manuscript No.
(will be inserted by the editor)

Security Model for Emergency Real-Time Communications in Autonomous Networks

Emmanouil A. Panaousis · Christos Politis · Konstantinos Birkos · Christos Papageorgiou · Tasos Dagiuklas

Received: 10 March 2010 / Accepted: 21 April 2010

Abstract Towards the proliferation of architectures, tools and applications that have the potential to be used during an emergency rescue mission, we present a framework for emergency real-time communication using autonomous networks, called emergency Mobile Ad-hoc Networks (eMANETs). By eMANETs we refer to networks that are deployed in emergency cases where default telecommunications infrastructure has failed. Our goal is to design a security framework that will secure real-time communications during emergency rescue scenarios. The proposed framework consists of a secure routing protocol, intrusion detection provision and security extension for real-time communications using peer-to-peer overlays. We envisage that the results of this work will aid and serve the needs of any society against any event that threatens serious damage to human welfare or to the environment.

Emmanouil A. Panaousis · Christos Politis
Kingston University London, Wireless Multimedia & Networking (WMN) Research Group, Penrhyn Road, Kingston upon Thames, KT1 2EE
Tel.: +44 (0)208417 7025
Fax: +44 (0)20 8417 2972
E-mail: {e.panaousis, c.politis}@kingston.ac.uk

Konstantinos Birkos · Christos Papageorgiou · Tasos Dagiuklas
University of Patras, Patras, Greece
Tel: + 302610996466
E-mail: kmpirkos@ece.upatras.gr, xpapageo@ceid.upatras.gr, ntan@ece.upatras.gr

Keywords Security · emergency · MANET · VoIP · routing · P2PSIP

1 Introduction

An extreme emergency situation refers to unpredictable events such as natural disasters or catastrophes (e.g. flooding, earthquake, terrorist attacks) and predicted major events, such as international summits for instance G8, sporting competitions (Olympic Games, Football World Cup, Formula 1 Grand-Prix) or itinerants (bicycle tour, Car Racing), and the various gatherings of crowd (festivals, concerts). In such events, existing telecommunication (e.g. PSTN, GSM/GPRS, etc) may either get collapsed or congested. In this case, it is important to design and develop alternative means of communication infrastructure allowing the emergency workers to communicate in a reliable and efficient manner.

Due to the absence or collapse of the default infrastructure, autonomic networking is one of the few options for communication among them. We refer to this special class of mobile ad hoc networks (MANETs) as emergency MANETs. Given the urgency of the situations that emerges in such scenarios, voice communication is a primary requirement. Furthermore, the sensitive nature of the transmitted information highlights the need for a secure and robust communication system.

Wireless mobile computing has introduced new classifications of communicational and computational activities that rarely arise in wired or static environments. Applications and services in a mobile wireless environment can be a decrepit link too. Additionally, in these environments there consistently exist software agents

or proxies running in intermediate nodes to serve the requirements for adequate communication links. In this setup, potential malicious entities can launch different kind of attacks to gain access to confidential and private information, to disrupt the undergoing communication links or to make some profit by behaving in a selfish way.

By ensuring confidentiality any unauthorised disclosure of the communications between two or more parties is prevented; namely eavesdropping is avoided. By ensuring integrity the data cannot be manipulated during the transmission. Indeed, integrity guarantees that the recipient of some data will realise if any alteration of the originator's message has been done. Additionally, integrity of the data includes the authentication of the user source. Authentication guarantees that the MANET participated entities are not pretenders. In fact, authentication gives solution to the problem of impersonation. Lastly, by ensuring availability users are always sure that information and resources are available.

In this article we propose a security model[1] for real-time communications in emergency MANETs, consisting of solutions of a secure routing protocol, intrusion detection provision and security extension at the protocol implementing real-time communications using peer-to-peer overlays.

The rest of the article is organised as follows. In section II, we discuss related work that has been done regarding secure models for distributed wireless networks. In section III, we present our proposed security model designed within the context of emergency mobile ad hoc networks. Section V concludes this article by summarising the main points of the security model.

2 Related Work

Some previous works have focused on the design of security models for MANETs. However, according to our knowledge, none of them has proposed any unified security model for MANETs in emergency cases. In the following we summarise some of the noteworthy related works within the context of trustworthiness in MANETs.

In (Sun et al., 2006) the authors propose a model that evaluates the trust in distributed networks. They especially address the problem of trust, develop trust metrics with physical meanings and build trust models to support trust propagation through third parties. They additionally present attacks against the aforementioned trust evaluation and they discuss how these can be prevented. Finally, a trust management system for distributed networks is proposed while a demonstration of the model in ad hoc networks is carried out. The latter assists route selection and detection of any malicious activity. However, this solution does not consider security for the overlay that has to be established among the different peers in our scenario.

The architecture presented in (Martigon et al., 2006) is a unified solution for access control and key distribution in wireless mesh networks. Its dependence on a semi-static backbone network formed by mesh routers makes it unsuitable for mission-critical networks in which such a backbone is a rather limiting factor. SCAN (Yang et al., 2006) is a network-layer approach that protects routing and data-forwarding. Through token renewal, collaborative monitoring and token revocation, nodes can detect and react to malicious ones. Although effective, the proposed solution does not cover other aspects of MANET security and it does not incorporate any cryptographic features.

The described approaches are applicable to general purpose MANETs and they do not meet the strict requirements of real-time emergency communication networks. Furthermore, they do not address the issue of security provision for a P2PSIP overlay that lies above the physical topology. Consequently there is a need for a new unified approach.

3 Security for emergency real-time communications in autonomous networks

In order to provide real-time communications in emergency environments autonomous networks can be considered as a possible network infrastructure solution. These must be deployed and operate in a self-organised manner regardless of topology changes, environment alterations, link breaks or network disruptions. They should additionally provide audio and video communication among the nodes that comprise the network, with Quality of Service (QoS) restrictions to be taken into account.

All the above must be implemented in a robust and secure way. Towards this goal we propose a security model entailing all the aspects of operation of such networks. Our idea is based on the concept that we illustrate in Figure 1. Namely, a three-tier communication model is considered, where: (i) the *Tier2* consists of the eMANETs where each group will be initially made up of rescuers from a particular emergency team, (ii) the *Tier1* or else the *Supernode Mesh Network* consists of semi mobile nodes compared to *Tier2* nodes, and (iii)

[1] This work is part of the EU FP7 ICT-SEC PEACE project. For more info visit: http://www.ict-peace.eu/.

