all the real human perception features: to a low PSNR value may subjectively correspond a high quality image.

The class *SsimMetric* has been implemented to compute the SSIM metric [48] to overcome to the PSNR drawbacks described before.

SSIM quality measure [48] takes into consideration the HVS characteristics to extract the structural information of an image (because spatially close pixels are tightly correlated and have strong inter-dependencies) and, in particular, to be sensitive to its variation, reproducing this feature in order to better predict the video quality as perceived by the human eyes. It gives values from 0 to 1: bigger values represent better quality, with values from 0.9 upwards representing a difference almost impossible for the human eye to detect.

The QoE evaluation through the SSIM index is characterized by a greater computational complexity than PSNR, because it is necessary the employment of a sliding window of $N \times N$ size (typically $N = 8$), which is shifted pixel by pixel from top-left corner to the bottom-right one of each single frame. Therefore, taken each frame of both video files, for each $N \times N$ block, we compute the mean value and the variance, and then the covariance between the two current blocks (see [48] for a more accurate discussion about the mathematical details of SSIM); then, the structural similarity index is computed.

In the end, with SSIM index we are able to quantify the loss of image struc-

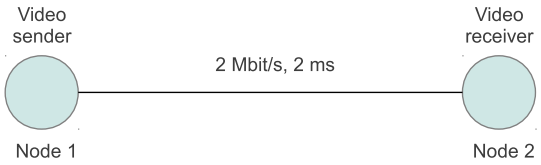


Figure 5.3: Network configuration related to Scenario 1.

tural information, that can provide a good approximation of the perceived image distortion.

5.4 Reference Scenarios and Numerical Results

In this Section, two reference network scenarios are described to provide a detailed overview of how our proposed tool works. Our goal is not to simulate simple or complex network topologies, but to exploit simulated networks to transmit a video file and, then, to evaluate the perceived quality at the receiver side (by comparing the transmitted video to the received one). Consequently, in order to emphasize the capabilities of *QoE Monitor*, we have considered both a simple network topology and a more complex one, to provide a clear view of the tool. Moreover, the simulated network topologies produce more repeatable simulation outcomes with respect to more complex scenarios and have provided us with a controlled framework that has considerably simplified debug procedures, avoiding, then, unpredictable results.

Furthermore, numerical results showing the capabilities of the current release, are provided and discussed, too. Finally, for each scenario, the simulation setup consists of NS-3.13, Ffmpeg 0.8.2 and libx264 [49] 0.120.2164.

5.4.1 Scenario 1: Video Streaming Over a Lossy Link

The first scenario (which is available together with the source code as `qoe-monitor-example-1.cc`) is composed by a simple network of two nodes connected by means of a point-to-point link at 2Mbit/s, with a delay of 2ms, as depicted in Figure 5.3.

The goal of this setup is to show, firstly in a simple topology, the objective QoE

evaluation, in terms of PSNR and SSIM metrics, of an H.264-encoded video stream through a lossy link. In our setup, we have chosen the "highway" CIF reference video [50], encoded with H.264. Please note that, at the time of writing, only video files with monotonically increasing PTS and DTS can be used with *QoE Monitor*. For instance, if the codec library is libx264, the conversion parameters that can be used are `preset=ultrafast`, `profile=baseline` and `tune=zerolatency` and the corresponding Ffmpeg command is:

```
ffmpeg -i <input-file> -vcodec libx264 -preset ultrafast
-profile baseline -tune zerolatency <output-file.mp4>
```

The packet-error-rate (PER) of the link can be varied at wish, depending on the chosen video file and on the simulation duration. More specifically, because the video file we have chosen is made up of 2000 frames and the total number of IP packets composing the data flow is approximately equal to 11400, the PER value should not be less than 10^{-3}, in order to provide meaningful statistical results. For this reason, in our evaluations we considered two PER values, namely $PER_1 = 10^{-3}$ and $PER_2 = 10^{-2}$.

The main simulation outcomes are presented in Figure 5.4, case (a) for PER_1 and case (b) for PER_2, respectively. As can be seen, the PSNR and SSIM profiles are different for the two cases, which clearly shows that the first one has experienced far better QoE with respect to the second. Moreover, please note that we have arbitrarily chosen the maximum PSNR value equal to 99, which means that the two compared frames are exactly the same (this value can be easily modified at wish, depending on the evaluation that has to be performed).

In more detail, considering again Figure 5.4 and taking as an example the 1000-th frame, it is possible to perceptually notice that, for the case where the error rate is lower (i.e., PER_1), the frame quality is high (almost the same of the transmitted one, with no noticeable artifact introduced), whereas, for the case where the error rate is higher (i.e., PER_2), the image degradation evidently grows, even if distortions remain acceptable yet.

Finally, please note that even if the PSNR graph is different from the SSIM one, both trends are quite similar, which clearly shows the positive correlation of the two considered metrics.

