Secure Decentralised Ubiquitous Networking for Emergency Communications

Emmanouil A. Panaousis*, Tipu A. Ramrekha†, Christos Politis* and Grant P. Millar*

*Wireless Multimedia & Networking (WMN) Research Group
Kingston University London
{e.panaousis, c.politis, g.millar}@kingston.ac.uk

†Synelyxis Technologies
arvind@synelyxis.com

***Abstract*—Our modern densely populated cities have created an Achilles heel for public safety services where natural or man-made disasters often result in high casualties. The 2005 London bombings have exposed the inadequacy of current First Responder (FR) communication systems for modern response operations. Additionally, FR organisations presently pay a tariff each time Public Protection and Disaster Relief (PPDR) communication technologies are used, rendering current PPDR communication expensive as compared to emerging license-exempt IP-based technologies. Decentralised ubiquitous networking proposes an alternative way of providing innovative secure wireless systems for IP-based, infrastructure independent PPDR communications. The ad-hoc setup capabilities of ubiquitous systems will reduce the cost for emergency response whilst allowing more flexible ways of communicating. Key characteristics of such systems are their ease of deployment and the interoperability across FR teams for national as well as cross border operations. In this paper we discuss how decentralised ubiquitous networking can assist emergency communications.**

I. Introduction

Wireless networking technologies are an appropriate foundation to support different rescuers in an emergency situation such as a forest fire or a tube terrorist attack. In a disaster case, each rescue team (e.g. police team, fire working team or ambulance team) has to be aware of the situation and all the teams have to collaborate towards the achievement of a particular goal. Discussions about civilian security usually diverge into discussions about the most prominent security incidents including terrorist attacks and the need to improve security systems in Europe. Such security breaches tend to create crisis and panic over the society. Thus, it is crucial to define an appropriate crisis response management scheme for the improvement of the security of citizens. This strategy will coordinate all the available resources in terms of public services (i.e. police, authorities, hospital, fire-brigade, military) so that this crisis is resolved smoothly. For instance, large-scale events such as the London Olympic Games 2012 and other co-hosted major sporting events (e.g. European Championships Poland/Ukraine 2012), are high security risk events where attackers tend to target both civilians and ICT (Information and Communications Technology) infrastructures in order to create chaos and to disrupt coordinated rescue efforts respectively.

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.

A. Decentralised Ubiquitous Networking in Emergency Cases

Since there are increasing threats against civilian security in modern society due to rising terrorist activities and increased causalities from natural calamities in densely populated cities there is a requirement for more efficient PPDR systems. These systems will allow proper coordination of FRs and consequently reduce fatalities. Hostile disaster environments are usually deprived of communication infrastructure that are often incapacitated by either high user demand or physical damage. Additionally, existing emergency teams use a variety of different radio systems based on TErrestrial Trunked RAdio (TETRA) technology. TETRA systems usually have less capabilities (no group communication, no video transmission and low bit rates) compared to modern mobile systems and are expensive to purchase and operate. All security forces, both national and international (in the case of cross-border operations), must be able to collaborate to guarantee minimal human casualties and material damage at large-scale emergency scenes.

In the context of secure responder communications during cross-border operations, it is recognised that interoperability among current responder communication systems, such as TETRA and TETRAPOL, is a critical issue. This is due to the fact that the basis for public safety communications is PMR (Professional Mobile Radio) based networks. These are being utilised by professional users including police and fire brigades across EU authorities and Member States. However, todays PMR networks have very limited capabilities for data transmis-

978-1-4673-2781-7/12/$31.00 ©2012 IEEE

sion while they cannot support services like internet/intranet browsing, emailing, and transferring large maps or video.

Our vision is to provide a secure cooperative wireless system which can run on modern mobile devices such as smart phones, offering a complete communication suite for FRs. Interoperability will be enabled by developing appropriate Application programming interface (APIs) for their smart devices or even mobile gateways. In this current financial climate, this concept will allow FRs to cut cost on setup, operation and maintenance from a communications viewpoint. This will happen by enabling infrastructure independent communications which will be free of charge regardless of the operation time and service. Additionally, costly communications with the command and control by using 3G or long range WiFi are still considered more cost effective than TETRA/TETRAPOL. In addition, this solution will offer secure IP-based peer-to-peer communications compatible with Internet and future mobile wireless infrastructures.

