IMS to Support Emergency Services and Applications

Christos Politis
WiMM lab, Kingston University,
London, KT1 2EE, United Kingdom

c.politis@kingston.ac.uk

Tasos Dagiuklas
Wireless Telecommunications
Laboratory, University of Patras,
Patras, Greece

ntan@teimes.gr

Yacine Rebahi
Fraunhofer Fokus, Kaiserin Augusta
Allee 31, 10589 Berlin, Germany

yacine.rebahi@fokus.fraunhofe.
de

ABSTRACT[1]
The transition to next generation networks is often coupled with the vision of innovative services providing personalized and customisable services over an all-IP infrastructure. To enable a smooth transition, next generation all-IP networks need not only support more services but also support emergency services. The idea here is to provide a general emergency management framework addressing extreme emergency situations such as terrorist attacks and natural catastrophes as well as day-to-day emergency cases based on the IP Multimedia Subsystem (IMS). In order to enable multimedia communication for emergency situations, an framework will be architected for supporting the distribution of currently centralised services such as VoIP and name translation and supporting those services in a reliable and secure manner withstanding any failures and changes of the network.

Keywords
IMS, emergency services, PEACE project.

1. INTRODUCTION
The transition to next generation networks is often coupled with the vision of innovative services providing personalised and customisable services over an all-IP infrastructure. To enable a smooth transition, next generation all-IP networks need not only support more services but also support current vital services, namely emergency services. In this work – in the framework of the ICT PEACE project – we will provide a general emergency management framework addressing extreme emergency situations such as terrorist attacks and natural catastrophes as well as day-to-day emergency cases based on the IP Multimedia Subsystem (IMS). To achieve this goal this work will be addressing two major technological challenges. First a general solution for secure multimedia communication in extreme emergency situations will be provided. Such emergency services in cases of natural disasters or catastrophes will often involve the establishment of an ad-hoc networking environment. In this context, we will be devising

mechanisms for fast and lightweight establishment of trust relations between ad-hoc members of an emergency team and ensuring the security of their communication. Further, to enable multimedia communication in such environments the architecture will be provided for supporting the distribution of currently centralised services such as VoIP and name translation and supporting those services in a reliable manner withstanding any failures and changes of the network.

The aim of this paper is to provide an overview of the our initial idea – part of the ICT PEACE project – which will architect a new way for communicating in emergency situations by utilising the All-IP infrastructures. This paper is structured as follows; section 2 provides a preliminary definition of the proposed framework, component architecture and IMS infrastructure; section 3 describes a set of emergency scenarios and their testing and demonstrations; followed by a conclusion in section 4.

2. THE FRAMEWORK
In this work we provide a general emergency management framework addressing extreme emergency situations such as natural catastrophes and terrorist attacks and as well as day-to-day emergency cases based on emerging standards. Therefore the work benefits from provisioning of emergency services using IMS (IP Multimedia Subsystem) [1]. To achieve these goals, the proposed architecture addresses two major technological challenges. Firstly a general solution for secure multimedia communication in extreme emergency situations will be architected for All-IP Networks. Secondly, in case of extreme emergency situations (e.g. flooding, earthquakes, forest fires) where part of the network may collapse, an ad-hoc network will be used to provide applications and services (e.g. P2P VoIP/Video Communications) among the rescue workers. In this paper, the first one only will be addressed.

Discussions about emergency services usually diverge into discussions about most prominent catastrophes and terrorist attacks, as illustrated in Figure 1. Such events tend to create havoc and panic over the general public. For this reason, it is important to define an appropriate crisis handling management scheme. This strategy will coordinate all the available resources in terms of public services (i.e. police, authorities, hospital, fire-brigade) so as this crisis is resolved smoothly. While these extreme events surely represent some of the most demanding scenarios for emergency services, in order to fulfil the requirements of modern societies, research and development in the area of emergency services need to address a much broader scope.