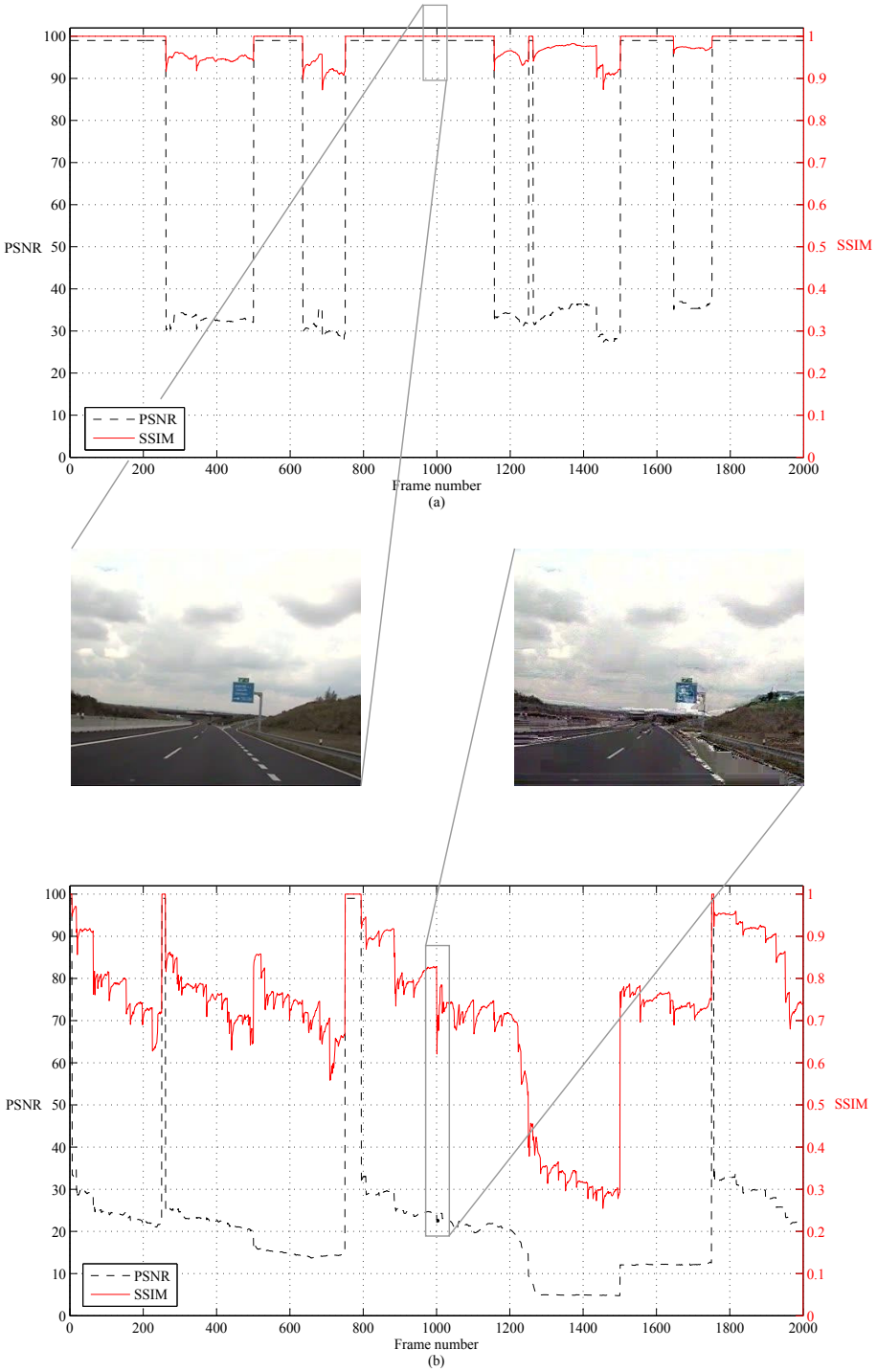


Figure 5.4: PSNR and SSIM - Scenario 1 for (a) $PER = 0.001$ and (b) $PER = 0.01$.

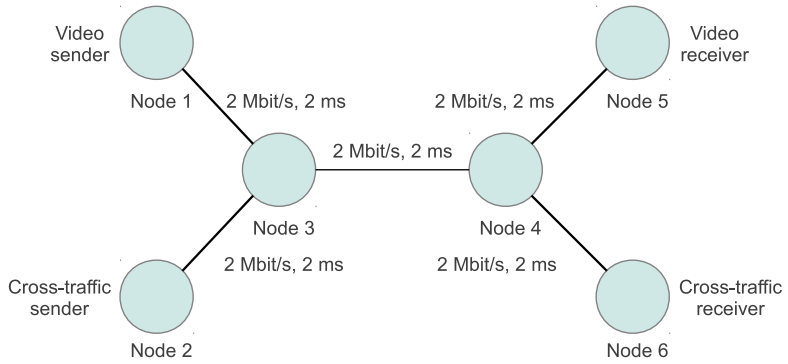


Figure 5.5: Network configuration related to Scenario 2.

5.4.2 Scenario 2: Video Streaming in Presence of Cross Traffic

The second scenario (available as `qoe-monitor-example-2.cc`) is composed by a more complex network, with respect to the previous one. In particular, a butterfly topology consisting of 5 nodes has been implemented, as reported in Figure 5.5. Each link is a point-to-point link at 2 Mbit/s, with 2 ms delay.

The goal of this scenario is to show how the proposed tool can be used to keep track of the QoE variation of a given video transmission, in case of heavy cross traffic.

Node 0 and Node 4 are the video sender and the video receiver, respectively, while Node 1 and Node 5 can be used to inject cross-traffic in the network. Again, we have considered the "highway" CIF reference video we adopted in the previous scenario, also for this case, which translates into a data flow of about 1.5 Mbit/s (measured at IP layer).

Here we consider only UDP-based cross traffic for a matter of brevity, but TCP-based flows are possible, too. More precisely, the cross traffic application we implemented injects an UDP stream of approximately 600 kbit/s, composed by 500 bytes long packets, with 0.0066 seconds inter-packet time interval, which saturates the bottleneck link between Node 3 and Node 4. In order to show the effect of the cross traffic application, its run is limited to the time interval $[10 - 40]$ seconds.