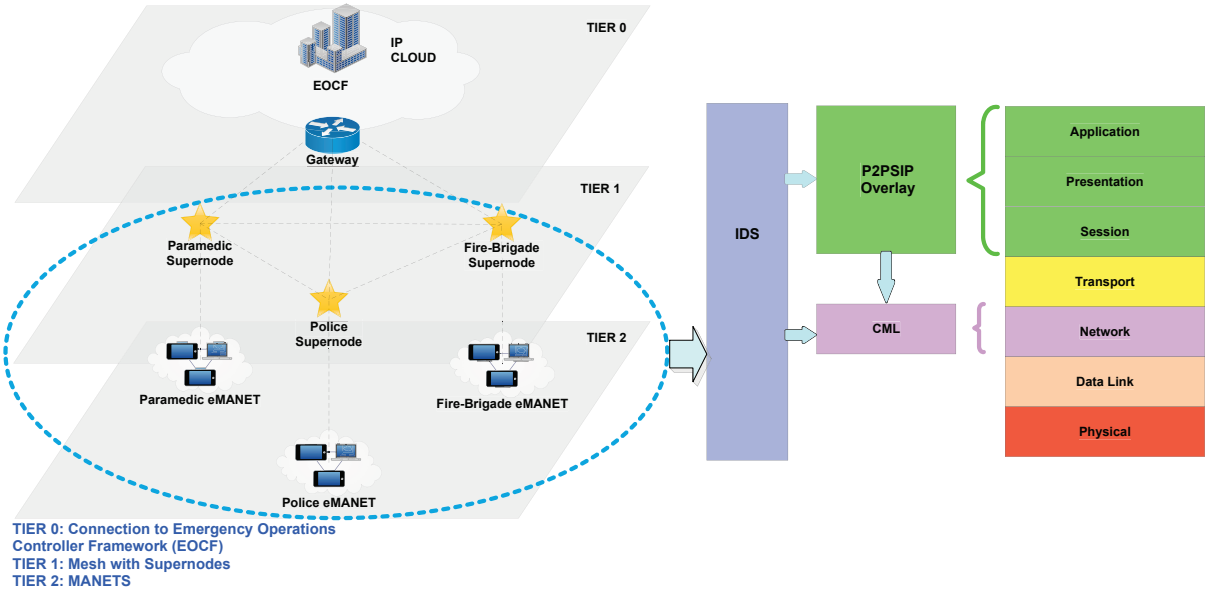


Fig. 1: Communication for emergency real-time communications.

the *Tier0* defines the connection between the MANET for the rescuers and the IP cloud via a gateway.

The super nodes have the following characteristics and responsibilities:

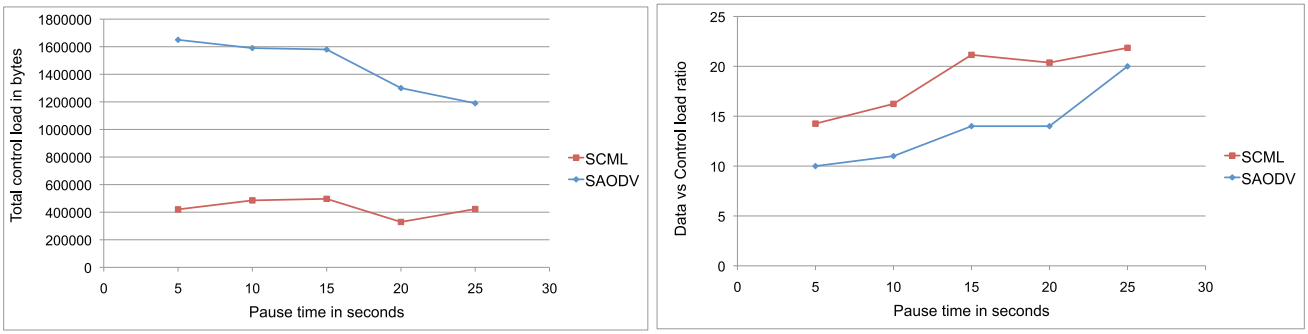
- semi-static behavior,
- provision of network connectivity within the disaster area,
- interconnection to multiple Tier-2 nodes,
- construction and maintenance of a secure overlay that is built among Tier-1 and Tier-2 nodes,
- initiation of a SOS service within a specific disaster area.

The semi mobility of these nodes should provide easy IP route discovery and IP route maintenance for both the *Tier2* nodes and the*Tier1* super nodes. The key elements of the proposed security model for emergency real-time communication, which are described in detail in the following subsections, are (i) provision of secure routing paths among the rescue workers when the routing tables should be adaptive to the topology changes, taking also into account the strict QoS requirements of the emergency communications sessions, (ii) establishment and maintenance of secure overlays among Tier-1 and Tier-2 nodes for real-time communication, and (iii) an Intrusion Detection System that handles various types of attacks from the physical up to application layer. It is worth noting here, that in this article we stress on network and P2PSIP security. Physical and link layer security are considered within the realm of intrusion detection systems which acts as a second wall of defense when conventional security solutions have failed or node capture attacks have succeeded to intrude in the MANET. Also, it is assumed that well-known standards such as IEEE 802.11i can be used as first line of defense for those two layers but they have not been examined further in this article.

3.1 Secure Routing

Routing is a critical function of any network either wired or wireless. Due to the fact that wired networks do not appear any kind of mobility and they typically have high available bandwidth, the routing protocols designed for them are apparently different than the wireless routing protocols. Especially, in MANETs resource constraints issues have to be taken into consideration before any routing solution is proposed. In addition, mobility and the fact that there are non trusted entities in advance within the network, stimulate spiritually an attacker to cause devastating damage to the MANET communications. In MANETs, routing protocols (Chen and Heinzelman, 2007) should be designed so that intermediate nodes will forward legitimate packets towards a destination as far as the latter is out of the transmission range of the source. Thus, network researchers and engineers have to design and develop appropriate routing protocols.

Within the context of eMANET multimedia communications operating within a pre-defined disaster area (referred in this article as the Critical Area), we have designed and developed a novel hybrid and adaptive routing protocol called ChaMeLeon (CML). The proto-



(a) The control load in bytes for SCML and SAODV.

(b) The ratio of data vs control load for SCML and SAODV.

Fig. 2: Comparison of SCML against SAODV.

col is a work in progress (Ramrekha et al., 2010) within the realm of IETF. The main concept behind CML is the adaptability of the utilized routing mechanism towards changes in the physical and logical state of the network so that the overall performance of the routing algorithm is improved. The importance of such an approach resides in the fact that the nodes in eMANETs have to provide a certain level of routing Quality of Service (QoS) to support multimedia communications but concurrently to cope with limited resources.

In the case of extreme emergency operations, the number of rescuers within the Critical Area (CA) is likely to vary whenever rescuers join or leave the operations according to the severity of the situation. In the case where an eMANET is deployed, the total number of nodes in the network will vary as the number of participating devices join or leave the network. In addition, the battery exhaustion of lightweight communicating devices used by rescuers might stipulate another reason for changes in eMANET sizes. Hence, the eMANET nodes have to be able to efficiently and effectively route data packets considering such extreme scenarios. Thus, for small networks, CML routes data proactively using Optimized Link State Routing Protocol (OLSR) protocol (Clausen and Jacquet, 2003) whereas for larger networks it uses the reactive Ad hoc On-Demand Distance Vector (AODV) protocol (Perkins et al., 2003) mechanisms so that the overall routing performance is improved as supported by our results. It is also important to note in the sphere of multimedia communications supported by eMANETs, the routing protocol efficiency can be quantitatively defined using routing QoS metrics such as delay and jitter (delay variations). These will also be used in this paper to define the efficiency of discussed protocols. For a more detailed description of CML, the readership is encouraged to refer to (Ramrekha et al., 2010).