With the increased reliance of our modern societies on communication infrastructures and the migration towards IMS and all-IP next generation networks, research and development activities must aim at providing secure and reliable communication infrastructures even under extreme situations as well as integrating and migrating the current emergency service infrastructure. This includes not only replicating current emergency services in an IMS and all-IP environment but also enabling new forms of high-quality and secure communication infrastructure for emergency workers. First a general solution for **secure IMS communication in extreme emergency situations** will be designed. Further, to enable IMS communication in such environments, a framework will be provided for supporting the distribution of currently centralised services such as VoIP and name translation and support those services in a reliable manner withstanding any failures and changes of the network. Secondly, this work investigates the **provisioning of day-to-day emergency communication** such as call to the fire-department in next generation all-IP networks. Due to the different structure of IP and PSTN networks it is not possible to simply reuse current standards and solutions for realising such communication over IP networks.
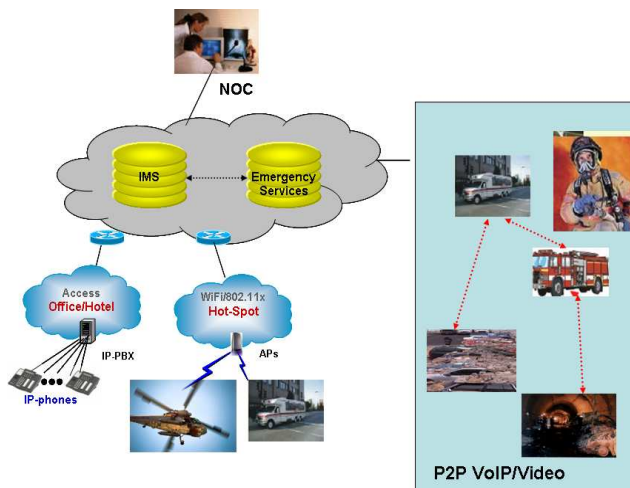

Figure 1. PEACE framework

The transition to next generation networks is often coupled with the vision of innovative services providing personalised and customisable services over an all-IP infrastructure. While this is surely an important aspect and a strong driving force behind the development of and transition to next generation networks, this is only one side of the coin. To enable a smooth transition, next generation all-IP networks need not only support multimedia services but also support emergency services. By supporting emergency services for both daily and catastrophe situations this architecture will enable a seamless transition from the plethora of currently used networks and technologies to an all-IP infrastructure.

The proposed framework primarily concentrates on providing secure and reliable communication services for emergency workers communicating in an ad-hoc manner in the field as well as to citizens placing an emergency call. This will involve defining the appropriate protocols and extensions to current standards, defining and realization of methods for protecting the

system against malicious use and denial of service attacks and supporting prioritised handling of emergency communication. ETSI (EMTEL), IETF (ECRIT) [3], 3GPP and the IST project EGERIS and PSC Europe Forum (www.psc-europe.eu) already look at providing emergency services based on IP federated networks (IPFN). The IPFN concept supports various multimedia services, authentication and VPN services as well as prioritised handling of emergency services. On the one side, we extend this concept by investigating more in detail the aspects of secure and reliable ad-hoc communication between emergency workers, legislative and technical aspects of supporting emergency call services using VoIP and/or Video and protecting the emergency services from malicious use and denial of service attacks. On the other side, we consider the gateways to IPFN networks and the usage of IPFN for connecting between different subsystems.

2.1 Objectives and Motivations

The key objectives of this work are described in terms of four major key goals as discussed below.

Next Generation Emergency Communication System; Work and development in the area of emergency services has often resulted in a separate communication infrastructure with special radio frequencies, protocols and hardware. This has resulted in expensive and often non-interoperable solutions. While current approaches such as TETRA already provide a networking technology that will be available to different emergency agencies it is still a closed network with expensive equipment. Besides its low bandwidth, there are already different non-interoperable flavours of the TETRA technology that will be used in different countries. This would make the communication between emergency agencies from different countries just as difficult. Our goal in the PEACE project is to realise emergency services based on an all-IP network and standardised platforms such as IMS, which is proposed by the 3GPP, ETSI and IETF as the basis for multimedia communication in next generation networks.

One of the major objectives of this work is to specify and design emergency management architecture for next generation networks. To achieve this, the project aims at:

- − Specifying a generic all-IP IMS-based emergency management architecture.

- − Investigating and providing solutions for supporting daily emergency communication based on IP protocols. This requires not only specifying extensions to current solutions but also devising new ones for user location for instance. This work involves thereby specification, development and standardisation efforts. While already first efforts at IETF and ETSI are being launched for specifying the requirements and extensions needed for VoIP, no complete solution exists till now.