The main simulation results are presented in Figure 5.6, where it is possible

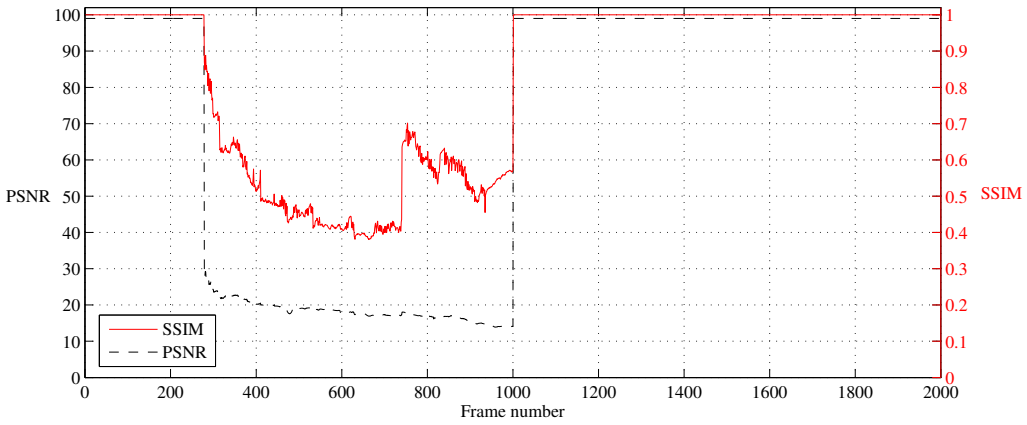


Figure 5.6: PSNR and SSIM - Scenario 2 with UDP cross-traffic.

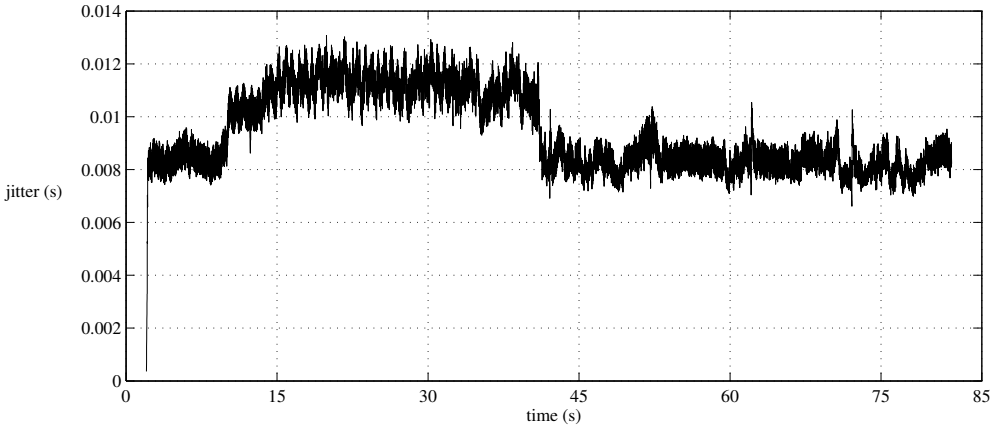


Figure 5.7: Jitter with UDP cross-traffic.

to see the effect of the UDP cross traffic source on the QoE perceived by the user. As can be seen, the presence of huge cross traffic abruptly increases the packet loss rate, which is correlated to a sudden QoE drop.

Moreover, considering Figure 5.7, where the jitter trace is plotted, it is immediately clear how the cross traffic source negatively affects the video reception, as expected, by introducing more jitter than that measured in the absence of congestion.

5.4.3 Discussion and Comments

As presented in the previous two subsections, *QoE Monitor* is a flexible tool, exploitable to perform diverse QoE evaluation over different networks. The numerical results, obtained by simulating the simple considered scenarios, have proved the validity of our proposed module to correctly predict the quality perceived by a human viewer, making it an useful tool to help the design of efficient video communication networks.

Even though we considered simple use cases to clearly present its main capabilities, more complex scenarios can be envisaged as well: networks with multiple video flows are possible, as well as those where a mixture of video and audio services are deployed.

Moreover, *QoE Monitor* can be effectively employed to perform service performance evaluations over the entire collection of technological models provided by the NS-3 framework, e.g., LTE, IEEE 802.16, IEEE 802.11, just to name a few, which make it a promising tool for both academia and industrial perspectives.

5.5 Validation Tests

In order to verify the effectiveness of *QoE Monitor*, a fundamental step consists in its validation against one or more reference tools for objective QoE evaluations. Since this process requires several tests to be performed to guarantee a full validation (e.g., different content and different network configurations), here we report some of the very first results we obtained so far.

Since both EvalVid and *QoE Monitor* use external tools to perform media conversions (e.g., Ffmpeg/Libav), we have set up a single evaluation platform for the whole validation process, which comprises the same tools and the same libraries for both; this way it has been possible to underline only the different behavior of the proper functions and capabilities of each of them. In particular, here we have employed NS-3.13, NS-2.35, EvalVid 2.7, Libav/Avconv 0.8.3-0ubuntu0.12.04.1 and Gpac 0.4.5+svn3462.

Since our focus has not been on the network itself, but on its effect on the video transmission, we have considered the same simple topology of scenario 1:

two nodes are connected by means of a point-to-point link with $PER = 10^{-2}$.

Our first goal has been to compare the implementation of the objective metrics we have developed for *QoE Monitor*, with respect to EvalVid. By means of NS-2, we have simulated the given topology (scenario 1), where the "highway" reference video has been transmitted. Then, the received (and possibly corrupted) video has been used to compare the evaluation performed by EvalVid metrics with those implemented for *QoE Monitor*.