Secure operation of the MANET routing protocol is crucial due to the absence of a fixed infrastructure. Nodes may cooperate virtually with any node including adversaries. The latter can disrupt the route discovery and data forwarding functions. Disruption of the route discovery will cause systematic problems to the data flow. The launch of attacks that target the route discovery phase of a routing protocol is done by obstructing the propagation of legitimate queries and routing updates. In order to prevent such attacks it is important for the receiver node to verify the *authentication* of the sender and the *integrity* of the data. Furthermore, *confidentiality* is critical to prevent confidential information of the packet payload to be seen by any malicious node. In (Argyroudis and O'Mahony, 2005) authors discuss the most of the secure routing protocols by classifying them into five categories: solutions based on asymmetric cryptography; solutions based on symmetric cryptography; hybrid solutions; reputation-based solutions; and a category of add-on mechanisms that satisfy specific security requirements.

As CML does not include any security extensions we have proposed the use of IPSec[2] in (Panaousis et al., 2010) to provide confidentiality, authentication and integrity. The choice of IPSec in a MANET environment is aligned with the work done in (Hegland and Winjum, 2008). The protocol does not introduce unaffordable time and space overhead to CML while, it outperforms the most of the proposed secure routing protocols. The latter use asymmetric cryptographic algorithms which are 1000 times slower than symmetric in addition to the fact that for low power devices such as PDAs the battery consumption is too high when they are used. Furthermore, most of these works secure only one specific protocol giving less flexibility in cases where

[2] Security Architecture for the Internet Protocol (Kent and Atkison, 1998).

we want to utilise an adaptive MANET routing protocol such as CML.

For the case of MANETs[3] the transport mode of the IPSec protocol has been proven more suitable than the tunnel model according to the bibliography (Hegland and Winjum, 2008), due to the power limitations of the devices. Specifically, SCML uses an hybrid version of IPSec that utilises the Authentication Header (AH) mode to provide authentication and integrity of the IP header of the packets and the Encapsulated Security Payload (ESP) mode to provide confidentiality of the packet payload. Towards this direction, the Advanced Encrypted Standard (AES) (Daemen and Rijmen, 2002) algorithm is used to encrypt the data while the Message Digest 5 (MD5) is used with a symmetric key as the Hash Message Authentication Code (HMAC-MD5) to provide authentication and integrity.

In this article, we have included some preliminary results that compare the performance of SCML in terms of total control load and ratio of data versus control load, with well known Secure AODV (SAODV) (Zapata, 2002). This protocol uses digital signatures, asymmetric encryption keys and hash chains providing characteristics such as integrity, non repudiation of the routing data and authentication of the nodes. Actually the SAODV protocol takes advantage of the pure routing functionality of AODV while it adds security mechanisms on top of the conventional protocol. The simulation results illustrated in Figures 2a and 2b show the control load and the ratio of data against control load for different pause times namely for different mobility models. We notice that the routing load of SCML is significantly lower than SAODV's whilst the SCML is delivering more data per control load than SAODV. This happens due to the lightweight compare to SAODV, mechanisms of symmetric cryptography that SCML uses. On the other hand, the security level of SCML is enough when AES is used and is comparable with asymmetric solutions in terms of security strength.

3.2 Secure P2PSIP

As we have mentioned in eMANETs legitimate nodes are willing to establish VoIP communication paths to cooperate towards the accomplishment of their rescue mission. Due to the infrastructureless nature of the emergency ad hoc networks, the establishment of the voice sessions must be carried out in a autonomous fashion. Thus, the P2PSIP (Baset et al., 2007) protocol is included in the proposed security model. The P2PSIP protocol is the peer-to-peer version of Session Initiation Protocol (SIP) (Rosenberget et al., 2002), which is the de facto standard for voice-over-IP (VoIP) communication over wireline networks.

P2PSIP, as described in (Baset et al., 2007), does not rely on central servers in order to store and retrieve the users registration information. This information is distributed among the network peers and it is obtained by queries forwarded through a peer-to-peer overlay network, which can be defined as a set of logical connections interconnecting the participating peers above the physical network topology. Each peer maintains a finger table used and a neighbour table that are used for lookup and data replication along with overlay maintenance, respectively. The lookup service is implemented by a Distributed Hash Table (DHT) functionality that is integrated into the overlay architecture.

IETF's P2PSIP working group (IETF P2PSIP WG, 2010) and other independent contributors have produced a series of drafts describing potential P2PSIP implementations. The most thoroughgoing is the Chord-Resource Location and Discovery (Chord-RELOAD) base protocol (Jennings et al., 2009). In the P2PSIP implementation within the context of the proposed security model we adopt the basic characteristics outlined in this draft. However, we extend the Chord-RELOAD protocol in order to make it more appropriate to be utilised within the emergency situations' environment. Below, we first give a brief description of the basic concepts of the Chord-RELOAD draft and then we present the details of our extensions.

3.2.1 Chord-RELOAD

In the original Chord-RELOAD base protocol a peer must first follow an Enrolment and Authentication or else E&A process in order to become a member of the overlay, which is handled by a designated E&A Server. The Join process defines all the necessary actions for neighbour discovery, establishment of logical connections and data transfer between peers. After a successful E&A process and before entering the core Join phase, the joining peer (JP) attempts to discover its overlay neighbours through a designated Bootstrap peer. The JP is then attached to its admitting peer (AP), which is the JP's immediate successor in the overlay, through the Bootstrap peer. Next, the JP joins the overlay by exchanging the respective request and response messages. Finally, an Update process finalizes the whole procedure after which peers JP and AP consider each other as logical neighbours.

Leaving the overlay must guarantee that the overlay routing functionalities remain intact and connectivity is

[3] the same holds for eMANETs.

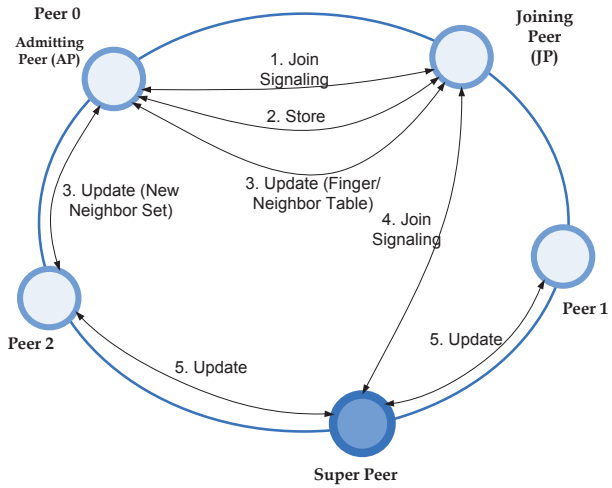


Fig. 3: Join process in Chord-RELOAD.

