ICT-MobileSummit 2009 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2009
ISBN: 978-1-905824-12-0

A Framework supporting Extreme Emergency Services

Emmanouil A. Panaousis[1], Arvind Ramrekha[1], Konstantinos Birkos[2], Christos Papageorgiou[2], Vahid Talooki[3], George Matthew[3], Cong Thien Nguyen[4], Corrine Sieux[4] Christos Politis[1], Tasos Dagiuklas[2], Jonathan Rodriguez[3]
[1]*Wireless Multimedia & Networking (WMN) lab, Kingston University, London, UK*
Tel: +442084172653, Email: {e.panaousis,a.ramrekha,c.politis}@kingston.ac.uk
[2]*Department of Electrical and Computer Engineer, University of Patras, Patras, Greece*
Tel: + 302610996466, Email: kmpirkos@ece.upatras.gr, xpapageo@ceid.upatras.gr, ntan@ece.upatras.gr
[3]*Instituto de Telecomunicações, Aveiro, Portugal*
Tel: + 351234377904, Email: {vahid,georgematthew,jonathan}@av.it.pt
[4]*Thales Communications, Colombes, FRANCE*
Tel: +33141303155, Email: {cong-thien.nguyen, Corinne.SIEUX}@fr.thalesgroup.com

Abstract: In many extreme emergency scenarios, such as natural or manmade disasters, the rescuers may face difficulty using traditional legacy networks due to destruction or collapse of infrastructure in such events or in case of remote disaster locations. The nature of mobile ad hoc networks (MANETs) makes them suitable to be utilized in the context of an emergency for various rescue teams. However, the security and reliability of the mobile ad hoc based communications can be decisive in the effectiveness and efficiency of rescue missions in extreme emergency cases. Furthermore, these stringent requirements propagate through to upper layers that include transport and application layer. In this paper we propose a framework for handling the P2P overlay serves different purposes and combines different technologies. The general functionalities of the framework are structured and unstructured overlays in MANETs. In addition, we propose a new suite of protocols called PEACE[1] Security Platform (PSP) that can address the key research challenges surrounding fast, reliable and secure MANETs for supporting emergency services in extreme catastrophic events.

Keywords: Mobile ad hoc networks, IP-based emergency infrastructures

1. Introduction

The transition to next generation networks is often coupled with the vision of innovative services providing personalized and customizable 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. These include communications solutions to address emergency situations. Such emergency services in cases of natural disasters or catastrophes will often involve the establishment of an ad hoc networking environment. In this context, there is a need for mechanisms for fast and lightweight establishment of trust relations between ad hoc members of an emergency team and ensuring the security of their communication. Furthermore, to enable multimedia

[1] The EU-FP7 PEACE project investigates the provisioning of day-to-day emergency communication in next generation all-IP networks. PEACE is a partly funded EU project. For more info visit: http://www.ict-peace.eu/.

communications in such environments an "emergency" architecture is required for supporting the distribution of currently centralized services. Second, the delivery of extreme emergency services require a general emergency risk management and coordination system to set 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 a complete picture on: "*How to face any emergency event*" to identify the required emergency handling tasks and coordinate the actions of all involved emergency workers.

The main objectives in this paper are to address novel research approaches in the areas of secure and reliable multimedia communications for extreme emergency services in heterogeneous wireless networks thus enabling the delivery of emergency services to the 'end-user' in a coordinated and optimized way. Furthermore, we propose a novel secure suite of protocols that is considered to be the key enabler for delivering secure, fast and reliable emergency services in extreme emergency events.

This paper is organized as follows. Section 2 identifies the scenarios and system requirements for the extreme emergency service architecture; whilst in section 3 we address the secure framework for extreme emergency scenarios in terms of vulnerabilities, countermeasures, secure ad hoc routing approaches and trust establishment processes; and the conclusion in section 4.