The plots showing the different implementation of the video metrics, between EvalVid and *QoE Monitor*, are presented, in Figure 5.8, for the PSNR, and in Figure 5.9, for the SSIM. In particular, Figure 5.8a and Figure 5.9a respectively show the PSNR and the SSIM values for each video frame. Since both curves in these figures are almost overlapped, in order to provide a more meaningful information, Figure 5.8b and Figure 5.9b report the normalized relative error ε, which represents the discrepancy between reference values (i.e., EvalVid values) and their approximations (i.e., *QoE Monitor* values):

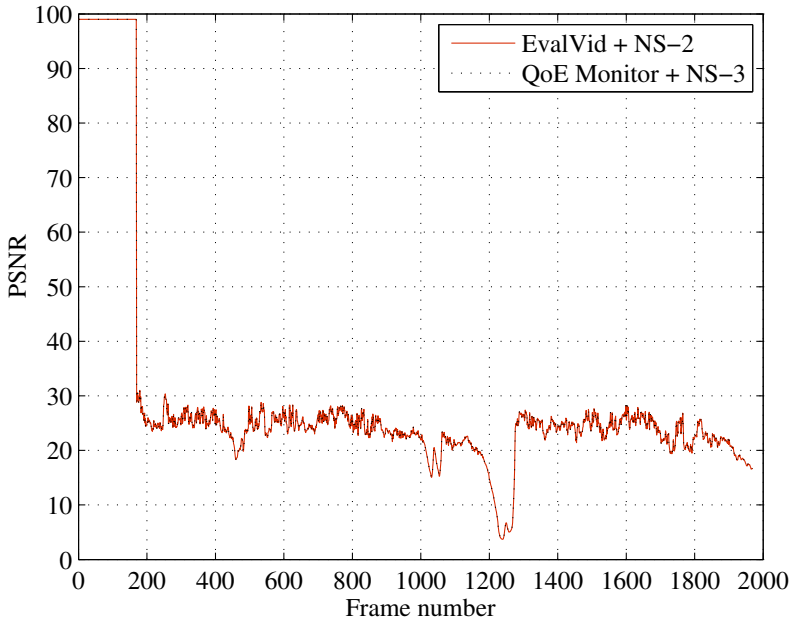
$$\varepsilon(m) = \frac{\|m_{EvalVid} - m_{QoE\,Monitor}\|}{m_{EvalVid}}$$

where m is the considered metric (i.e., PSNR, SSIM).

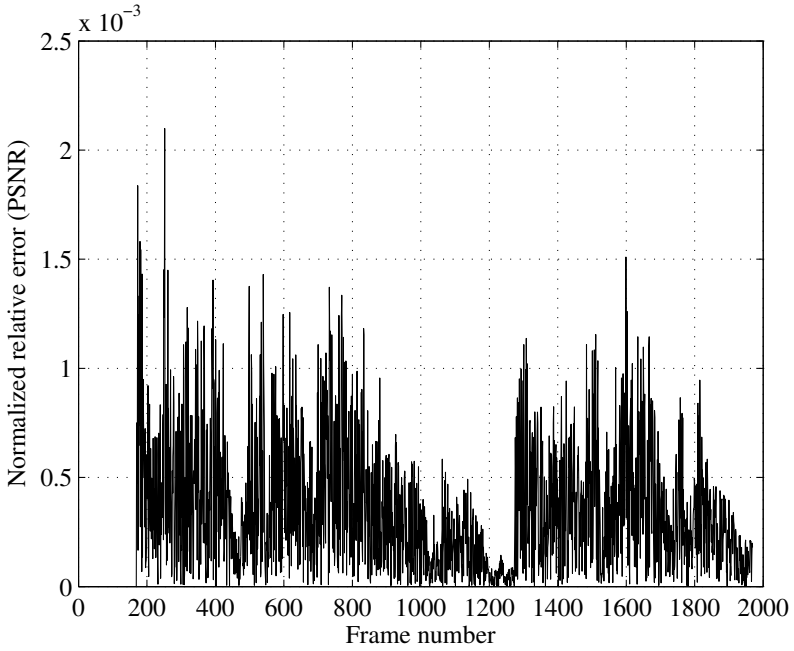
It is possible to observe that we obtain maximum errors of the order of about $2 \cdot 10^{-3}$ for PSNR and $2 \cdot 10^{-2}$ for SSIM, that allow us to conclude that both implementations are practically equivalent, which confirms the validity of our implementation.

Furthermore, to provide meaningful statistical results, for each tool (namely EvalVid and *QoE Monitor*) we have simulated the same topology, with the same packet-error-rate and the same video as before, and we have evaluated both PSNR and SSIM metrics for each frame. Then, for a sufficiently long simulation run, these values have been collected in two box-plot graphs[4] [51] reported in Figure 5.10a for PSNR and in Figure 5.10b for SSIM.

[4]The box-plot we have adopted here depicts the *median* value of a statistical sample, together with the *first* and the *third* quartiles (denoted as Q_1 and Q_3, respectively), which determine the width of the box. Here, the length of the *whiskers* depends on the *inter-quartile-range* (IQR), defined as $IQR = Q_3 - Q_1$. The edge of each whisker is the most extreme data point within the range $k \cdot IQR$ from the edge of the box (here we have $k = 1.5$). Those points falling next to the whisker's edge are considered *outliers*.

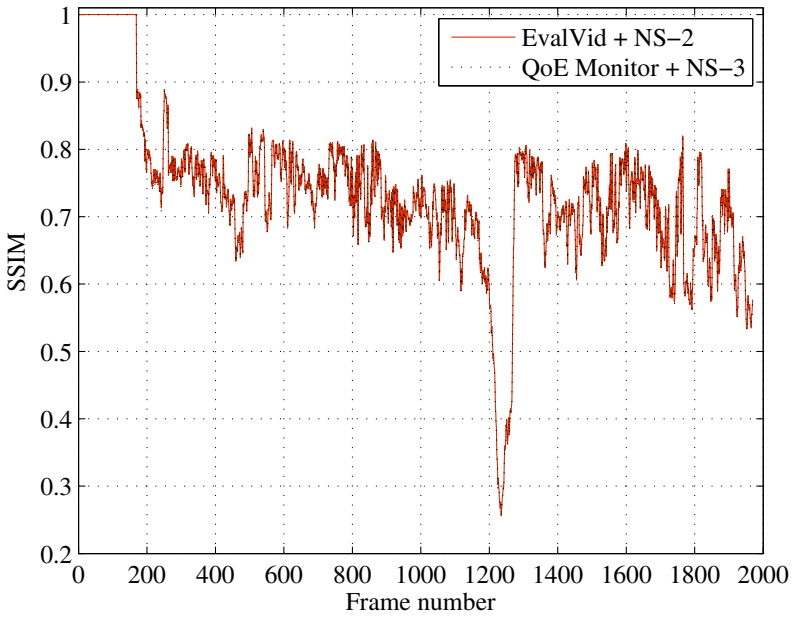


(a)