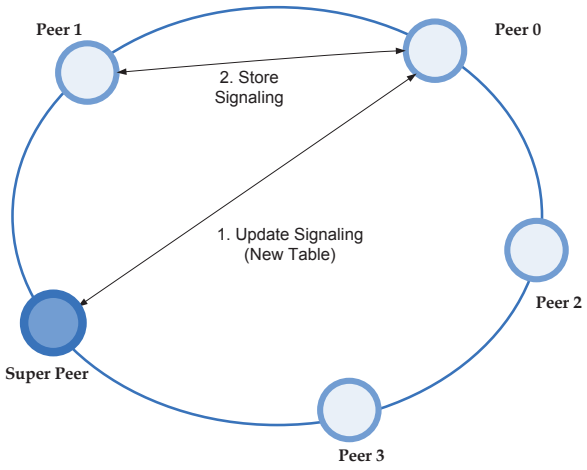


Fig. 4: Update process in Chord-RELOAD.

maintained. The leaving peer (LP) informs its overlay neighbours by sending them a Leave message. These peers remove LP from their tables and inform their own neighbours so that the information is propagated to all the affected peers in the overlay.

The Chord-RELOAD protocol describes a stabilisation process, according to which the overlay structure is updated periodically or in response to peers entering or leaving the overlay or changes to the network topology. This process is implemented in a distributed fashion by exchanging messages that inform the peers about the changes and, possibly, force them to reposition themselves inside the overlay network.

3.2.2 Hierarchical Chord-RELOAD

In the *Hierarchical Chord-RELOAD (HCR)* the peers are organised in a hierarchical manner. Apart from the ordinary peers, there are some super peers, i.e. peers with advanced capabilities and extended functionalities that have a more important role. They are actually responsible to authenticate incoming peers in the overlay and accomplish join requests. Furthermore, they initiate any possible updates and they carry out a new process, called *Refresh*, that aims at delivering new keying material to participating peers. In the following subsections the proposed extensions are presented in detail.

Join. The Join process is undertaken between the JP and a super peer. After its completion, the super peer informs the JP about its finger table and neighbour table by sending an UpdateReq message. Moreover, the super peer sends multiple UpdateReqs to all the peers affected by the entrance of JP in the overlay. This is a very important difference compared to the original

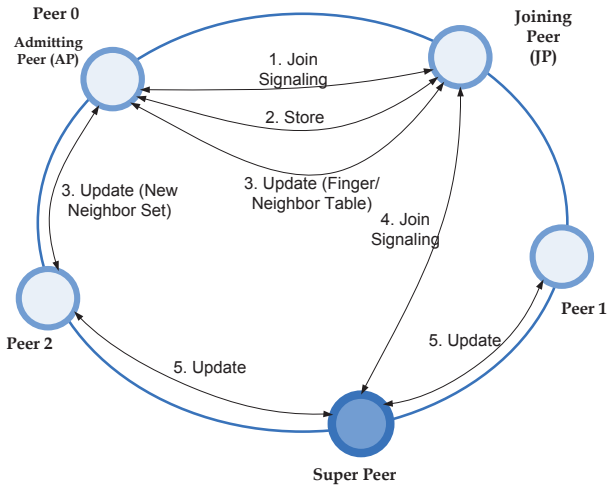


Fig. 5: Join process in the Hierarchical Chord-RELOAD

protocol, where each peer sends Update messages that are flooded in the overlay. This Join process enables the JP to be part of the overlay for a specific time period. Before this period expires, the JP must receive an updated version of its keying material from a super peer following the Refresh process described below. Details of the Join process appear in Figure 3.

Leave. In the Leave process, as we illustrate in Figure 5 the leaving node directs the Leave message only to the super peer. After removing this peer from its finger and neighbour table, the super peer informs any other peer affected by its exit via an UpdateReq message. It also sends StoreReq messages to properly order essential data transfer.

Update. The basic difference in the Update process is that only super peers can initiate updates and they di-

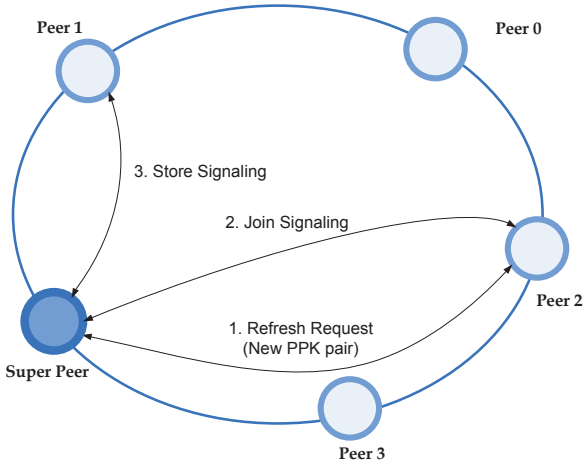


Fig. 6: Refresh process in the Hierarchical Chord-RELOAD

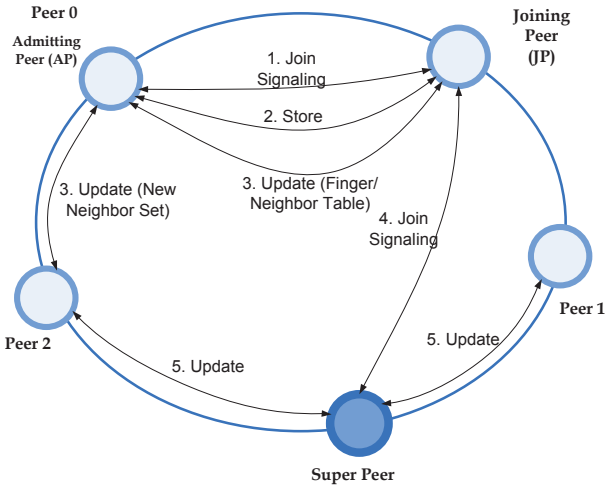


Fig. 7: Join process in the Semi-Hierarchical Chord-RELOAD

rectly inform any peer that needs to be updated. The Update process for the HCR protocol is depicted in Figure 4.

Refresh. Security considerations necessitate the periodical refresh of the peers' security credentials. The super peers are responsible for this mechanism (Figure 6). When a super peer detects that a peer's p_i PPK pair will expire in time less than a predefined critical margin, it transmits a RefreshReq message destined to p_i. When peer p_i receives the RefreshReq message, it produces a new PPK pair and sends a JoinReq to the super peer containing its new public key, so the super peer informs (via a StoreReq message) all the peers about the new version of p_i's public key.

The basic assumption for the Refresh process is that each node is preconfigured with a system-wide master key MK and a specific public/private key PPK pair. The MK is used to authenticate the joining peer in a secure manner via symmetric cryptography. The PPK is the credential used for authentication, message secrecy and confidentiality under the asymmetric cryptography notion. The Refresh process is included in protocol extensions proposed in (Birkos et al., 2010) which constitutes a work in progress within the realm of IETF.