- − Supporting ad-hoc communication in a secure manner between workers of the same emergency agency as well as between workers of different agencies with least possible configuration overhead (in cases where fire-vehicle units and personnel must operate in remote areas and the conventional communication technology is insufficient). This involves specifying mechanisms for establishing trust relations between the involved parties

in a dynamic manner as well as supporting IMS in distributed environments. While first concepts for supporting secure communication in ad-hoc networks already exist, there is still a clear need for identifying fast and light-weight authentication mechanisms in a distributed manner.

- Integrating the emergency infrastructure with next generation networks.

- Providing light-weight and fast mechanisms for user authentication and authorisation. This is especially needed for preventing malicious and fraudulent emergency calls or misuse of the emergency infrastructure for private use.

- Integrating methods for call prioritisation with SIP-based [4] communication to allow the networks to better identify emergency calls and provide higher QoS for such calls.

- Besides providing higher QoS to emergency calls, it is also of utmost importance to ensure the capability of wireless and fixed networks to deal with sudden bursts of emergency calls. Emergency congestion is a situation hardly managed in cellular networks of today. Overload arises due to day-to-day emergency situations and quite often in non-predictable events, since cellular networks are not built with a redundancy similar to the one of fixed networks; therefore, they are more sensitive to congestion situations than fixed networks. The need of reliable and easy to use, in combination with low costs, network data technologies

Secure and Reliable Networking Infrastructure for Emergency Management Systems; The Internet is usually described as a reliable network providing services in a distributed and end-to-end manner. However, taking a closer look we often find that services are supported using centralised servers or hierarchically distributed infrastructures. Hardware, software or network failures due to DoS or terrorist attacks or natural catastrophes would render the support of different services such as VoIP or even DNS useless. To overcome these problems solutions for providing reliable servers are needed. While there are already several solutions for redundant servers overcoming hardware or software problems, solutions are still needed for overcoming DoS attacks and network failures. Some of the major benefits of ad-hoc networks are their high reliability and survivability. By integrating some of the concepts of ad-hoc routing and transport into service provisioning platforms one can support such features in the fixed networks as well. This not only results in higher reliability in face of denial of service attacks but also more scalable solutions as well. This work would involve:

- Investigate and realise mechanisms for providing reliable services in IP networks in general and ad-hoc networks in particular. Current approaches for achieving reliability require a massive overhead in hardware and software components and sometimes even changes in end systems as well. In our work we look at different solutions such as anycast, reliable server pooling and federated servers.

- Providing of mechanisms for identifying DoS attacks and triggering appropriate defence solutions. This on the one hand includes providing mechanisms for identifying and reacting to bulk attacks. On the other hand mechanisms are specified and realised for identifying attacks on the protocols used in the emergency infrastructure such as SIP and DIAMETER.

- Specification and realisations of fallback solutions for overcoming DoS attacks and network failures.

- Integration of a general measurement platform in the networking infrastructure for collecting data on failures and attacks and reporting them to the emergency handling system.

- Specification and development of a security infrastructure allowing the secure cooperation between different involved entities in the emergency system.

Emergency Risk Management and Coordination System; To identify the required emergency handling tasks and coordinate the actions of all involved emergency workers this work will develop a general emergency risk management and coordination system.

The emergency risk management and coordination function (ERMCS) sets the activities to be carried out during the entire disaster event lifecycle, from the emergency planning up to the dissemination of the required tasks to the appropriate entities and the coordination between those entities. This will provide the PEACE project a complete picture on: "*How to face any emergency event*".

2.2 IMS Evolution and Emergency Services

The IP Multimedia Subsystem (IMS) is the key enabler in the mobile world for providing rich multimedia services to the end-users and it is currently being standardized by 3GPP (IMS Release 6). Although originally designed for mobile networks, IMS has been considered as core component for NGN fixed networks. This vision is supported by the standardisation bodies 3GPP, ETSI TISPAN and 3GPP2/LTE.