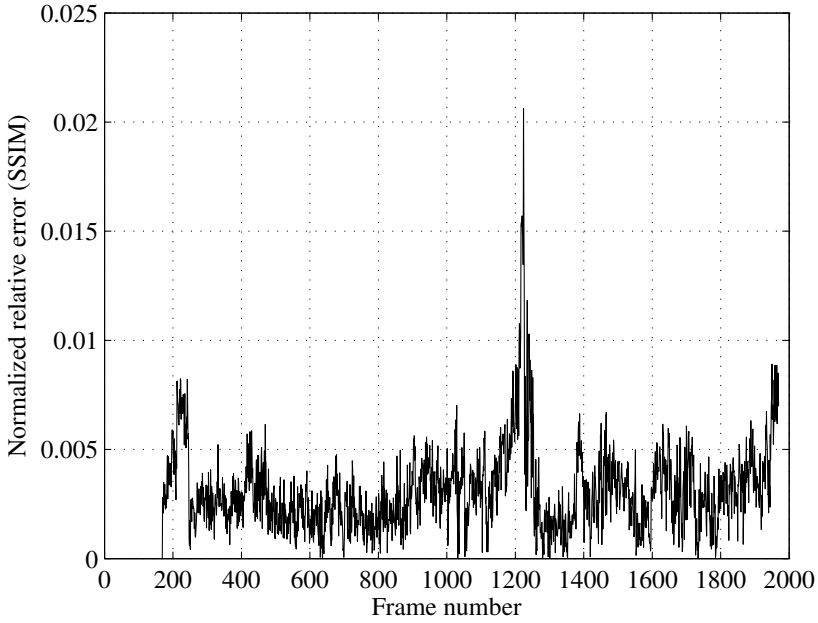


(b)

Figure 5.8: PSNR implementation comparison between EvalVid and *QoE Monitor*: (a) trend for each frame and (b) normalized relative error.



(a)



(b)

Figure 5.9: SSIM implementation comparison between EvalVid and *QoE Monitor*: (a) trend for each frame and (b) normalized relative error.

As can be seen, even though several outliers are present (they are pictured as small crosses in the graphs) the box-plots are very similar for both metrics, across the implementations; again, this confirms the correctness of the proposed design. However, please note that slightly lower values of both PSNR and SSIM can be found regarding *QoE Monitor*; since the same evaluation platform has been used for both tools, the reason for this discrepancy can be found in their different implementations. Currently, the *QoE Monitor*'s *MultimediaFileRebuilder* class does not conceal any lost video frame with the last correct one, as EvalVid does. Especially for high packet-loss-rate values, this leads to lower metric values, which is consistent with the reported results.

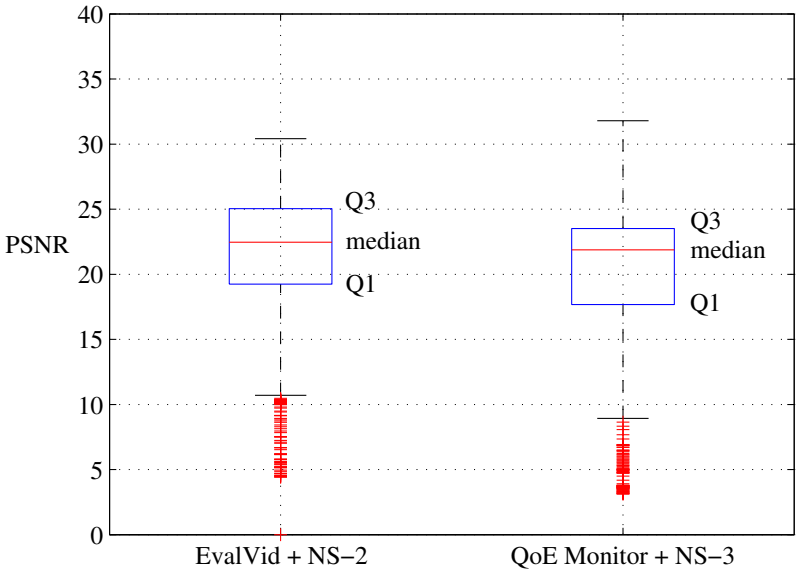
Finally, this first set of preliminary validation outcomes suggests that both tools (i.e., EvalVid and *QoE Monitor*) show comparable capabilities regarding the objective QoE assessment for video services. However, it is worth noting that the validation process has still to be completed, and more comprehensive results will be reported in future works.