3.2.3 Semi-Hierarchical Chord-RELOAD

The *Semi-Hierarchical Chord-RELOAD (SHCR)* protocol implements a flexible mechanism that allows a joining peer JP to establish connections and immediately become part of the overlay immediately. The role of the super peer as the main entity for authentication still holds but the constraint of the first contact point is relaxed in order to offer fast integration into the overlay.

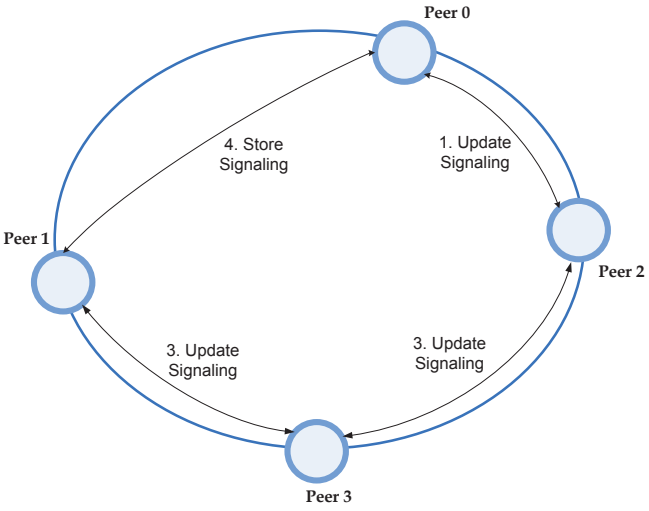


Fig. 8: Update process in the Semi-Hierarchical Chord-RELOAD

More specifically, a JP is directly attached to the first peer it encounters in the network. In fact, the JoinReq message is directed to this peer. The main difference is that the Join handshake that follows leads to a temporary acceptance of the JP as a legitimate peer. The JP becomes an active part of the overlay and can serve as a relay for overlay routing, forward queries and access stored data items. Nevertheless, all peers that have established logical connections with the JP know that these connections are timely bounded and they wait for an authentication from the super peer. If the proof of authentication is not received within a specific time interval, the connections are considered

invalid and the overlay is self-reconfigured without the JP.

The super peer learns that the JP is part of the overlay by the propagation of the UpdateReq messages that follow the Join process. The credentials carried by this message (public key and master key) enable the super peer to authenticate the JP and informs it with a JoinResp message that contains a certificate of the successful authentication. Then, the JP informs its logical neighbours via UpdateReq messages. The latter contain a copy of the certificate signed by the super peer. This message and the accompanying certificate designate the completion of the JP's join process. Consequently, any connection is considered valid and secure.

As far as the Leave and Update processes are concerned, they are identical to the ones described in the original Chord-RELOAD protocol and the Refresh process is the one presented in the HCR protocol. Signaling flows regarding the Join and Update processes in SHCR are presented in Figures 7 and 8 respectively.

3.2.4 Secure SOS Service provision

One of the main functions of the secure P2PSIP overlay in emergency situations is the provision of *SOS service* among emergency workers in a fast and efficient way. Emergency workers often need to respond to urgent requests and come to the aid of their colleagues in the disaster area. Sometimes emergency workers that belong to different groups need to cooperate according to the operational characteristics of the response to the incident. SOS service enables a group leader to cast a SOS message to multiple workers that are in physical proximity.

By means of a neighbour discovery mechanism, the group leader selects a set of emergency workers the SOS message will be addressed at. Workers included in this set map to peers in the overlay that are subject to different super peers. For those peers that belong to the same group with the super peer that initiates a SOS request, the SOS message is directly delivered via the overlay routing mechanism. For peers belonging to different groups, the message is transferred to the super peer of each group which in turn unicasts it to the recipients.

3.2.5 Discussion

The proposed P2PSIP overlay schemes are characterised by a distributed self-configuration logic. Although security considerations are extensively described in the IETF's drafts 6, there is none single solution that addresses every aspect of P2PSIP security. Efforts mainly

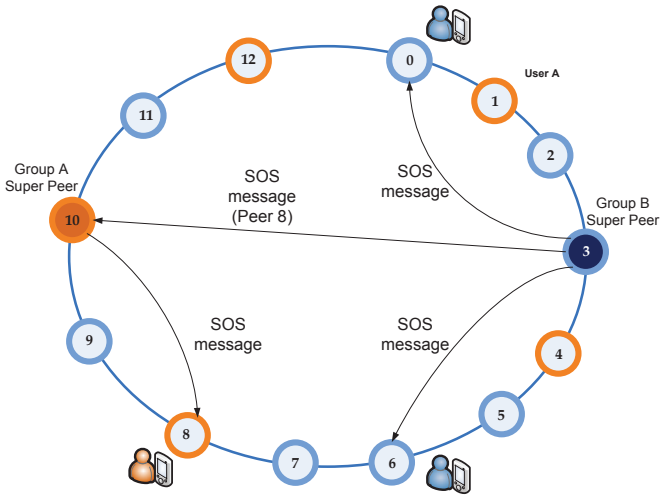


Fig. 9: SOS Service provision via the secure P2PSIP overlay

focus on the security of the overlay routing and the integrity of the data stored in the DHT.

HCR and SHCR provide two alternative approaches with different functional characteristics, complementary to the proposed drafts. The adoption of each approach depends on the security requirements and also on the intrinsic networking characteristics of the platform the P2PSIP overlay architecture will be deployed in. For example, the ad hoc nature, mobility constraints and strict security requirements of an emergency communications system, are factors that need to be taken into consideration.

A major difference between those three protocols is observed in the Join process. In the original RELOAD protocol, the Join process is directed at JP's first successor in the overlay which is usually an ordinary peer. On the contrary, in HCR, Join is in super peer's exclusive responsibility. An intermediate approach is adopted by SHCR since Join can be performed in conjunction with the first peer encountered in the network but JP is a full part of the overlay only after approval by the super peer. The usage of JP's first successor as an admitting peer for the accomplishment of the Join process as defined in (Jennings et al., 2009) constitutes a weak point an attacker may take advantage of in order to launch a man-in-the-middle attack and compromise the overlay construction. Better control is achieved in HCR since Join is in super peer's exclusive responsibility. The approach followed by SHCR reduces the overhead produced by the Join process and is suitable for ad hoc networks but it makes the system vulnerable in the time interval between the first Join and the certificate reception. In general, the degree of decentralisation

determines the trade-off between security risk and performance.

Complexity in terms of signalling overhead is also different. In HCR, low signalling overhead is achieved since during Updates the super peer directly informs every peer, avoiding the UpdateReq message flooding. Although SHCR facilitates the fast integration of JPs in the network, it yields in increased signalling overhead due to the distributed Update mechanism and the additional signalling produced in the second phase of Join process.

