Eliminating the Communication Black Spots in Future Disaster Recovery Networks

Eliane Bodanese[1], Liljana Gavrilovska[2], Veselin Rakocevic[3], Robert Stewart[4]

[1]Electronic Engineering Department, Queen Mary, University of London, E1 4NS, UK
[2]Faculty of Electrical Engineering, University Ss Cyril and Methodius, Skopje, Macedonia
[3]Information Engineering Research Centre, City University, London EC1V 0HB, UK
[4]Electronic Engineering Department, Athlone Institute of Technology, Ireland

***Abstract*: This paper presents the current challenges and possible solutions for eliminating communication black spots in emergency environments. Establishing sustainable communication in emergencies and disaster recovery situations is an area that is increasingly attracting global attention. This paper analyses integrated information systems operating in disaster recovery environments. Specialized disaster recovery information systems are normally established in non-conventional environments in response to random events that normally disable some or all services in the vicinity. Current research shows that these specialized information systems require dedicated communication systems that are intelligent, robust, scalable and responsive. In this paper we analyse the challenges and present a solution. The solution proposes the use of fixed and mobile public network infrastructure to eliminate communication black spots in emergency information systems. We show how these solutions could be provided by using adequate policy-based network management systems.**

Key words: *emergency services, premium service delivery, end-to-end QoS, policy-based network management*

1. INTRODUCTION

Currently, emergency communications are being deployed over dedicated communication systems such as TETRA [1] or Project 25 [2]. While the quality and the coverage of these systems are constantly improving, the need for high-speed transparent communication in emergency environments is rapidly growing. With the increased need for multimedia information, it is highly unlikely that a dedicated system will be able to answer all the needs of an advanced emergency team, and therefore, public network infrastructure will have to be used.

In real-life scenarios, this is equivalent to the following scenario: in the immediate vicinity of an emergency, a spontaneous network is established composed of several different types of wireless devices, for example, sensors, notepads, cameras, mobile phones, PDAs, vehicles, computers, etc. This ad hoc collaborative networking will perform several rescue processes, e.g. to monitor medical information from a number of patients. Regardless of the size of the disaster, the objective of the communication system is to enable the ad-hoc network to communicate to the outside world. This *spontaneous* network needs to be able to discover the presence of the global network and, by communicating application information such as authentication data and network service specification, to discover the network entities ready to relay the data towards a remote hospital or emergency control centre where data can be further processed. The performance and reliability of current communication networks under critically overloaded conditions triggered by large-scale emergencies (natural disasters or man-made catastrophes) have been shown to be inadequate. There is a clear need for a uniform policy-based framework for premium service provision in heterogeneous network environments.

This paper contributes to the ongoing research in heterogeneous network systems by presenting the most important issues disaster recovery networks face. Section 2 presents the particular requirements disaster environments put on the network; section 3 explains the challenges of using public network infrastructure to support

disaster recovery; section 4 briefly introduces policy-based network management and, finally, section 5 provides the direction towards a feasible solution.

2. DISASTER RECOVERY NETWORKS

In recent years the global disaster recovery community has highlighted that existing "early warning systems" have a serious weak point in the dissemination of the warning to the vulnerable community: *"... the single most important weakness of existing early warning systems is the growing improvements in the technical identification, detection and modelling of hazard threats built upon relatively unchanging capability and procedures for warning and response management: a case of modern forecasting using unchanged warning procedures and systems. Consequently, the communication from forecast agencies to warning organizations to vulnerable communities represents the weakest links in warning systems"* [3].

In emergency scenarios, effective co-ordination of emergency services relies on the timely dissemination and distribution of mission critical data from the field. The future dedicated emergency response communication environments need to become more intelligent, robust, scalable and responsive. Especially important in this respect is the end-to-end provision and correlation of data from a series of simultaneously activated emergency response systems. The emergency response systems may be a few kilometres or hundreds of kilometres apart. Robust connectivity in difficult environments and support for the integration of heterogeneous networks is needed.

Immediately before a disaster, or in the period just after the disaster, the communication between different emergency services and between the emergency services and control centres is essential. Applications that are critical in the event of disasters require information systems that maintain high levels of security yet are instantaneously accessible for authorized end users.

The main challenge faced by the research community is to transform a potential communication black spot or series of black spots where little or no facilities remain to a reliably functioning emergency response system. As we can see in Figure 1, any available network must be used to create the best possible communication link. Crucial to this development is the ability of network gateways to communicate information regarding the authentication, quality of service and availability of the networks they belong to.