2. Extreme Emergency Service Architecture

2.1. Scenarios and requirements for extreme emergency services

Emergency situations can be natural disasters including earthquake, hurricanes, flood, fire and volcano or human made emergencies such as terrorism. In both cases the consequences could be very heavy. Hence, these emergency cases might require ad hoc communication networks to be setup quickly and efficiently as other pre-installed networks might be damaged or not present in case of remote locations. In the extreme emergency situations, the following requirements are required:

- Capability of the system to quickly set up ad hoc networks interconnected to other ad hoc networks and remaining functional infrastructures, when no existing or when all existing infrastructures have been destroyed.
- Automation of deployment (self deployment and self coordination).
- Autonomous systems (Dynamic reconfiguration and rerouting functionalities).
- Self healing functionalities (ability to recover after a link break or other network disruption).
- System availability (the system must be available and operating during the whole life time of the deployment).
- Connection to the outside world.
- P2P communications must be supported by the wireless system (either voice or video).
- The network architecture will be comprised of a mixture of hybrid wireless mesh/ad hoc networks.
- Efficiency of the whole system (including the network and RF efficiency).
- Testbed and solutions should be evaluated.
- Benefiting of the necessary security (authentication of users, peers, secured and trusted communications, privacy of users and communications) and Quality of Service (QoS) services.
- Interoperability (the basic technological solution may be supplemented by facilities provided by the public networks and their resources).
- System sharing (potentiality of the system to be shared by many entities).

2.2. Network architecture for extreme emergency services

In many extreme emergency scenarios, such as natural or manmade disasters, the rescuers may face difficulty using traditional legacy networks due to destruction or collapse of infrastructure in such events or in case of remote disaster locations. The nature of MANETs makes them suitable to be utilized in the context of an emergency for various rescue teams. Due to their flexibility and self-organization capabilities, MANETs are well suited for scenarios where certain network services such as message routing and event notification have to be provided quickly and dynamically without any centralized infrastructure like in an extreme emergency scenario. The network architecture consists of a mixture of leader nodes that may or not move in the disaster area and normal nodes that are mobile. The leader nodes are the hierarchically superior policemen, firemen, etc. that supervise the emergency operation, while the mobile nodes are normal emergency workers operating in the field of the disaster. Figure 1 depicts this wireless mesh network architecture that will serve as reference for the security framework to be described below.

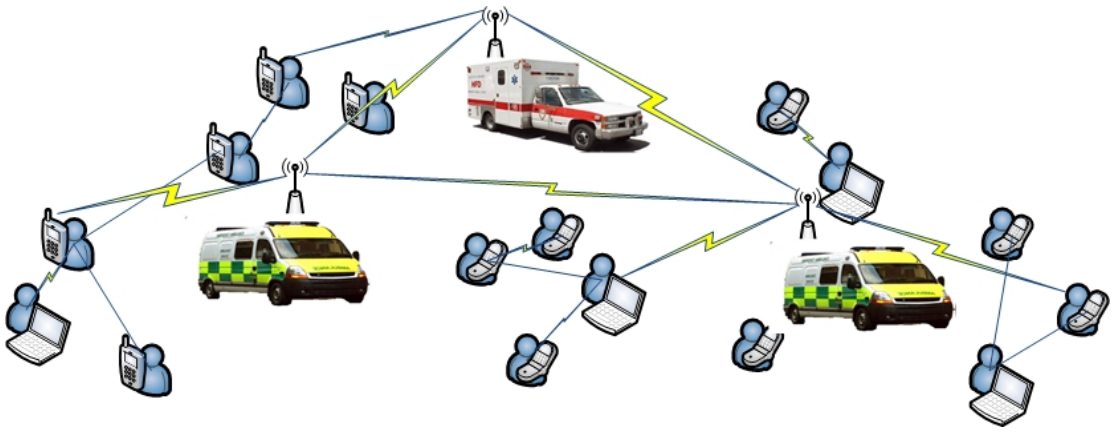

Figure 1: Network architecture for extreme emergency services

3. Security Framework for Extreme Emergency Scenarios

3.1. Vulnerabilities

The security of the mobile ad hoc based communications can be decisive in the effectiveness and efficiency of rescue missions in extreme emergency cases. Actually, the inherently vulnerable characteristics of MANETs make them susceptible to attacks and counter attacks might end up being too little too late. Traditional security measures are not applicable in MANETs according to [8]. Therefore, several kinds of attacks could be launched within a MANET by malicious nodes. We categorize generally the attacks against MANETs as follows.

- *Passive attacks:* adversaries obtain data exchanged between the nodes of a MANET without diluting the communication between them.
- *Active attacks:* adversaries attempt to change the behavior of the operational mechanisms. Instances of active attacks include spoofing, DoS, replication etc.
- *Internal/ insider attacks:* adversaries are authorized nodes that belong to the MANET. Obviously, these nodes know valuable and confidential information fact that makes them a more critical thread for the MANET.
- *External/ outsider attacks:* adversaries are nodes that do not belong to the MANET. The malicious nodes try to cause congestion, to prevent the normal usage of the services and applications and diffusing incorrect routing information.