IMS is defined as a network architecture that defines functional elements. Each functional element does not have to relate one-to-one to a physical element. A number of functional elements can be incorporated into a physical element depending upon a vendors implementation. The Service Architecture defines standard methods for services to be introduced while the Core Network defines the interactions between functional elements, as illustrated in Figure 2.

Figure 3 reflects exactly 3GPP specifications and defines protocol interfaces required to deliver a call to the legacy Emergency Services Network or an IP-capable PSAP. Note that PSAP selection is left to implementation. Also the IP PSAPs are treated a peer network since the interface is from a S-CSCF to the PSAP and a P-CSCF is not included to manage the PSAP interface. Serious work on Emergency Services has just started within IMS standards. The initial assumption is that Emergency Services would follow legacy methods. This slide illustrates the conceptual model currently defined in 3GPP. The IP Connectivity Access Network (which represents the wireless access, cable access, etc.)

forwards the call to the P-CSCF in the IMS Core Network and the call is routed to the S-CSCF. The S-CSCF performs PSAP selection. However, 3GPP currently defines this as left to the implementation. There is current work within IETF to define this. The emergency call may be delivered to the legacy Emergency Services Network through Media Gateways.
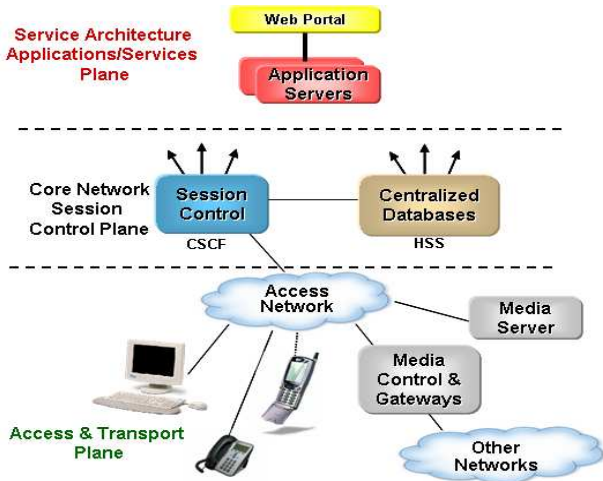

Figure 2. IMS Framework

The emergency call may be delivered to a PSAP capable of directly handling SIP calls. Note that a significant amount of work is required to define the interactions between the IMS network and a IP-capable PSAP. (Note that the IMS Core network treats the PSAP as a foreign network since the interface is from a S-CSCF to the PSAP and a P-CSCF is not included.)
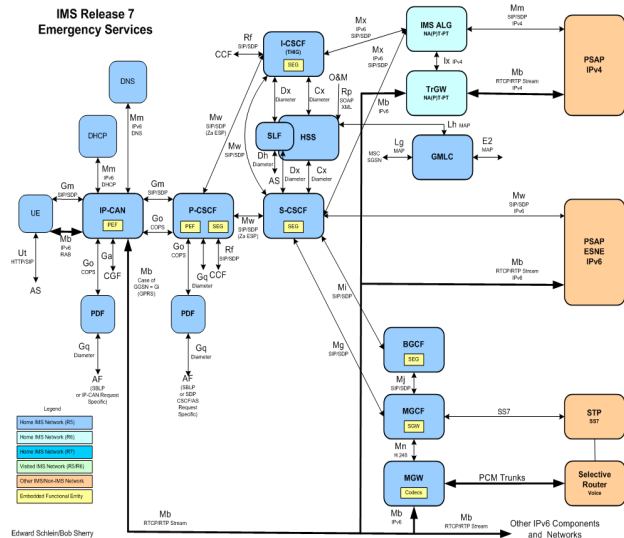

Figure 3. **Emergency Services in IMS**

3. TESTING AND DEMONSTRATIONS

To assess the practical usability and technical correctness of the proposed emergency framework will be tested and demonstrated in two phases. In the first phase, the system will be tested in the laboratories of the involved partners. At this stage, the aspects of ad-hoc communication, integration with other technologies, the measurement and denial of service detection as well as other aspects of the project will be tested and evaluate regarding their technical correctness, performance and scalability. The second stage will involve the user community and it will be deployed in a real-life environment.

Within the context of this work, a first set of experiments will be carried out in IMS/SIP environment. In this testbed the following tests will be carried out:

- Reliability of the emergency services within the IP network using IMS.
- Scalability of the architecture to support a large number of users.
- Support and demonstration of emergency services.