5.6 Future Works

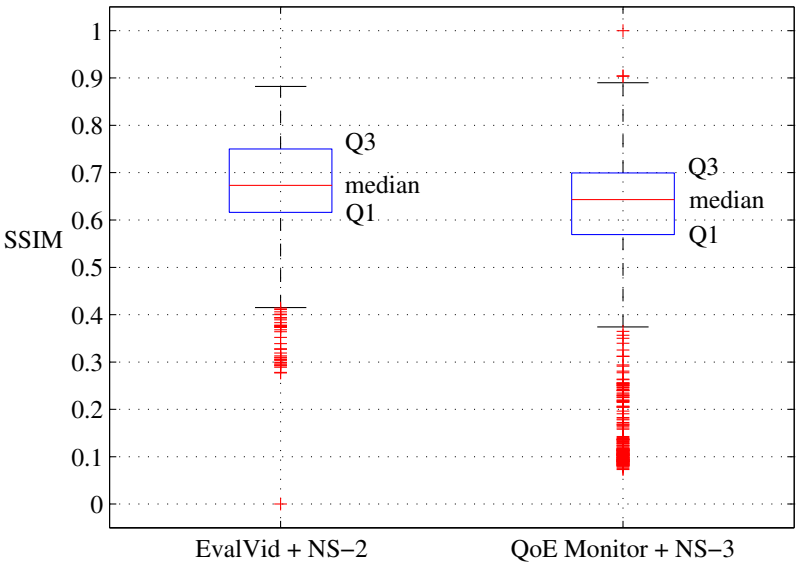
5.6.1 Possible QoE Monitor enahncements and improvements

Currently, the proposed *QoE Monitor* module can be effectively employed to perform video QoE evaluations over any possible network conceivable within the NS-3 framework, with the sole limitation of using H.264 encoded content (with Mpeg4 input and output contexts) with monotonic PTS/DTS. However, the modular architecture we have adopted for *QoE Monitor,* makes it perfectly suitable to be extended with respect to new codecs, new contexts and new metrics.

One of the main future works to have a more complete version of *QoE Monitor* module is the implementation of a set of objective metrics for the quality assessment of audio content. Up to now, only a simple difference between the transmitted audio sample and the corresponding received one is available, which can be roughly used to determine the overall noise resulting from the transmission. However, more complex and effective metrics must be implemented, in order to



(a)



(b)

Figure 5.10: Distribution comparison between EvalVid and *QoE Monitor*: (a) PSNR and (b) SSIM

provide a more solid and objective QoE evaluation, that can be possibly related to the MOS rank and closer to the real human auditory system perception. Among the others, metrics such as *Perceptual Evaluation of Speech Quality* (PESQ) [52] and/or the more recent *Perceptual Objective Listening Quality Assessment* [53] are two possible candidates for a future release.

Another important feature that is currently under study regards how transmission errors are concealed at the receiver side. As described in the previous Sections, when a packet loss is detected, dummy data is inserted into the output file, in order to align it with the file used at the transmitter side. However, other possible Forward Error Correction (FEC) solutions could be implemented, to greatly improve the user perceived QoE (e.g., the last correctly decoded video frame in place of the lost one) and to be more consistent with real implementations.

As previously stated, a fundamental process is validation. Though some results have already been presented in this Chapter (see Section 5), a significant work still has to be carried out, e.g., against more diverse reference scenarios and against other QoE evaluation tools.

5.6.2 QoE performance assessments for emergency network applications

Although the design of *QoE Monitor* originated from research activities related to the E-SPONDER project, until now (2012) only the very first steps of its implementation have been effectively completed, namely:

1. the implementation of a (small) set of core functions regarding video and audio assessments;

2. the validation of these functions by means of other systems, used as references.

Among all the work that still has to be done we may find the application of *QoE Monitor* to the E-SPONDER network, to validate the set of network services we expect for a real deployment, from the QoE perspective. This way, a connection between those results reported in the previous Chapter, with those that can be

obtained with *QoE Monitor*, could be established, which, in turn, could be used to improve the effectiveness of the preliminary design phase of a system like E-SPONDER.

5.7 Summary

Given the paramount importance that multimedia communications have in both the current and the future Internet, performance evaluation tools, that could be exploited by researcher and engineers to evaluate new networks design, in order to check if they can support high quality multimedia transmissions, and quickly perform objective QoE evaluations, are of great interest. In this Chapter, a novel QoE assessment tool for the NS-3 framework, named *QoE Monitor*, has been presented and described in great details.

A couple of practical reference scenarios have been presented to show how the current version works. Up to now, our tool provides the user with a working set of functions to assess the QoE performance of H.264-encoded transmissions over arbitrarily networks.

The obtained numerical outcomes, presented in Section 4, have demonstrated the validity of *QoE Monitor*, to provide the QoE evaluation of a video file coded and transmitted in two different contexts, that is comparable to the real perception of human eyes. Furthermore, a couple of validation results have been presented as well, which strengthen the value and the capabilities of the proposed tool. In more detail, in this Chapter we have demonstrated that the performance achievable with *QoE Monitor* tool over NS-3 match almost exactly with those obtained with EvalVid over NS-2, proving the effectiveness of our approach.

Moreover, *QoE Monitor*'s modularity and its open-source nature allow researchers to easily extend its features and capabilities (e.g., by adding support to new codecs or QoE metrics), as well as to validate its code base and share knowledge (e.g., setups, examples, test code). Besides, being designed especially for the NS-3 framework, *QoE Monitor* adds enhanced value to this framework, further expanding its already excellent capabilities. Finally, the reported numerical results prove the effectiveness of our tool in evaluating user QoE for video services.

Chapter 6

Conclusions and future works

In this Thesis, several important research issues regarding new generation public safety systems have been presented and discussed in details, from the perspective of the E-SPONDER EU project.

Starting from a general analysis about the current state-of-the-art of public safety systems and their current trends, we have moved, then, toward the analysis of the most important requirements that need to be addressed in next generation deployments.

Based on this, a feasible network architecture for the E-SPONDER system has been proposed, adopting a wireless mesh network approach. Accordingly, several possible technologies for its implementation have been identified, with the ultimate goal to compose a really interoperable network architecture, based on the IP protocol.

Furthermore, since information and communication security play a vital role for any public safety system (e.g., attacks performed by malicious users could greatly reduce the effectiveness of the whole emergency response) our research activity within E-SPONDER has moved toward the analysis of the most important security issues arising in modern emergency networks, to have a clear understanding of their impact on the whole system design.