Availability is the main drawback of HCR because the super peer is involved in every action related to peers joining/leaving the overlay and overlay maintenance. A super peer failure will eventually result in malfunctioning and may facilitate certain types of DoS attacks. SHCR is more robust since the temporal failure to reach a super peer does prevent peers from joining and neither obstructs overlay maintenance. What limits the availability of RELOAD-based network is the dependence on the E&A Server. However, the inexistence of a super peer equivalent does not affect availability after a peer has joined.

Contrary to the RELOAD protocol, both HCR and SHCR include a key refresh mechanism that limits the vulnerability of the system through time and makes attacks based on cryptanalysis almost useless. In the drafted protocol the initial PPK pair is chosen by the user whereas in the proposed ones it is preconfigured. The second option is more appropriate for non-open-access networks like in the extreme emergency communications. This PPK pair is used for providing message secrecy by means of asymmetric cryptography.

Finally, scalability is an important factor directly related to security. Types of attacks like malicious churn, massive queries or peers massively joining the overlay that depend on the level of scalability may arise. SHCR is more scalable than the others since it keeps the distributed approach of Chord-RELOAD while relaxing the constraint for a priori authentication through a super peer. HCR is less scalable since the super peer is involved in every process related to overlay maintenance and topological changes. Therefore the minimum number of super peers versus the number of participating peers to sustain a secure and fully functional p2p overlay needs to be studied.

3.3 Intrusion detection

Security in the most enterprise environments supports in-depth defence mechanisms. This is based on the concept that if an adversary penetrates one of the system's defence layers, he will not be able to cause much dilapidation due to the provided protection by the other defence layers. In this context, *Intrusion Detection Systems* (IDSs) constitute a second line of defence that is usually activated when the attackers have already penetrated the perimeter defences. In fact, an IDS is in charge of detecting malicious activity by monitoring events in a computer system and detecting attempts to misuse preventive mechanisms or leverage the weaknesses of preservative mechanisms.

An IDS designed for an autonomous network must be able to operate efficiently in a mobile wireless environment. The fact that mobile networks do not communicate as frequently as their wired counterparts, makes the case more difficult for the IDSs to collect audit data and consequently recognise a malicious activity. Due to the nature of the eMANETs, where the proposed security model targets to, a peer-to-peer IDS architecture is considered. In this context, every node has its own local detectors to detect malicious activities. To improve the performance of the detection, the nodes exchange information about their observations. This is a cooperative IDS approach where each node monitors the traffic that reaches him either as relay or as final destination. When a malicious activity is detected, the rest of the nodes within the eMANET are informed about it. However, this can be exploited by an adversary advertising fake intrusion detection reports in order to accuse legitimate and well-behaved nodes. To avoid this, nodes must rely more on local information than on reports received by other nodes.

The critical thing about the aforementioned architecture is that each node can share local data with others in order to extend the range of attacks that can be detected. For instance *stealthy attacks* do not disclose detrimental features to a single node thus collected information by all nodes is required to make possible the detection of one or more adversaries.

Nevertheless, in the generic case where nodes do not have to detect a kind of attack such as the 'stealthy', each node must be capable of detecting hazards within the network. Thereupon, the main feature of this architecture is that the IDS is fully distributed and therefore more resilient. This is an important characteristic in case of MANETs where nodes move around and lose connectivity. Likewise, another main advantage of the discussed architecture is that the distributed nature of the intrusion detection makes the network more defiant against attacks that endeavor to damage the IDS architecture. In other words, any compromised IDS node can not cause total disruption of the intrusion detection functionality of the MANET.

3.3.1 Cross layer intrusion detection systems

Our envision within the context of the security model is to design a multi-layer IDS mechanism that will be capable of defending eMANETs against different kind of attacks on each layer of the OSI model. To this end, we are planning to have an architecture such as the one highlighted in Figure 10. In the following, the basic types of attacks an IDS may face are outlined.

Physical Layer Attacks. In a case of an extreme emergency scenario it is imperative to establish perfect secrecy between the legitimate nodes. In this case any malicious node can not reveal critical information (*eavesdropping*) about the rescue mission in order to react accordingly and harm the mission in any way. In the case of an active attack on the physical layer such as *jamming* or *interception*, a significant amount of noise is sent towards the receiver to avoid a proper reception of the actual signal by the legitimate nodes. Ergo, the communications among the emergency workers collapse and the accomplishment of the mission is impossible.

MAC Layer Attacks. In the MAC layer, the *disruption of the IEEE 802.11 protocol* occurs when adversaries deny channel access to their neighbour nodes. Specifically, adversaries may add one or more bit errors to a neighbour node's link layer frame. This situation leads to the disconnection of multi-hop links disabling in some cases whole a part of the eMANET. Furthermore, adversaries may pretend that they are overloaded in order to take advance of the characteristic of CSMA/CA to allow the heavy load nodes to send first. In this case, the light load nodes can be waiting for a long period to send their packets. According to *WEP vulnerabilities*, adversaries target the message privacy and the message integrity. The reason for these for instance is the fact that a non-cryptographic integrity algorithm (CRC 32) is used with a stream cipher in addition to the fact that WEP does not specify key management.

Network Layer Attacks. In network layer, attacks are mainly targets at disrupting the appropriate functionality of the MANET routing protocol. These kind of attacks can be classified at first hand into two types namely internal and external attacks. When an internal attack is launched, it is difficult any alteration of the legitimate information to be detected. The reason for this is that compromised nodes are able to generate valid signatures using their private keys. Regarding the external attacks we can classify them into active and passive. An instance of an external passive attack against the routing protocols is the man-in-the-middle attack where the eavesdropper can discover valuable information by listening to the routed traffic. On the other hand, external active attacks could be DoS attacks causing degradation or complete halt in communication between nodes. Besides the fact that the active attacks are extremely dangerous due to the fact that they can destroy the whole communication in a MANET, they are mainly detected if appropriate security mechanisms have been applied making them a less inviting option for adversaries. In (Panaousis and Politis, 2009), we have proposed a game theoretic mechanism based on intrusion detection systems. The mechanism reduces the probability of a blackhole attack to be launched successfully whilst it consumes minimum energy. The mechanism is proposed for AODV but it can be slightly modified to be applied to SCML and this is one of our prospective targets.

Transport Layer Attacks. In the transport layer, according to the *session hijacking* attack, an adversary impersonates one node in the TCP three-way handshake by determining the correct sequence number and spoofing its IP address. After the launch of the aforementioned attack, the TCP ACK storm problem causes harmful delay to the eMANET communications. The same attack can be applied over the UDP protocol to impair the VoIP communication links.Likewise, according to the *SYN flooding* attack the adversary creates a large number of half-opened TCP connections with a victim node without completing the handshake in order to fully open the connection. Specifically, the attacker sends a several SYN packets and the victim answers with SYN-ACK packets waiting for ACK packets that it will never receive. As a result the victim node has so many open connections that its buffer is overflown. In this case, it can not receive any data from other legitimate nodes. Although, a timeout of the half-opened sessions is expired the attacker may still sending data to launch the SYN flooding attacks causing a critical damage to an eMANET's communication links.