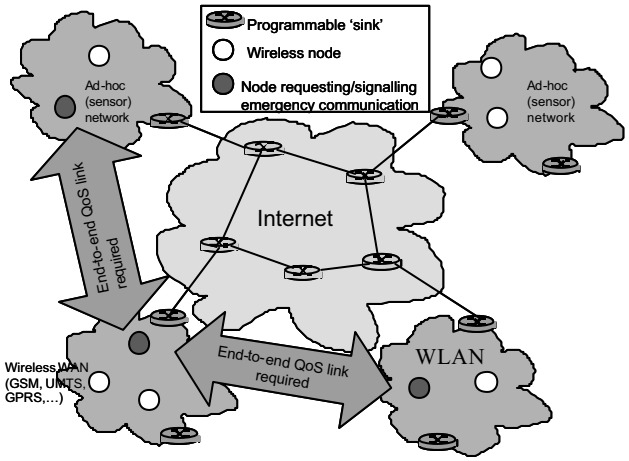

Figure.1: Heterogeneous network coexistence in an emergency scenario

3. PUBLIC NETWORK CHALLENGES

Most of the existing work is concentrated on maximising the performance of (typically) ad-hoc networks in the close vicinity of the disaster area. For example, IST project WIDENS [4] focuses on providing a common 2Mbps communication system in the disaster area. WIDENS specifies the functionality of the so-called *terminodes* which are to operate as centralised intelligence in these ad-hoc networks. Although the existence of a high data rate ad hoc network is highly desirable in a emergency scenario, it is necessary also to extend this vision by providing solutions for the integration of *the existing* public network infrastructure into a communication system capable of providing guaranteed high-speed reliable end-to-end communication in all links.

The main challenges in the process of integration of the public network infrastructure include:

- Poor interfaces between individual network infrastructures
- Inadequate interfaces between military and civil network infrastructures
- Incompatibility of network design with emergency situations
- Inadequate support for traffic prioritization and Quality of Service in mobile networks, resulting in the lack of reliable high-speed links between mobile emergency teams and remote services.

4. POLICY-BASED NETWORK MANAGEMENT

Any communication solution for emergency scenarios will rely in the application of emerging technologies and will embrace new features predicted in the *Next Generation Network (NGN)* framework. The next generation networks will be QoS adaptive, will require fast service creation and resource management through a combination of 'network-aware applications and application-aware networks' [5]. Policy-based network management (PBNM) is a promising way to achieve adaptive QoS and application-aware networks. PBNM is based on the use of **policies** to guide management decisions and execution. Policy-based networking configures and controls various operational network features, providing the network operator with a simple, usually centralised and automated network control.

The key feature of policy management is the ability to express a hierarchy of related policies at different levels of abstraction. *Top-level* policies directly express service provider business goals and rules in terms of products, services, customers, and financial objectives. Also special policy rules shall be deployed regarding different types of emergencies (fire, earthquake, flood, etc.). A PBNM system allows these rules to be mapped to a series of *lower level*, concrete, policies that are used for service creation, deployment and operation and for configuration of network rules, elements and entities [6, 7].

For the disaster recovery networks, the policy-based management issues are somewhat different than in the standard commercial networks. Important issues for emergency networks include:

1. Need for **quick** policy deployment and modification. Dynamic policies are needed to assure dynamic policy enforcement on an ongoing basis. The most important dynamic functions include monitoring, policing, maintenance, renegotiation, adaptation and feedback
2. Policies must include intelligent and dynamic re-routing rules of the traffic away from congested or highly damaged network domains
3. Risks of admission rejection must be minimized – contingency plans for the deployment of PBNM in the network domains that do not support general policies must be firmly established. . Research on heterogeneous network policy deployment and correlation/interconnection shall be performed
4. There is a need for **special policies**, which may not be influenced only by operator's business needs. For example satisfying the customers in emergency situations is very different to satisfying the customers in commercial networks
5. Security and authentication policies are essential. There must be a quick method of translating authentication policies between network domains.

In terms of the implementation issues, we have identified four main challenges for the use of PBNM in the integrated disaster recovery network solutions: Policy definition language for specifying policies; Policy information and data model; Policy management architecture for emergency communication; Policy enforcement and monitoring.

5. PROPOSED SOLUTION

We have seen in the previous discussion within this paper that interoperable gateways are the key to any efficient solution for disaster recovery networks. The gateways must use a customized policy management solution for premium service provision. Policy-based Network Management (PBNM) can reconfigure network devices by producing or changing policies, bringing the flexibility needed in an emergency scenario. An appropriate distributed policy-based management

infrastructure is used to collect, manage and distribute all the relevant information.