- *Cryptography primitive attacks:* adversaries attack the various cryptographic primitives like authentication, confidentiality, integrity and cryptography key management protocols. Instances of these attacks include digital signature attacks, hash collision attacks, pseudorandom number attacks and security handshake attacks.
- *Non-cryptographic attacks:* adversaries attack without taking into account any vulnerability of the cryptographic algorithm. Example of this kind of attack is the well known man-in-the middle attack which is a kind of active eavesdropping when attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the adversary.
- *Denial of service (DoS) attacks:* adversaries attempt to make a computer resource unavailable to its intended users. Although, the means to carry out motives for and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent a service from functioning efficiently or at all, temporarily or indefinitely.
- *Impersonation attacks:* these attacks are categorized among the most critical attacks in MANETs. Adversaries can masquerade as trusted nodes when authentication mechanisms are not applied. As a result the impersonator can send false or corrupted information to other nodes and disrupt the appropriate function of the network.

3.2 Countermeasures

For the purposes of PEACE project we will develop a novel platform called PEACE Security Platform (PSP) proposed on [5]. This platform will be comprised of the following parts:

- *Trust establishment* [6]: covering all layers of operation of an ad hoc network, trust establishment provides the means to secure both the routing process and the applications intended to be performed in the network.
- *Intrusion detection*: the concept of the intrusion detection is very important for the security of the ad hoc network due to the fact that it can be a second wall of defense when prevention mechanisms have failed.
- *Key management*: the implementation of the key management mechanism is based on our trust establishment protocol. The latter is responsible for the creation, distribution and refresh of the asymmetric keys too.
- *Network layer security*: towards the development of the security in the network we will propose novel secure routing protocol based on our new routing protocol CHAMELEON.
- *Secure overlay*: our final work for securing the function of the emergency MANET will be the development of secure protocols of higher layers such as transport and application layers.

In Figure 2 we depict the architecture of PSP. The simulation of potential attacks and the application of countermeasures will be critical in order to evaluate the performance of our protocols.

3.2.1 Secure ad hoc routing

Due to the fact that there is no pre-deployed infrastructure in MANETs, nodes cooperatively form the network by agreeing to certain routing messages. Therefore, it is obvious that routing plays an important role in the appropriate function of a MANET. Due to the fact that routing is critical, security mechanisms have to be applied to protect the

function of existing routing protocols. However, existing routing protocols such as the reactive Ad hoc On-Demand Distance Vector Routing (AODV) [1] and the proactive Optimized Link State Routing (OLSR) [2] protocols are vulnerable to different kind of attacks. In this environment, a new hybrid routing protocol is proposed that is called, CHAMELEON [3]. CHAMELEON is an adaptive QoS routing solution, with improved delay and jitter performances, enabling multimedia communication for MANETs in extreme emergency situations. The protocol is designed to adapt its routing behaviour to the