As current PPDR systems are significantly expensive to operate, decentralised ubiquitous networking can have a significant economic impact by reducing the cost of procuring and operating First Responder (FR) PPDR communication systems. Additionally, cross-border European PPDR initiatives would be feasible at much lower cost since decentralised ubiquitous networking can provide an appropriate interoperable communication platform. Decentralised ubiquitous networking can also reduce cost of mobile data traffic compared to existing PMR technologies and will have no operational cost by using license exempt parts of the spectrum while at the moment FR organisations must pay whenever the FRs press the button to communicate with each other.

Furthermore, the main social impact of the decentralised ubiquitous networking is that civilians will now be able to transparently or actively participate with their consent in the provision of PPDR services and communications. They will be able to either transparently use personal devices to act as relays within a secure network environment thus increasing the communication range of our PPDR systems or to directly communicate with FRs. In the second case, civilians will assist FRs during a critical mission such as the one that took place during the 2005 London bombings incident where the telecommunication infrastructures collapsed. In addition, civilians will be able to contact FRs for reporting their location and situation when for instance, in case of an earthquake, people are trapped under collapsed buildings. Therefore, civilians will have a higher sense of safety and security. Last but not least, the interoperability provided by decentralised ubiquitous networking described above can foster international collaborations for disaster relief missions such as cross-border security collaborations among European countries e.g. UK-FRANCE or UK-HOLLAND.

In terms of environmental benefits, decentralised ubiquitous networking would be very effective towards mitigating the impact of remote environmental catastrophes. Calamities such as remote maritime oil spillage or forest fires can be more effectively dealt with using the decentralised ubiquitous communication systems. In addition, such systems can use long-range versions of Wi-Fi radio technologies with reduced radiation levels and health hazards for humans and other living entities. Also, by using such low power technologies FR communication will be greener compared to the current PPDR systems as it will not need infrastructural constructions.

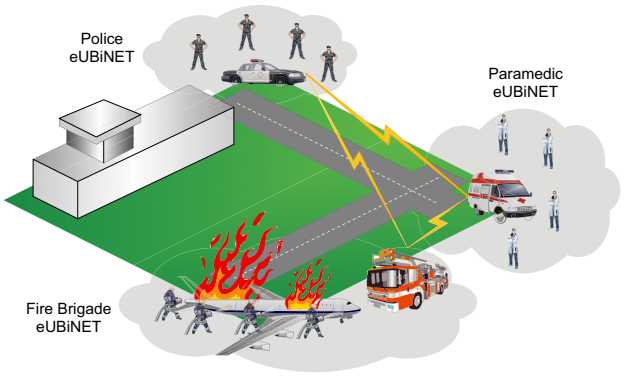

Fig. 1. An emergency scenario where the concept of eUBiNETs can be utilised.

Our work investigates the provisioning of day-to-day emergency communications in next generation all-IP networks. We use the term emergency ubiquitous networks (eUBiNET) in order to describe next generation IP-based networks which are deployed in emergency cases. Our main scope is to provide emergency workers, who form eUBiNETs, with intelligent devices such as smart phones and PDAs on the road to establish ad-hoc communication ”islets” between the members of the same or different emergency teams. The nature of eUBiNETs makes them ideal to be utilised in the context of an extreme emergency for all involved rescue teams. We define an emergency case as any event which threatens to cause serious damage to human welfare or the environment. During these catastrophic events it becomes imperative, members belonging to different rescue teams coordinate their actions to expedite recovery missions as it is illustrated in Fig. 1.