The gateways must be able to exchange available service descriptions and authentication information, and to forward the data from network to network. The emergency policies must be distributed, maintained and enforced throughout the network. The proposed system should provide quick load balancing and/or vertical handovers in the case of infrastructure failures.

One of the main issues is how to provide *premium* service in emergency environments. The premium service refers to applications which require delay and bandwidth guarantees. The premium service must be provided end-to-end across various network domains. The two main features of the premium service are the prioritised treatment of the emergency traffic and the reliability of the communication. We can identify the main network environments as the UMTS wide area network, the local wireless network built under the IEEE802.11 standard (both ad-hoc and infrastructure), and the fixed IP network (Figure 2). At the access to the network domains, gateways will have to provide context recognition and admission. After the admission, the gateway will identify the policy to be applied, distribute this policy to local Policy Enforcement Points and following the data transmission monitor the policy enforcement.

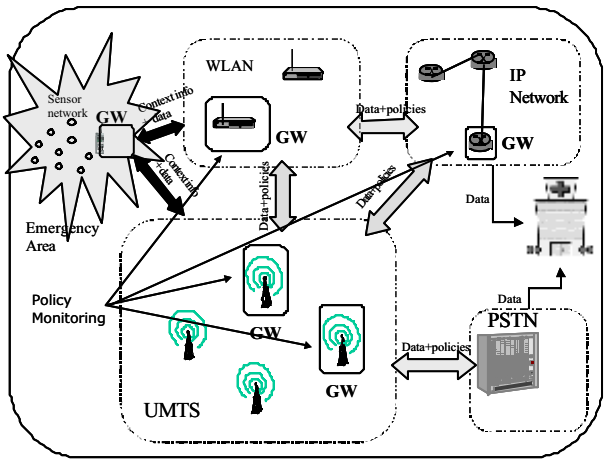

Figure 2 Emergency Gateways Architecture

The lack of uniform service definition across heterogeneous network contexts presents another important challenge. A gateway finding itself in a new network context will require detailed information about the existing services in order to be able to establish a guaranteed service communication. One important issue to be tackled is the problem of selecting the most suitable network to transfer the emergency data. The gateway will probe available networks and select the most suitable access network depending on the available infrastructure.

In emergency scenarios, once the traffic is created at the origin, this traffic will require high priority treatment in the intermediate network domains. This means that the gateway will have to perform these main activities:

a) Probe available networks to obtain *service descriptions*
b) Perform service prioritisation
c) Manage communications depending on the surrounding infrastructure
d) Manage the communication security for the established connections

The main issues that arise from these discussions include: integration of spontaneous networks with multiple functionalities, definition of the service discovery process to be used by the gateway and the devices and the communication protocols within the spontaneous network, intelligent network access selection and definition of communication interfaces with the neighbouring network contexts, context description and modelling, integration of adaptable policy management, and unique user identification and authorization.

The gateway needs to work as an intelligent and autonomous entity adapting policies according to the incoming information. The logic adaptation must process all relevant device and application contextual information. The range of gateway functionality in disaster recovery networks differentiates it from other policy based propositions and is a major challenge.

Once the device is recognized and identified, the Policy Decision Point (PDP) is activated and it enforces the policy on the Policy Enforcement Point (PEP). PDP and PEP are standard elements of a PBNM system. At this point the major activities triggered by the policies are fully characterizing the traffic for the transmission, context exchange with other networks

and probing the surrounding networks. The gateway needs to be able to decide the best possible network access for the application, maximizing the delivery guarantees of the traffic to be transmitted. This decision must be based on the application and context characteristics and triggered policy actions.

6. CONCLUSION

This paper presented a very important issue of using public network infrastructure in the design of disaster recovery networks. The paper presents the problem and highlights that end-to-end quality of service and reliability is the main design requirements. Policy-based network management, combined with complex intelligence within the network gateway has been presented as the way forward.

REFERENCES

[1] www.tetramou.com

[2] www.project25.org

[3] Seth D. Vordzorgbe. “Synthesis of the findings of the early warning regional consultations in Africa, Asia, the American Hemisfere and Europe”. Report of the 2° International Conference on the Early Warning (EWC II)" held in Bonn in October 2003 and supported by the UN ISDR (International Strategy for Disaster Reduction).

[4] http://www.widens.org/

[5] Sloman M and Lupu E., “Security and Management Specification”
IEEE Network March/April 2002.

[6] D. Raz and Y. Shavitt. “Active Networks for Efficient Distributed Network Management”. IEEE Communications Magazine, 38(30:138-143, March 2000.

[7]IETF Policy Framework Working Group web page: http://www.ietf.org/html.charters/policy-charter.html