To guarantee the validity of the proposed network design, several QoS performance assessments have been carried out by means of NS-3, considering realistic traffic flows, to understand how possible network impairments could affect the performance of the deployed services.

Finally, in order to perform user-oriented quality assessments (i.e., in terms of QoE), a new software tool, named *QoE Monitor*, has been developed for the NS-3 framework and has been released to the community as open-source software. Preliminary results have shown the validity of our tool, if compared with other well-known alternatives, such as *EvalVid*.

Although considerable work has already been done in the emergency networks field, several possible future research activities can originate from the topics described in this Thesis. In particular, we may suggest the following:

- the actual implementation of the proposed security solutions in a real testbed, to clearly understand the impact of the security protocol suite on the user's QoE;
- the fitting of emergency networks data traffic models with real data, to improve the accuracy of simulations outcomes for future QoS assessments;
- the adoption of QoE Monitor to perform QoE assessments in emergency network architectures, such as that proposed for the E-SPONDER system.

Bibliography

[1] "E-SPONDER homepage." http://www.e-sponder.eu/.

[2] D. Vassiliadis, A. Garbi, G. Calarco, M. Casoni, A. Paganelli, R. Morera, C. Chen, and M. Wódczak, "Wireless networks at the service of effective first response work: the e-sponder vision," in *Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on*, pp. 210–214, IEEE, 2010.

[3] G. Calarco, M. Casoni, A. Paganelli, D. Vassiliadis, and M. Wódczak, "A satellite based system for managing crisis scenarios: The E-SPONDER perspective," in *Advanced Satellite Multimedia Systems conference (ASMS), 2010 5th*, pp. 278–285, IEEE.

[4] "Tetra and critical communications association." http://www.tetramou.com/.

[5] "Tetra security." http://www.tetramou.com/Library/Documents/About_TETRA/TETRA%20Security%20pdf.pdf.

[6] "Project 25 technology interest group." http://www.project25.org/.

[7] "Project 25 phase 2." http://www.p25phase2.com/.

[8] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (special agent) johnny (still) can't encrypt: a security analysis of the apco project 25 two-way radio system," in *Proceedings of the 20th USENIX conference on Security*, pp. 4–4, USENIX Association, 2011.

[9] "Tetrapol website." http://www.tetrapol.com/.

[10] M. Portmann and A. Pirzada, "Wireless mesh networks for public safety and crisis management applications," *Internet Computing, IEEE*, vol. 12, no. 1, pp. 18–25, 2008.

[11] "Statement of requirements for public safety wireless communications and interoperability." `http://www.safecomprogram.gov`.

[12] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, and L. Stibor, "Ieee 802.11 e wireless lan for quality of service," in *Proc. European Wireless*, vol. 2, pp. 32–39, 2002.

[13] G. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "Ieee 802.11 s: the wlan mesh standard," *Wireless Communications, IEEE*, vol. 17, no. 1, pp. 104–111, 2010.

[14] B. Braden, D. Clark, and S. Shenker, "Integrated service in the internet architecture: an overview," 1994.

[15] D. Grossman *et al.*, "New terminology and clarifications for diffserv," tech. rep., RFC 3260, April, 2002.

[16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, *et al.*, "Sip: session initiation protocol," tech. rep., RFC 3261, Internet Engineering Task Force, 2002.

[17] H. S. et al, "RTP: A transport protocol for real-time applications." `http://tools.ietf.org/html/rfc3550`.

[18] R. Anderson, *Security Engineering: A guide to building dependable distributed systems*. Wiley, 2010.

[19] "An industry roadmap for open strong authentication." `http://www.openauthentication.org`.

[20] P. Zimmermann, "The official pgp user's guide," 1995.

[21] B. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *Communications Magazine, IEEE*, vol. 32, no. 9, pp. 33–38, 1994.

[22] K. Hoeper and G. Gong, "Models of authentication in ad hoc networks and their related network properties," *International Association for Cryptologic Research*, 2004.

[23] D. Harkins, "Simultaneous authentication of equals: a secure, password-based key exchange for mesh networks," in *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, pp. 839–844, IEEE, 2008.

[24] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. of Australian Unix Users Group Annual Conference*, pp. 95–102, 2004.

[25] "DVB-RCS homepage." `http://www.dvb.org/technology/dvbrcs/`.

[26] B. Goode, "Voice over internet protocol (VoIP)," *Proceedings of the IEEE*, vol. 90, no. 9, pp. 1495–1517, 2002.

[27] J. Rosenberg, "A framework for conferencing with the session initiation protocol." `http://www.ietf.org/rfc/rfc4353.txt`, 2006.

[28] M. Perkins, K. Evans, D. Pascal, and L. Thorpe, "Characterizing the subjective performance of the ITU-T 8 kb/s speech coding algorithm-ITU-T G.729," *Communications Magazine, IEEE*, vol. 35, no. 9, pp. 74–81, 1997.

[29] T. Stockhammer, M. Hannuksela, and T. Wiegand, "H. 264/AVC in wireless environments," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 13, no. 7, pp. 657–673, 2003.

[30] "NS-3 Project Homepage." `http://www.nsnam.org`.

[31] A. Molisch, *Wireless Communications*. Wiley, 2005.

[32] D. Green and A. Obaidat, "An accurate line of sight propagation performance model for ad-hoc 802.11 wireless LAN (WLAN) devices," in *Communications, 2002. ICC 2002. IEEE International Conference on*, vol. 5, pp. 3424–3428, IEEE, 2002.

[33] M. Ismail, G. Piro, L. Grieco, and T. Turletti, "An improved IEEE 802.16 WiMAX module for the NS-3 simulator," in *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques*, pp. 1–10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2010.