B. The Vision of Decentralised Ubiquitous Networking

The term decentralised ubiquitous networking refers to networks that can provide end-users with access to data communication facilities in a pervasive manner [1]. The requirement for ubiquity of networks becomes more apparent with the necessity for end-users to be able to exchange information while on the move. This modern user requirement trends from the popularisation of wireless seamless connected lightweight devices. Moreover, with the emergence of the smart machine-to-machine (M2M) services in the perspective of an Internet of Things (IoT) [2] networks have to be established in a more autonomous, cost efficient and distributed fashion in order to allow for localised services. These services could provide information to end-users or other machines without accessing core networks such as server clouds. In this way, there will be a lower data load to be supported by the core networks and capability to provide higher bandwidth, user-centric personalised

services in peripheral distributed networks. A decentralised approach can be greatly beneficial for implementing a ubiquitous network as mentioned above. In summary, the objective is the development of a decentralised localised implementation of future pervasive services on ubiquitous networks to sustain higher throughput per area of service, higher user density and will enable a greener method of communication environment.

In terms of the actual architectural format of decentralised pervasive networks, a cooperative, multi-hopping, self-configurable and autonomous system of entities is the most likely path that will be adopted as indicated by literature [3] industry and international research efforts e.g. EU FP7 ICT-SEC PEACE project. Therefore, the sphere of ad-hoc networking is particularly considered as the suited candidate for implementing the ubiquitous distributed networking solution for the future. Communicating entities can then readily setup, join or leave networks depending on the scenarios and user requirements. For instance, in an emergency communication situation, FRs could use portable or vehicle-equipped mobile devices to effectively setup networks by a simple power-up/power-off and play/shutdown method. The whole process would be cost efficient and users would have sufficient privileges to achieve such actions. These privileges will be assigned by a command and control authority of each first response team in order to ensure as highest security for their systems as possible while at the same time appropriate and required privileges to the users will be provided. In another use case, civilians will only be able to join and leave a network of live regional transportation information, as initiated and maintained by relevant authorities. In both scenarios though, the communication is required and achieved in a distributed and localised fashion.

Ad hoc networks exist in several forms as characterised by the nature of the participating devices and the mobility of communicating bodies namely mesh networks, mobile ad-hoc networks (MANETs), sensor (both static and mobile) networks and RFID networks. The mesh networks consist of static longer-range wireless devices that can form an ad-hoc backbone for such dynamic networks. MANETs on the other hand mainly consist of lightweight cooperative devices such as smart phones that will be mainly mobile. Sensor and RFID networks are mostly static low power, low range devices used to monitor situations in order to create a situational awareness in a multi-hoped M2M communication fashion. This information will be useful for humans or actuator smart machines alike in order to assess further actions e.g. local weather maps or local traffic maps. Since cooperation is the only way to transfer data from source to destination using direct interconnected source-destination (S-D) pairs or using multi-hopping via intermediate nodes acting as routers, security and routing are the two main research challenges associated with decentralised ubiquitous networks.

C. Routing for Decentralised Ubiquitous Networking

The routing mechanism in decentralised ubiquitous (ad-hoc) networks is a cooperative action that is required if the Source-Destination (S-D) pair is not directly interconnected. In that case, a multi-hopped forwarding scheme is required whereby intermediate nodes act as routers to forward information from source to a node closer to the destination until the data reaches its intended recipient. The Internet Engineering Task Force (IETF) MANET Working Group [3] is responsible for the standardisation of IP-based routing protocol functionality for wireless routing in both static (MESH) and dynamic (MANETs) ad-hoc routing networks. Since MANETs are a representative type of decentralised ubiquitous networks we believe that any standardisation activity within the MANET realm will set the basis for the creation of significant work in the field of decentralised ubiquitous networks.