A second set of experiments will be carried out using autonomic networks. For the specified, scenarios, the autonomic nodes will demonstrate their ability to:

- Support the uninterrupted provisioning of both emergency VoIP applications in a dynamic setting.
- Run a common middleware platform that will allow the deployment of message-oriented, reliable overlay architecture.
- Self-configure.

3.1 Emergency Scenarios

Within the context of this work, the following emergency scenarios will be designed and evaluated:

1. Emergency Call Delivery from VoIP Towards Legacy PSAP: If a call originates from a VoIP network capable providing the location of the caller (PIDF-LO) and must be delivered to the Legacy ESNet or a Legacy PSAP (see figure below).
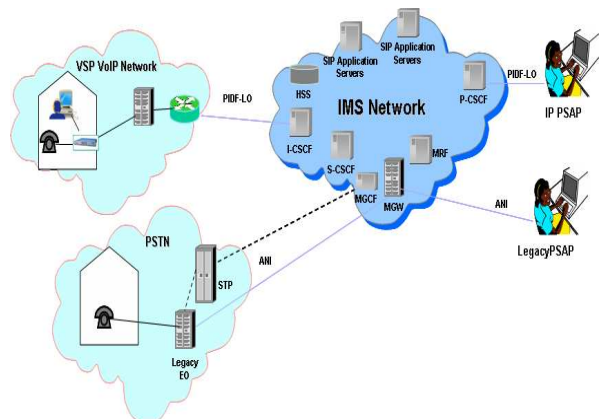

Figure 4. Emergency Call Delivery from VoIP Towards Legacy PSAP

2. Emergency Call from Legacy PSTN to IP PSAP: Calls from the PSTN or legacy end offices can only pass the caller's number. f the call is destined to a IP PSAP, the IMS would require a mechanism to acquire the caller's location, use it to select the PSAP and forward the call to the IP PSAP with location (PIDF-LO) (see figure below).
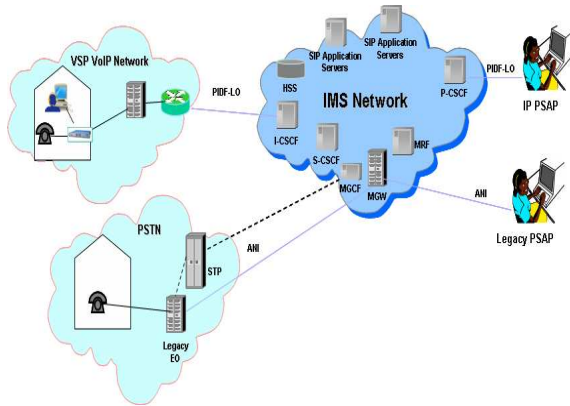

Figure 5. Emergency Call from Legacy PSTN to IP PSAP

4. CONCLUSIONS

In the context of this work, we will address the issue of providing support for emergency services for a wide range of scenarios in next generation all-IP networks. This involves specifying and realising mechanisms for supporting secure and reliable communication infrastructures fulfilling the requirements of current and future emergency support services. To achieve this goal the work distinguishes between extreme emergency situations (e.g. handling natural catastrophes) and daily emergency situations (e.g. calling an ambulance, fire-brigade or a police station). Further, to ensure the reliability and security of the system a major part of the work will also be dedicated to securing the emergency infrastructure and providing solutions for increasing the reliability of the communication services.

5. ACKNOWLEDGMENTS

6. REFERENCES

[1] 3GPP, (2005), "IP Multimedia Subsystem version 7", 3G TS 23.228.

[2] Akyildiz I. et al, (2008, in print) "Wireless mesh networks: a survey", Computer Networks, Elsevier.

[3] IETF/ECRIT, http://www.ietf.org/html.charters/ecrit-charter.html, Emergency Context Resolution using Internet Technologies.

[4] Singh K., Schulzrinne H., (2004), "Peer-to-Peer Internet Telephony using SIP", Columbia Univ. Technical Report CUCS-044-04.

[5] Stojemenovic I., (2002), "Position-based routing in ad hoc networks", IEEE Communications Magazine, 40(7):138–134.