Application Layer Attacks. In the application layer *repudiation* and *data corruption* can be maliciously accomplished when (i) a node does not accept to carry on a "transaction" with another within a MANET or (ii) a mobile virus sends probe packets to vulnerable UDP/ TCP ports at several various IP addresses. As a result, nodes get infected by the malicious entity with the most possible consequence to be the corruption of the data. As far as the attacks on SIP signalling are concerned, we discuss the most important of them in the following. *SPIT* is commonly referred to as SPam

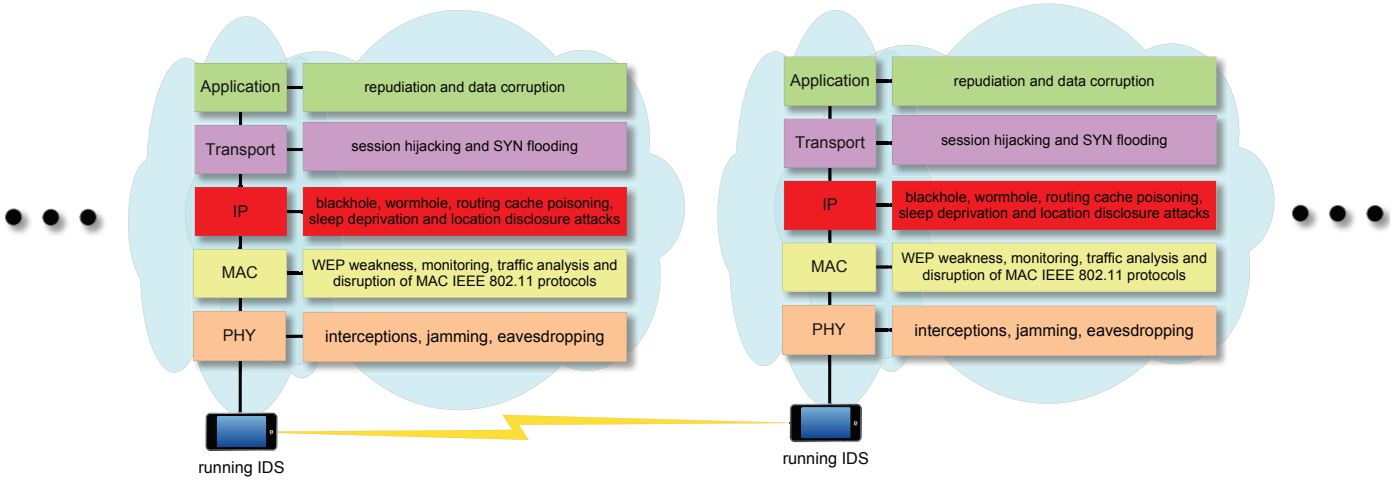


Fig. 10: IDSs mechanisms should detect attacks on all the layers of the OSI model.

over Internet Telephony (SPIT). In order to initiate a SPIT attack a malicious node has to find out the location of his victims. Therefore, the malicious node sends lookup-requests to a node of the overlay network. After getting the responses, the malicious node can start calling his victims. This threat is similar to spam in the email systems but is delivered by means of voice calls. This leverages the cheap cost of VoIP when compared with legacy phone systems. Such SPIT calls can be telemarketing calls that sell products. SPIT attacks have high impact on the operability of an network and its nodes, as every time a SPIT session is established, nodes have to establish many useless connections or must accept calls that are annoying. As countermeasure against SPIT attacks, a node could use a throttling mechanism in order to accept only a limited number of requests per second, or to integrate a time-to-live so that a lookup has a limited hop count in the overlay network. In addition, *flooding attacks* have the potential to flood the network while sending many requests to one or more nodes of the network, so that the destination nodes get distracted from working properly, and the network is heavily loaded due to the increasing traffic. Lastly, a *blocking attack* is launched by a node that silently drops messages that must be routed.

4 Conclusions

In this article we proposed a security model for autonomous networks such as MANETs to establish real time communication during emergency rescue missions. Secure routing, secure P2PSIP and intrusion detection techniques are crucial part of any security model. We have discussed some of the aforementioned issues within the realm of emergency MANETs and we have emphasized in P2PSIP overlays. Two extensions of the IETF drafts were presented and analysed in terms of security strength and scalability. These extensions were designed to meet the requirements of a mission-critical eMANET where rescuers have to establish communication bridges among them by using lightweight devices such as PDAs. The secure P2P overlays along with intrusion-detection mechanisms can provide a full and robust solution for emergency real-time communications. We have also discussed the case of our adaptive routing protocol and its security extension by using IPSec. The latter has been compared with the well known SAODV and been proved more efficient in terms of total control load and data sent. In future work, we intend to implement intrusion detection techniques against different kind of attacks. To this end, we have already based our studies on game theoretic tools such as (Panaousis and Politis, 2009). Additionally, we will show the performance evaluation of our security and key refresh mechanisms for P2PSIP. Finally, future work includes but it is not limited to implement a network simulator module, which will integrate the different functionalities of secure routing, intrusion detection and secure P2PSIP protocol. Then, a testbed can be implemented to evaluate the behaviour and the performance of the security model in a real life network.

Acknowledgements The work was undertaken in the context of the project ICT-SEC-2007 PEACE (IP-based Emergency Applications and serviCes for nExt generation networks) with contract number 225654. The project has received research funding from the European 7^{th} Framework Programme.

References

Sun, Y. L., Han, Z., Yu, W. and Liu, K. J. R.: 2006, *A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks*, Proc. 25^{th} IEEE International Conference on Computer Communications, pp.1-13, April, Catalunya, Spain. doi: 10.1109/INFOCOM.2006.154.

Martigon, F., Paris, S. and Capone, A.: 2009, *Design and implementation of MobiSEC: A complete security architecture for wireless mesh networks*, Elsevier Computer Networks, vol. 53, no. 12, pp. 2192-2207. doi: 10.1016/j.comnet.2009.04.002.

Yang, H., Meng, X. and Lu, S.: 2006, *SCAN: Self-organized network-layer security in mobile ad hoc networks*, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 261-273. doi: 10.1109/JSAC.2005.861384.

Panaousis, E. A., Ramrekha, T. A., Millar, G. P. and Politis, C.: 2010, *Adaptive and Secure Routing for Emergency Mobile Ad-hoc Networks*, International Journal of Wireless and Mobile Networks (IJWMN)

Kent, S. and Atkison, R.: 1998, *Security Architecture for the Internet Protocol*, IETF RFC 2401,http://www.ietf.org/rfc/rfc2401.txt (1998).

Hegland, A. and Winjum, E.: 2008, *Securing QoS signaling in IP-based military ad hoc networks*, IEEE Communications Magazine, vol. 46, no. 11, pp. 42-48. 10.1109/MCOM.2008.4689243.