[34] "NS-3 QoE Monitor Homepage." `http://sourceforge.net/p/ns3qoemonitor`.

[35] J. Klaue, B. Rathke, and A. Wolisz, "EvalVid – A framework for video transmission and quality evaluation," *Computer Performance Evaluation. Modelling Techniques and Tools*, pp. 255–272, 2003.

[36] C. Ke, C. Shieh, W. Hwang, and A. Ziviani, "An evaluation framework for more realistic simulations of MPEG video transmission," *Journal of information science and engineering*, vol. 24, no. 2, pp. 425–440, 2008.

[37] "NS-2 Project Homepage." `http://www.isi.edu/nsnam/ns/`.

[38] GERCOM, "NS3 + EvalVid module developed by GERCOM." `http://gercom.ufpa.br`.

[39] "Everything about the data compression." `http://compression.ru/video/quality_measure/video_measurement_tool_en.html`.

[40] C. Lee, M. Kim, S. Hyun, S. Lee, B. Lee, and K. Lee, "OEFMON: An open evaluation framework for multimedia over networks," *Communications Magazine, IEEE*, vol. 49, no. 9, pp. 153–161, 2011.

[41] "GloMoSim." `http://pcl.cs.ucla.edu/projects/glomosim/`.

[42] "Q-Master Video System Homepage." `http://www.qoesystems.com/QMasterVideoSystem.html`.

[43] "Video Quality Analyzer Homepage." `http://www.acceptv.com/page/products_vqa`.

[44] "FFmpeg project homepage." `http://ffmpeg.org/`.

[45] "Libav project homepage." http://libav.org/.

[46] Y.-K. W. et al, "RTP Payload Format for H.264 Video." http://tools.ietf.org/html/rfc6184.

[47] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electronics letters*, vol. 44, no. 13, pp. 800–801, 2008.

[48] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *Image Processing, IEEE Transactions on*, vol. 13, no. 4, pp. 600–612, 2004.

[49] "VideoLAN organization, x264 homepage." http://www.videolan.org/developers/x264.html.

[50] "YUV CIF reference videos - lossless H.264 encoded." http://www2.tkn.tu-berlin.de/research/evalvid/cif.html.

[51] R. McGill, J. Tukey, and W. Larsen, "Variations of box plots," *American Statistician*, pp. 12–16, 1978.

[52] ITU-T, "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs, recommendation P.862." http://www.itu.int/rec/T-REC-P.862/en, Feb. 2001.

[53] ITU-T, "Perceptual objective listening quality assessment, recommendation P.863." http://www.itu.int/rec/T-REC-P.863/en, Jan. 2011.

Publications list

International journals:

1. D. Saladino, **A. Paganelli**, M. Casoni, "*A Tool for Multimedia Quality Assessment in NS3: QoE Monitor*", Simulation Modelling Practice and Theory, Volume 32, March 2013, Pages 30-41.

International conferences:

1. D. Vassiliadis, A. Garbi, G. Calarco, M. Casoni, **A. Paganelli**, R. Morera, C. Chen, M. Wodczak, "*Wireless Networks at the Service of effective First Response Work: the E-SPONDER Vision*", presented at the "5th IEEE International Symposium on Wireless Pervasive Computing", Modena (Italy), May 5-7 2010.

2. G. Calarco, M. Casoni, **A. Paganelli**, D. Vassiliadis, M. Wodczak, "*A Satellite based System for Managing Crisis Scenarios: the E-SPONDER Perspective*", presented at the "5th IEEE Advanced Satellite Multimedia Systems Conference", Cagliari (Italy), September 13-15 2010.

3. M. Casoni, **A. Paganelli**, "*Security Issues in Emergency Networks*", presented at the "7th IEEE International Wireless Communications and Mobile Computing" conference, Istanbul, July 4-8 2011.

4. **A. Paganelli**, D. Saladino, M. Casoni, "*QoS Performance Evaluation of Multimedia Services in Emergency Networks*", presented at the "8th IEEE International Wireless Communications and Mobile Computing", Limassol, August 27-30 2012.

5. G. Calarco, M. Casoni, **A. Paganelli**, D. Saladino, M. Schaap, "*A Resilient ICT System for Managing Crisis Scenarios*", presented at the "7th International Conference on Critical Information Infrastructures Security", Lillehammer, September 17-18 2012.

6. **A. Paganelli**, P. Valente, M. Casoni, "*A Modular Architecture for QoS Provisioning over Wireless Links*", accepted at the "8th IEEE International Workshop on the Performance Analysis and Enhancement of Wireless Networks (PAEWN-2013)".

Acknowledgments

The work described in this thesis has been made possible thanks to the continuous efforts made by tutor, Prof. Maurizio Casoni, who spent considerable time in coordinating the research activities we conduced within the E-SPONDER project. I would like to warmly thank him for all the work we have done together these years, which has considereably enhanced my professional knowledge, my approach on research and my skills.

Then, I would like to thank all the members of ELECOM laboratories at University of Modena and Reggio Emilia, who have helped me to become who I am now, by teaching me how to become a real engineer. Thank you guys, thank you friends and thank you for everything you have done for me!

This goal has been made possible also thanks to who helped me to understand how to face the life, during the last years, by means of training my mind according to the principles of Karate-Do. Thank you Sensei, you have been fundamental for teaching me how to never give up. Oss!

Furthermore, I would like to thank all the friends of mine of "La Panca", for all the great moments we have lived together these years, which gave me the strength to keep going on toward this goal.

Then, I would like to thank my family, which supported me along this long journey toward the Ph.D., even when problems arose along the way.

Last, but not least, I would like to thank my only reason for living, who really supported me during these years, by continuously pushing me toward pursuing the best I could do. Thank you Mile, thank you for being my love, my constant and my daily happyness!