The MANET WG has proposed three main standardisation tracks for routing approaches, which are proactive, reactive, and hybrid. These approaches differ mainly in the way that route discovery and route maintenance mechanisms are defined. In proactive approaches, also known as table-driven, route discovery and route maintenance is carried out by each node in the network on a periodic basis to maintain consistent and updated information of routes to all nodes in the network. In the reactive approach, routing is carried out on-demand when data is ready to be sent from a source node to a destination node. The route discovery packet is flooded into the network by the source node until a destination is found and the route to the destination is signalled back to the source to form a bi-directional route. This route is then only temporarily maintained while active transmission still occurs through that route. There are also emerging trends of hybrid and adaptive routing protocols being proposed in literature. For instance, the ChaMeLeon (CML) routing protocol [4] is an adaptive protocol that uses a hybrid approach towards ad-hoc routing in emergency cases. The CML protocol is designed to provide a scalable quality of service (QoS) to nodes in a MANET by providing improved delay and jitter performances as compared to Ad hoc On-demand Distance Vector (AODV) (reactive) [5] in smaller networks and OLSR (proactive) [6] in larger networks. Thus, the CML protocol operates based on a threshold value of the network size whereby it shifts the routing mechanisms it utilises from OLSR to AODV and vice-versa. In the proactive phase (P-phase) CML uses OLSR mechanisms for routing and monitors the network size in parallel by counting the number of nodes in the OLSR table. Once the number of nodes is found to have exceeded the network threshold value, CML enters the Oscillation phase (O-phase) of operation whereby it continues monitoring the network size to validate that the network size has actually changed as opposed to periodic network size perceptions due to bad links or oscillatory movements of nodes.

In fact, the number of ubiquitous network nodes in disaster rescuer communication scenarios may vary rapidly depending on the severity of the rescue operations. Thus, the employed protocol should have the ability to efficiently route data in small, large as well as variable sized MANETs operating in a delimited disaster area called the Critical Area (CA) both with and without the presence of obstacles that impede line of sight

(LoS) communications and rescuer mobility. To summarise, the specific requirements for emergency communications is the topological distribution of ubiquitous nodes and the nature of obstacles.

D. Peer-to-peer decentralised ubiquitous networking

Peer-to-peer overlay networks have the potential to accommodate large-scale, decentralised applications that can be integrated into a MANET architecture to enable peer-to-peer communication among different mobile peers. These overlay architectures must be very resilient and their utilisation, reliability and availability must satisfy the needs of mobile computing. One must also heed the fact that the wireless nature of the medium introduces security vulnerabilities.

The increase in computing power over time has caused an evolution in every day personal computers and laptops making them lightweight and portable with capabilities to act as both routers and clients in the network. This has spawned the creation of MANETs, which encompass the peer-to-peer (P2P) ad-hoc paradigm.

To exploit the peer-to-peer paradigm of MANETs, one must look towards an integrated solution to applications and information sharing, such as Distributed Hash Tables (DHTs) [7]. The motive for using DHT in MANETs is due to an extremely quick setup time in both application and network layer in addition to the fact that no additional infrastructure is needed in either layer other than the devices themselves. DHTs allow us to find the exact location of a party or piece of information stored within the network, using a piece of simple meta-data for example a name and domain, as proposed in Peer-to-Peer Session Initiation Protocol (P2PSIP) [8].

However the use of DHTs is not limited to simple name resolution and their distributed structure also allows for fast propagation and high availability of information through the network. When applied to MANETs which have no central authority, DHTs could provide the answer to distributed services such as DNS (Domain Name System), P2PSIP, distributed storage and information sharing, whilst aiding service lookup and discovery. Last but not least, all types of data could be stored redundantly and accessed easily and quickly by any peer.

II. Security for Decentralised Ubiquitous Networking

Having discussed the main aspects of decentralised ubiquitous networks, we then discuss the threats, attacks, and vulnerabilities in such networks as well as existing solutions within the security realm. Due to their special nature, decentralised ubiquitous networks raise a set of new challenges to the security design of wireless networks presenting open network architectures and variable topologies. The main four vulnerabilities that are security concerns in decentralised ubiquitous networks are the following:

- *Wireless medium*: Decentralised ubiquitous networks impose several challenges since the use of wireless links allows a large set of attacks to target these networks. This happens because signals are propagated from the source over the open air to all directions and prospective attacks can be launched by anyone and from any direction. Although a mechanism can provide confidentiality and integrity of the messages sent over a decentralised ubiquitous network, traffic analysis is still feasible. In addition, adversaries can launch a Denial of Service (DoS) attack such as jamming disrupting the ubiquitous communications [9].
- *Routing based on cooperation*: Decentralised ubiquitous network nodes need to cooperate with each other to carry out routing functionalities. Thus, routing can introduce a significant security hole in the presence of malicious nodes. Data tampering, DoS and impersonation attacks are some examples of malicious activities that can be easily launched against decentralised ubiquitous networks due to the cooperative nature of routing protocols. Particular well-known attacks include but are not limited to wormhole attacks [10] and rushing attacks [11].
- *Lack of fixed and centralised infrastructure*: Decentralised ubiquitous networks do not deploy any fixed infrastructure and there are no actual central nodes to direct packets. Therefore, monitoring traffic in decentralised ubiquitous networks becomes a harder problem. Another aspect of such networks that increase the difficulty for monitoring is the network segmentation which takes place when nodes move in different locations of the network in a way that they make communication partitions with some of them losing connection towards some destination nodes. The same situation occurs when some nodes die faster than other due to battery limitations. Another effect of the decentralised nature is that public key cryptography schemes are hard to employ since they require the existence of a certificate authority (CA) which must be centralised trust point.
- *Low capacity of ubiquitous devices*: Decentralised ubiquitous networking devices are usually mobile phones, PDAs or laptops. These have limited memory, battery level, processing power and cannot support very high network bandwidth. This hinders the application of computationally intensive security algorithms such as greedy asymmetric cryptographic schemes.

Among the most important security requirements in decentralised ubiquitous networks are: authentication, authorisation, confidentiality, integrity, efficiency, key management, non-repudiation and scalability. Authentication is the way to prove that nodes participating in a PPDR communication are not pretenders. In fact, authentication gives solution to the problem of impersonation and it be achieved through digital signatures. There exist two kinds of authentication. First, it is the channel end point authentication and second it is the authentication needed to ensure that a node can use a service because it is not an impersonator. The latter is called authentication of the message originator. Authorisation is the

concept of giving permission privileges to the nodes.

Confidentiality means that in a communication between two PPDR devices must be no other party, which can understand the content of the transmitted packets. This can be achieved through encryption algorithms. Integrity of packet means that a packet is remained pure during its transmission from the source to destination. Efficiency of the security solution in terms of computational complexity, energy consumption and communication overhead is very critical. Key management includes key creation, key storage and key distribution. Non-repudiation means that the sender of a message cannot later deny sending the information or the receiver cannot deny the reception. Finally, scalability means that the security solution should be scaled well to a large number of nodes within a decentralised ubiquitous network.

We envisage security mechanisms to protect traffic in decentralised ubiquitous systems, tailored for the purposes of emergency communications. We assume two modes of operation. In the first mode, we allow an infrastructure operation to enable communication between FRs and the command and control centre. To this end, FRs devices are connected directly to a trusted wireless access point (WAP).

In the other mode, decentralised ubiquitous networking allows the FRs' devices to communicate with the command and control centre through an intermediate node, which has access to the Internet (either using 3G, or WiFi). A real scenario where this can take place is when, for instance, an FR is out of his car and he carries his PDA, which can use to access the laptop which is located in the car. In this way, the FR device can access the command and control centre using 3G. In the same mode, nodes communicate with each other in an ad-hoc manner replacing in this way TETRA systems. In this way, decentralised ubiquitous networking is enabled in order to support multimedia communications in emergency cases when telecommunications infrastructures have collapsed.

One of the main goals of our work is to prevent potential eavesdroppers from spying on the FRs data stream, hence a combination of filtering and encryption is required. Another threat could be if someone manages to hack into a WLAN and piggybacks onto the Internet connection stealing the bandwidth. Worse, anyone on a WLAN will be using the same Internet protocol (IP) address as an FR. In that case, he appears to be that FR hijacking his identity.

Physical and MAC layer security can be provided by the FIPS (Federal Information Processing Standards) certified standard WPA2 Enterprise (IEEE 802.11i), the AES (Advanced Encrypted Standard) and the IEEE 802.1X. WPA2 works by encrypting traffic as it leaves the WAP or the FR's device and decrypting it on arrival. WPA2 implements the mandatory elements of the IEEE 802.11i. The IEEE 802.11i includes specifications on encryption, authentication and key management in a multi-layered approach to security.