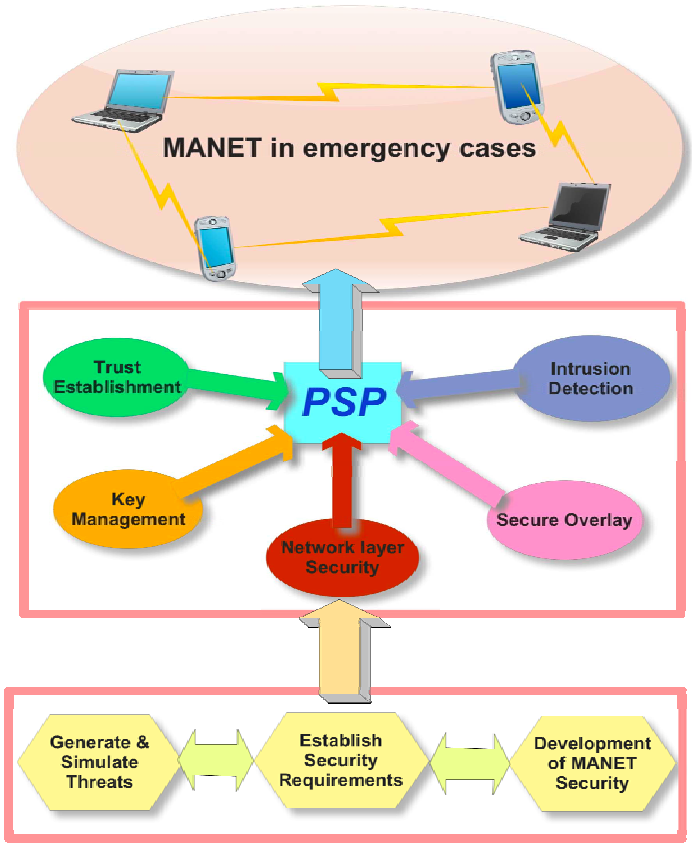

Figure 2: PEACE Security Platform Architecture

size of a MANET. The reactive AODV and the proactive OLSR protocols are deemed appropriate for CHAMELEON through their performance evaluation in terms of delay and jitter for different MANET sizes. Our choice to develop a new hybrid routing protocol based on AODV and OLSR has been taken due to the fact that studies, such as [4], have shown that these two protocols are the most attractive for a QoS hybrid solution.

The mobility of source, destination and relay nodes in MANET results in regular changes to the topology of the network. Hence, the routing paths from source to destination regularly changes, requiring a dynamic solution for both routing and QoS support as opposed to solutions for fixed networks [7]. In addition, the resources, such as battery power and link state, required for QoS support varies with time in MANETs. These time-varying low-capacity resources at each node would have to be accounted for in such measurements to provide the actual QoS limitations of considered paths and consequently, a route could be selected according to the required QoS guarantee. These new concepts entail further security issues. One possible threat would be a node that could unjustly reserve resources. Then, nodes could also provide false statistics to a sender thus disrupting the appropriate function. The secure version of CHAMELEON will be called S-

CHAMELEON. The latter will be able to defend MANET against the most well known attacks such as wormhole and blackhole attack.

3.2.2 Trust establishment

Trust establishment, as part of a complete security solution covering all layers of operation in an ad hoc network, provides the means to secure both the routing process and the applications intended to be performed in the network. The proposed trust establishment protocol enables the nodes of an ad hoc network to establish security associations among each other in a distributed and P2P manner. The basis of the protocol is a node-to-node security handshake using a network-wide key that every node is preconfigured with. The protocol is dynamic in the sense that the nodes' keying material is periodically renewed by a set of leader nodes in order to enhance the system security. In defining the protocol, no assumption has been made regarding the routing protocol in use or the nodes' communication capabilities (e.g. secure side-channel). In the initial stage, all the nodes are preconfigured with a private and public key pair and a network-wide key. When two nodes establish a security association between them, they also exchange information about which nodes each of them already trusts. The merged information is then forwarded by both nodes to their direct trusted neighbours in a secure way. Thus, a secure network overlay is constructed in a distributed manner, where all nodes are securely associated with each other.

The established trust relationships are timely bounded. Therefore, a refresh mechanism is periodically performed in order to issue new certificates and securely transmit them to the nodes, before those currently in use expire. A set of *leader* nodes is responsible for the renewal process. The leader nodes are assumed to be reliable and resilient to security threats. The proposed protocol falls in the category of authority-based protocols that use preconfigured keying material that is periodically renewed. However, in contrast to other works, it does not use threshold or advanced cryptographic mechanisms (e.g. Diffie-Hellman), while special communication capabilities like a secure side-channel are not needed either. This makes the protocol ideal for environments, where a fast and lightweight operation is required. Such scenarios are cases of emergency like forest fires, earthquakes and floods, where the network nodes are the firemen, policemen and medical staff. Interestingly, the above examples are, by definition, among the primary applications of the ad hoc networks. Furthermore, the assumptions made in the operation of the proposed protocol about the pre-configuration of the nodes with trusted keying material, and the existence of reliable leader nodes in charge of the renewal process suit perfectly in the setting of the emergency ad hoc networks. In these scenarios the networks consist of hierarchical groups of nodes that after leaving a common secure starting point, operate in the site of emergency. Therefore, the protocol presented in this paper mainly targets emergency ad hoc networks.

3.2.3 Secure P2P overlays

In general, the proposed framework for handling the P2P overlay serves different purposes and combines different technologies. It is a complicated multi-tasking scheme in which information flow combined with multiple real-time operations achieves the goal of creating and maintaining an efficient overlay. The general functionalities of the framework are structured and unstructured overlays in MANETs.

Efforts to create structured overlays using MANETs have shown that technologies such as DHT can be adapted for use in MANETs. They do however incorporate much more complexity into the network giving us the advantage of creating more complex applications compared to unstructured overlays.