Baset, S., Schulzrinne, H. and Matuszewski, M.: 2007, *Peer-to-Peer Protocol (P2PP)*, IETF Internet Draft, http://tools.ietf.org/html/draft-baset-p2psip-p2pp-01, (work in progress, November 2007).

Rosenberget, J. et al.: 2002, *SIP: Session Initiation Protocol*, IETF RFC 3261, http://www.ietf.org/rfc/rfc3261.txt (2002).

IETF: 2010, *P2PSIP Working Group*, http://www.ietf.org/dyn/wg/charter/p2psip-charter.html (2010).

Jennings, C., Lowekamp, B., Rescorla, E., Baset, S. and Schulzrinne, H.: 2009, *Resource Location And Discovery (RELOAD) Base Protocol*, IETF Internet Draft, http://tools.ietf.org/html/draft-ietf-p2psip-base-08, (work in progress, July 2009).

Birkos, K. et al.: 2010, *Security Mechanisms and Key Refresh for P2PSIP Overlays*, IETF Internet Draft, http://www.ietf.org/id/draft-birkos-p2psip-security-key-refresh-00.txt , (work in progress, March 2010).

Ramrekha, T. A. et al.: 2010, *ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations.*, IETF Internet Draft, http://tools.ietf.org/html/draft-ramrekha-manet-cml-00.txt, (work in progress, March 2010).

Clausen, T. and Jacquet, P.: 2003, *Optimized Link State Routing Protocol (OLSR)*, IETF Internet RFC 3626, http://www.ietf.org/rfc/rfc3626.txt (2003).

Perkins, C. and Belding-Royer, E. and Das, S.: 2003, *Ad hoc On-Demand Distance Vector (AODV) Routing*, IETF Internet RFC 3561, http://www.ietf.org/rfc/rfc3561.txt (2003).

Panaousis, E. A. and Politis, C.: 2009, *A Game Theoretic Approach for Securing AODV in Emergency Mobile Ad Hoc Networks*, Proc. 34^{th} IEEE Conference on Local Computer Networks (IEEE LCN), Zurich, Switzerland, pp. 985-992. doi: 10.1109/LCN.2009.5355020.

Zapata, M. G.: 2002, *Secure Ad hoc On-Demand Distance Vector Routing*, Proc. ACM Mobile Computing and Communications Review (MC2R), Vol 6. No. 3, pp. 106-107. doi: 10.1145/581291.581312.

Chen, L. and Heinzelman, W. B.: 2007, *A Survey of Routing Protocols that Support QoS in Mobile Ad Hoc Networks*, IEEE Network Magazine, vol. 21, no. 6, pp. 30-38. doi: 10.1109/MNET.2007.4395108.

Argyroudis, P. and O'Mahony, D.: 2005, *Secure Routing for Mobile Ad hoc Networks*, IEEE Communications Surveys and Tutorials, vol. 7, no. 3, pp 2-21. doi: 10.1109/SNPD.2007.223.

Daemen, J. and Rijmen, V.: 2002, *The Design of Rijndael*, Springer-Verlag New York, Inc.

Emmanouil A. Panaousis (www.panaousis.com) is currently a research Ph.D. student at Kingston University, UK, Faculty of Computing, Information Systems and Mathematics (CISM). He works within a team on Wireless Multimedia & Networking (WMN) Research Group. Emmanouil received his M.Sc. in Computer Science with distinction at the Department of Informatics of the Athens University of Economics and Business and his B.Sc. in Informatics and Telecommunications at the National and Kapodistrian University of Athens. Emmanouil has published more than 15 papers in international journals and conferences and one book chapter. Emmanouil is a student member of the British Computer Society, the IEEE and the IEEE Communications Society.

Christos Politis is a Reader (Associate Prof.) at Kingston University London, UK, Faculty of Computing, Information Systems and Mathematics (CISM); where he leads a research group on Wireless Multimedia & Networking (WMN) and teaches modules on wireless communications in the CISM faculty. Prior to this he was the Research and Development (R&D) project manager at Ofcom, the UK Regulator and Competition Authority. Christos was for many years he was a post-doc research fellow at the Centre for Communication Systems Research (CCSR) at the University of Surrey, UK. He is/ was involved with several EU (IST and ICT), national and international projects, and was the project manager of the IST UNITE. Christos is a patent holder, and has published more than 70 papers in international journals and conferences and chapters in two books. Christos was born

in Athens, Greece and holds a PhD and MSc from the University of Surrey, UK and a B.Eng. from the Technical University of Athens, Greece. He is a member of the IEEE and Technical Chamber of Greece.

Konstantinos Birkos received his engineering diploma from the Electrical and Computer Engineering Department of the University of Patras, Greece in 2006. He is a PhD candidate in the Wireless Telecommunication Laboratory of the same institution and he is currently involved in the PEACE research project under the FP7 framework of the European Union. His main research interests include wireless network modeling, p2p overlays, teletraffic analysis and security of wireless ad hoc networks. He is a member of the technical chamber of Greece.

Christos Papageorgiou received a Ph.D. degree in 2009, a M.Sc. degree in 2005 and a Diploma in 2002 from Computer Engineering and Informatics Department of University of Patras, Greece. He is currently employed as a post-doc research associate at the Electrical and Computer Engineering Department in the University of Patras, working in the context of various research projects. His research activities are mainly focused in the area of ad-hoc networks. Dr. Papageorgiou has published a series of scientific papers. He speaks English, Spanish and German and is a member of the Technical Chamber of Greece.

Tasos Dagiuklas (www.tesyd.teimes.gr/cones) received the Engineering Degree from the University of Patras-Greece in 1989, the M.Sc. from the University of Manchester-UK in 1991 and the Ph.D. from the University of Essex-UK in 1995, all in Electrical Engineering. Currently, he is employed as Assistant Professor at the Department of Telecommunications Systems and Networks, Technological Educational Institute (TEI) of Mesolonghi, Greece. He is the Leader of the Converged Networks and Services Research Group. He is also Senior Research Associate within the Wireless Telecommunications Laboratory of the Electrical and Computer Engineering Department at the University of Patras, Greece. Past Positions include teaching Staff at the University of Aegean, Department of Information and Communications Systems Engineering, Greece, senior posts at INTRACOM and OTE, Greece. He has been involved in several EC R&D Research Projects under FP5, FP6 and FP7 research frameworks, in the fields of All-IP network and next generation services. Currently, he is the Technical Manager of the FP7-ICT-PEACE project. He was the Conference General Chair of the international conference, Mobile Multimedia 2007 (ACM Mobimedia 2007), Technical Co- Chair of MMNS Conference of MANWEEK 2008, IMS Workshop Chair as part of ACM Mobimedia 2008 and Workshop Chair for ACM Mobimedia 2009. He has served as TPC member to more than 30 international conferences. His research interests include Future Internet architectures and converged multimedia services over fixed-mobile networks. Dr Dagiuklas has published more than 80 papers at international journals, conferences and standardisation fora in the above fields. He is a member of IEEE and Technical Chamber of Greece.