Another layer of protection is individual authentication by using the IEEE 802.1X protocol. If the protocol is enabled, unauthenticated users cannot get connected to the WAP to access the rest of the network. Apart from authentication services, IEEE 802.1X (EAP-TLS) provides port access control to establish and change the appropriate cryptographic keys. EAP-Transport Layer Security (EAP-TLS), defined in RFC 5216, is an IETF open standard, and is well supported among wireless vendors. The security of the TLS protocol is strong, provided the user understands potential warnings about false credentials. It uses PKI to secure communication to a RADIUS authentication server or another type of authentication server.

To enable secure end-to-end communication between users of a network there is a need for establishment of shared security attributes between them to support secure communication in the network layer. Only the destination of a packet is able to decrypt it and retrieve the required information. To this end, users that need to communicate with each other can use the IPsec protocol [12] which has been proven lightweight compared to other asymmetric approaches [13]. The devices must securely and confidentially share a key in other words must set up a security association (SA). Hence only the owner of a pairwise private symmetric key can decrypt the packets guarantying end-to-end security between source and destination. A testbed with initial results in this field has been published in [14].

IPsec works on the network layer of the OSI model securing all data (using AES encryption) that are transmitted between the two endpoints. When connected on an IPsec VPN the client smart device is virtually a full member of the corporate network and it can see and have access to the entire network. Thus, it is possible to implement a simple VPN between users by creating an IPsec security policy. In that way, FRs share a password or phrase, which is then used to generate a shared encryption key. The drawback to this system is that the shared key must be manually provided to each partner. In a practical sense, this often means that the key is written down or sent via email, resulting in a breach of basic security.

To overcome this weakness, each FR's device possess a public-private key pair, which are unique for each user and they are generated in the beginning of the network's setup, along with a self-signed X.509 certificate. This contains the user's public key, as well as the user's name and device ID. The user must enter his or her full name, while the device name is initialised to a default value retrieved from the operating system. The expiry time of a certificate is configurable. When establishing a secure connection with another FR for the first time, the users certificate is transmitted and displayed to the destination partner. Once a user has verified a partners certificate, it is imported into a local cache of trusted certificates. Subsequent connections with that partner are established transparently, until the partners certificate expires or is manually removed from the cache.

Last but not least, it is important to address all the security breaches that emerge due to the participation of civilians in eUBiNETs. As we have discussed, civilians will now be able to transparently or actively participate in the provision of PPDR services and communications. Whilst, this approach is efficient in terms of network provisioning services since more

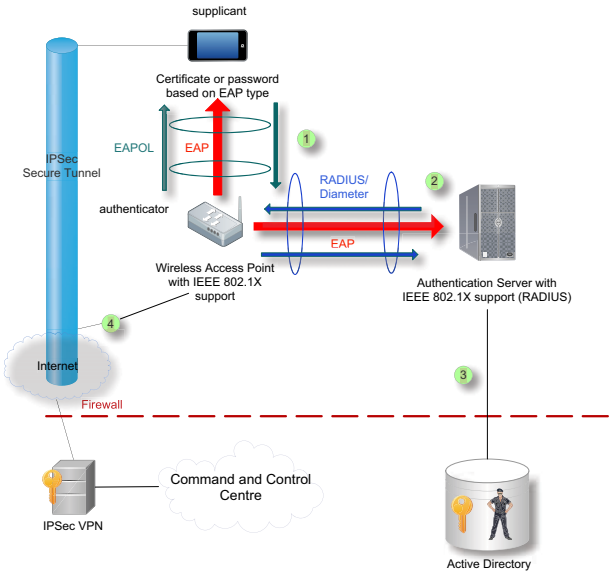

Fig. 2. The architecture of the secure eUBiNET when a connection with command and control centre is required.

devices will help in the setup and maintenance of the network, security vulnerabilities that come with this approach might critically affect emergency missions.