Unstructured overlays have been covered by a wide range of research in MANETs. These include simple flooding protocols, and some more complex cross-layer approaches which involve modifying the routing protocol on the network layer. Unstructured overlays are much simpler to adapt for use within MANETs due to the similar topology which both share. The aforementioned studies above have demonstrated that unstructured overlays which try to follow the underlying network topology are more successful in situations where lookups are not so heavily used and where 100% search success rate is not needed to be guaranteed as they tend to be less efficient when searching the network. Therefore we will initially look at both a structured and unstructured approach. The major challenges of the P2P framework are the following:

- *Node join/leave/failure*: The dynamic nature of peers imposes several problems regarding both connectivity and optimality of the resulting overlay in a secure manner.
- *Connectivity maintenance*: The most fundamental function of the P2P overlay is to maintain connectivity between any pair of nodes that may decide to initiate a session over it.
- *Cluster formations*: As scalability arises as a main problem in ad hoc networks, clustering is the simplest and most feasible solution to address this issue. Clustering serves at topping down the responsibilities by creating relatively small functional units-clusters.
- *Peer discovery*: One of the basic functionalities of the P2P overlay is fast peer discovery, especially when it comes to data sharing. An inefficiently formed overlay may result in far from optimal paths for data exchange paths.

One of the many fields of the decentralized computer architecture which might be quite important is the SOS Service. This Service describes the ability of various security and protection units such as Police, Fire Department and Civil Protection to cooperate when necessary in order to prevent or suppress a disaster that might endanger human lives and properties whether private or public. Each one of those units may have their own telecommunication equipments but if there is a lack of cooperation and optimal resource handling the result might not be good enough. A P2P system might be the answer to the optimal cooperation problem, because it utilizes the existing equipments, works with peers that might be heterogeneous and also keeps a strict, uncompromised hierarchy between all participants. The Figure 3 below presents the above idea using a SuperNode P2P network architecture.

The SuperNode is in charge of the communication to other SuperNodes for picking up information on how the situation is developing. After communicating to every other SuperNode, receives instructions on how to proceed and passes these instructions along to its peers. The same thing occurs to the other SuperNodes as well, except the Civil Protection SuperNode which is in charge of the whole operation. From the architecture aspect there are a few things that need to be taken under consideration. The SuperNode P2P network approach is a partially decentralized P2P architecture. This is based on the fact that not all peers are equal in capacity, bandwidth and capabilities in general. Therefore some of them play a more important role to the overall case. One of the major tasks of SuperNodes is to act as local central indexes. For example they may store parts of the network's Distributed Hash Table (DHT) holding all essential information concerning peers.

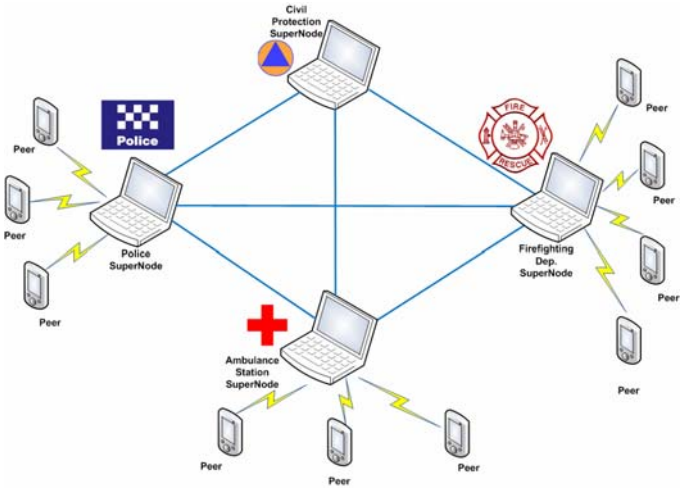

Figure 3: P2P Voice Communications for the support of emergency communications

3.2.4 Multicast secure routing in ad hoc networks

One specific aspect of the emergency deployment is the availability of allowing group communications. During emergencies the same communication services will be required, but the personnel utilizing them may differ. Groups shall contain members from multiple services and/or multiple geographic units.

Within a wireless medium, it is crucial to reduce the transmission overhead and power consumption. Multicasting can improve the efficiency of the wireless link when sending multiple copies of messages by exploiting the inherent broadcast property of wireless transmission. Hence, reliable multicast routing plays a significant role in MANETs. This part deals with problems of multicast routing in ad hoc network and secure communications. Designing multicast routing protocols in an ad hoc network is a complex problem, as group membership can change, and network topology can highly evolve causing links failure. In addition, the limited bandwidth availability together with the limited energy resources make the design of a multicast routing protocol a challenging one.