To address such issue, we need to provide civilians with a robust and secure application that will run on different platforms and will allow communication with PPDR devices operated by FRs. To mitigate security risks, the application can use different tools to separate running programs and executing untrusted or untested programs from unreliable third parties, users, suppliers and websites, various access control features and file system encryption. To avoid cases where a rogue user will try to maliciously participate in the network, some pre-defined certificates will be given to users of the devices which will run the specialised software. To ensure that only legitimate civilian users are owners of valid certificates a thorough validation of their devices and their personal details must take place in advance whilst at the same time a monitoring mechanism will be critical to identify malicious activities from the civilians side during the emergency cases.

III. Conclusion

Discussions about PPDR usually diverge into discussions about most prominent security incidents including terrorist attacks and the need to improve security systems in Europe. Such security breaches tend to create crisis and panic over the society. It is therefore important to improve European PPDR systems interoperability to ensure secure and reliable communications among different responder organisations at all times and across European locations. To this end, decentralised ubiquitous networking can be utilised to satisfy the requirements of a 'modern' emergency communications paradigm by enabling multimedia services in a lower cost and with user-friendly functionalities. Needless to say, security is the one of the most important requirements for any system. In this paper we discuss the importance of an alternative type of secure networks called eUBiNETs which will support emergency communications utilising two modes operation. One mode enables communication between the FRs and a command and control centre while the other allows FRs to communicate with each other in a decentralised manner. In such way, FRs need to be equipped with only one smart device which enables rich media and broadband services. We envisage that the deployment of such technologies will create a new generation of emergency communications systems.

Acknowledgment

This paper carried out within the scoope of a Technology Strategy Board Smart "Development of Prototype" funded project.

References

[1] D. Braun, J. Buford, R. Fish, A. Gelman, A. Kaplan, R. Khandelwal, S. Narayanan, E. Shim, and H. Yu, "Up2p: a peer-to-peer overlay architecture for ubiquitous communications and networking," *Communications Magazine, IEEE*, vol. 46, no. 12, pp. 32 –39, december 2008.

[2] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless- and mobility-related view," *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 44 –51, Dec. 2010.

[3] T. Ramrekha, E. Panaousis, and C. Politis, "Standardisation advancements in the area of routing for mobile ad-hoc networks," *The Journal of Supercomputing*, pp. 1–26, 2011, 10.1007/s11227-011-0705-2. [Online]. Available: http://dx.doi.org/10.1007/s11227-011-0705-2

[4] T. Ramrekha and C. Politis, "An adaptive qos routing solution for manet based multimedia communications in emergency cases," *Mobile Lightweight Wireless Systems*, pp. 74–84, 2009.

[5] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on demand distance vector (aodv) routing (rfc 3561)," *IETF MANET Working Group (August. 2003)*, 2003.

[6] T. Clausen and P. Jacquet, "Rfc 3626-optimized link state routing protocol (olsr)," *IETF RFC3626*, 2003.

[7] E. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *Communications Surveys & Tutorials, IEEE*, vol. 7, no. 2, pp. 72–93, 2005.

[8] K. Singh and H. Schulzrinne, "Peer-to-peer internet telephony using sip," *Proc. of the ACM International workshop on Network and operating systems support for digital audio and video*, pp. 63–68, 2005.

[9] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," *Proc. of MILCOM*, vol. 6, 2006.

[10] E. Panaousis, L. Nazaryan, and C. Politis, "Securing aodv against wormhole attacks in emergency manet multimedia communications," *Proc. ACM/ICST MOBIMEDIA*, Sep. 2009.

[11] Y. Hu, A. Perrig, and D. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 30–40, 2003.

[12] S. Kent and K. Seo, "Rfc 4301: Security architecture for the internet protocol," Dec. 2005. [Online]. Available: http://tools.ietf.org/html/rfc4301

[13] C. Chigan, L. Li, and R. Bandaru, "Providing unified security mechanisms for manet network layer," *Proc. ICWN*, vol. 2, pp. 721–726, Jun. 2004.

[14] E. Panaousis, G. Drew, G. Millar, T. Ramrekha, and C. Politis, "A testbed implementation for securing olsr in mobile ad hoc networks," *International Journal of Network Security & Its Applications*, vol. 2, no. 4, October 2010.