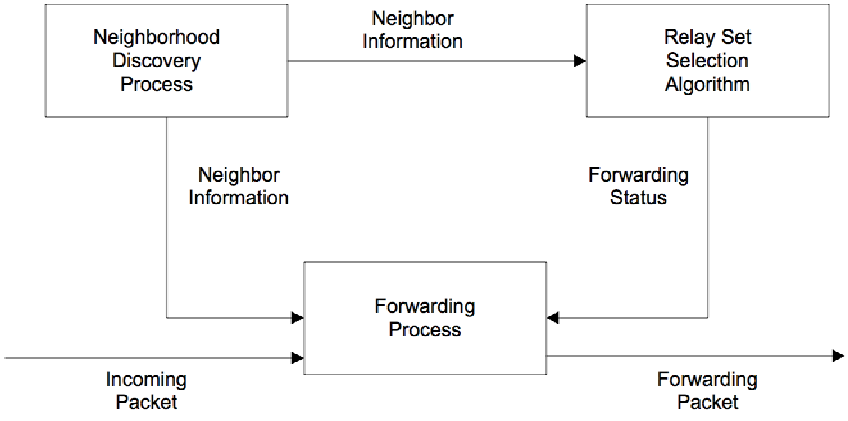

Figure 4: SMF node architecture

In contrary to the wired networks, there is no standard protocol for multicast routing in MANETs. Several protocols were defined and published as drafts but expired for the great majority. In the context of the PEACE project, a routing multicast solution based on SMF [9] will be implemented and deployed on real test-bed.

MANET unicast routing protocol designs have demonstrated efficient mechanisms to flood routing control plane messages in the ad hoc network such as the optimized flooding

technique of OLSR. SMF extends efficiently the flooding concept to the data forwarding plane to provide a multicast forwarding capability. In Figure 4 we show the SMF node architecture.

4 Conclusions

The aim of this paper is to address the key research challenges which target a new enabling technology for extreme emergency scenarios and how the PEACE project aims to address these goals. In order to achieve secure MANET based multimedia communications we propose a novel suite of protocols called PSP. The architecture of PSP will be comprised of (i) a trust establishment protocol which covers all the layers of operation of the MANET, (ii) intrusion detection systems in each node which will be installed as a second wall of defence when prevention mechanisms have failed, (iii) a key management process which is implemented by the trust establishment protocol, (iv) the network layer security module which will built on the CHAMELEON protocol and (v) a secure P2P overlay mechanism for securing the function of the emergency MANET at higher layers.

Acknowledgments

The authors wish to acknowledge the support of the ICT European Research Programme and all the partners in PEACE: PDMF&C, Instituto de Telecomunicaes, FhG Fokus, University of Patras, Kingston University London, Thales, Telefonica, CeBit.

References

[1] C. Perkins and E. Royer, “Ad hoc on-demand distance vector routing,” In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1997, pp. 90–100.
[2] T. Clausen and P. Jacquet, Eds. 2003 Optimized Link State Routing Protocol (Olsr). RFC. RFC Editor.
[3] T. A. Ramrekha and C. Politis, “An adaptive qos routing solution for manet based multimedia communications in emergency cases,” in ICT Mobilight Conference, Athens, Greece, 2009.
[4] A. Huhtonen, “Comparing aodv and olsr routing protocols,” in Seminar on Internetworking, Sjkulla, 2004.
[5] E. A. Panaousis and C. Politis, “Securing ad hoc networks in extreme emergency cases,” in World Wireless Research Forum meeting, Paris, France, 2009.
[6] C. Papageorgiou, K. Birkos, T. Dagiuklas, S. Kotsopoulos, Dynamic Trust Establishment in Emergency Ad Hoc Networks, accepted at the 5th International Wireless Communications and Mobile Computing Conference (IWCMC), 2009.
[7] D. D. Perkins and H. D. Hughes, “A survey on quality-of-service support for mobile ad hoc networks,” Wireless Communications and Mobile Computing, 2002.
[8] F. Anjum and P. Mouchtaris, Security for Wireless Ad–hoc Networks. John Wiley & Sons, 2006.
[9] SMFD Team - 2007 - internet draft, IETF Network Working Group, “Simplified Multicast Forwarding for MANET.