



**FP6 – Priority 2.3.2.9
Improving Risk Management
Integrated Project**

Project Acronym	OASIS		
Project Full Name	Open Advanced System for dISaster and emergency management		
Contract Number	004677		
Starting date	01/09/2004	Ending date	31/08/2008

Deliverable ID	D-SP2_04 (Summary Report)		
Document Reference	OASIS_SP24_RPT_102_BAE		
Title of the Document	Communication Activities Research Summary Report		
WP related to the document	SP2.4		
Type	PU		
Partner(s) Contributing	BAE Systems		
Date	17/12/2006	Version	2.0

	Name / Function	Company / Organisation	Date
Managed by :	M.D. Otter SP2.4 Work Package Leader	BAE Systems	18/12/06
Checked by:	J. Cardell SP2 Leader	Ericsson AB	18/12/06
Approved by:	J. Milsom Acting Head of Department	BAE Systems	20/12/06
Released by:	Martine Couturier / OASIS coordinator	EADS DS	21/12/06

Project Coordinator

Company name EADS DS
 Name of representative Martine COUTURIER
 Address
 Phone number +33 (0)1 61 38 5 252
 E-mail
 Project WEB site <http://www.oasis-fp6.org/>

This document is the property of OASIS -"Open Advanced System for dISaster end emergency management"-Consortium.

Its utilisation should clearly mention its OASIS FP6 Consortium source.



Deliverable ID: D-SP2_04 (Summary Report)
Document Ref.: OASIS_SP24_RPT_102_BAE_2_0

Communication Activities
Research Summary Report

Document Status Sheet

Version	Date	Details
1.0	14/02/2006	Creation of the document
1.1	20/02/2006	Minor changes to issue 1 following comments from EMW
2.0	17/12/2006	Update following EU reviewers comments on version 1.1

Table of contents:

1	<i>Introduction</i>	4
2	<i>Study of Routing Policies and Protocols in Heterogeneous Networks</i>	5
2.1	Introduction	5
2.2	Relevance to OASIS	6
2.3	Findings of the study	7
3	<i>Review of standards for long range wireless networks</i>	8
3.1	Introduction	8
3.2	Relevance to OASIS	8
3.3	Findings of the study	8
4	<i>Review of Secure Multicast Protocols</i>	9
4.1	Introduction	9
4.2	Relevance to OASIS	9
4.3	Findings of the study	10
5	<i>Availability of Spectrum for WLANs</i>	10
5.1	Introduction	10
5.2	Relevance to OASIS	11
5.3	Findings of the study	11
6	<i>Testing performance in an OLSR-based MANET with QoS capabilities</i>	11
6.1	Introduction	11
6.2	Relevance to OASIS	12
6.3	Findings of the study	12
7	<i>Analysing security services in a MANET connected to other infrastructure</i>	13
7.1	Introduction	13
7.2	Relevance to OASIS	13
7.3	Findings of the study	14
8	<i>Conclusions</i>	14
9	<i>Summary of recommendations</i>	15

1 INTRODUCTION

The overall aim of OASIS work package SP2 is to provide the communications infrastructure and the communications sub-system for OASIS disaster and emergency management systems. This requires a number of key communication capabilities that are supported by a range of communication services. For the former the prime importance is interoperability between integrated multi-technology access networks connected to a common core IP network, ensuring quality of service, security and mobility. For the latter SP2 includes the provision of, and access to, services such as voice, data and communications management.

The SP2 work leading to the POS1 trials and demonstration in September 2006 was based around the application of mature COTS technologies such as LANs, WANs, Wireless LAN (WLAN), TETRA/TETRAPOL, 2G, 3G, satcom, VPN over the internet, Voice over IP, SMTP/POP and LDAP. In addition ad hoc networking was used experimentally; it was successful but cannot be considered mature for reasons that will be described later in this report.

This document is a report of work carried out in work package SP2.4 which consists of selected parallel research activities. The objectives are to identify and progress a set of network issues where special solutions are required to build and operate a communication infrastructure for emergency/crisis management. It was initially intended to insert solutions in the POS1 and POS2 trials but, at the time of writing, it appears more likely that most insertions will be on a longer timescale. The reasons for this include the maturing of some new technologies and the dangers of large complex trials with high risks in the infrastructure.

This document is a summary of the following research activities that have been carried out in SP2.4 over the period 2005/6:

- Study of Routing Policies and Protocols in Heterogeneous Networks (RTG)
- Review of standards for long range wireless network (LONG)
- Review of Secure Multicast Protocols (MSEC)
- Availability of Spectrum for WLANs (SPECT)
- Testing performance in an OLSR-based MANET with QoS capabilities (PERF)
- Analysing security services in a MANET connected to other infrastructure (AHSEC)

Each research report has been given an acronym (indicated above) for ease of reference within this report. The reports are internal OASIS deliverables and are not released to the public.

The SP2.4 work in 2005/6 was carried out by three of the OASIS partners:

- BAE Systems (BAES, SP2.4 leader): RTG, LONG, MSEC
- Ericsson Microwave Systems (EMW)¹: SPECT
- Thales Norway AS (TNR): PERF, AHSEC

These research reports focus upon the following key requirements: information capacity and/or security. The relationships between the reports is illustrated diagrammatically below:

¹ Ericsson AB at the time of writing this report.

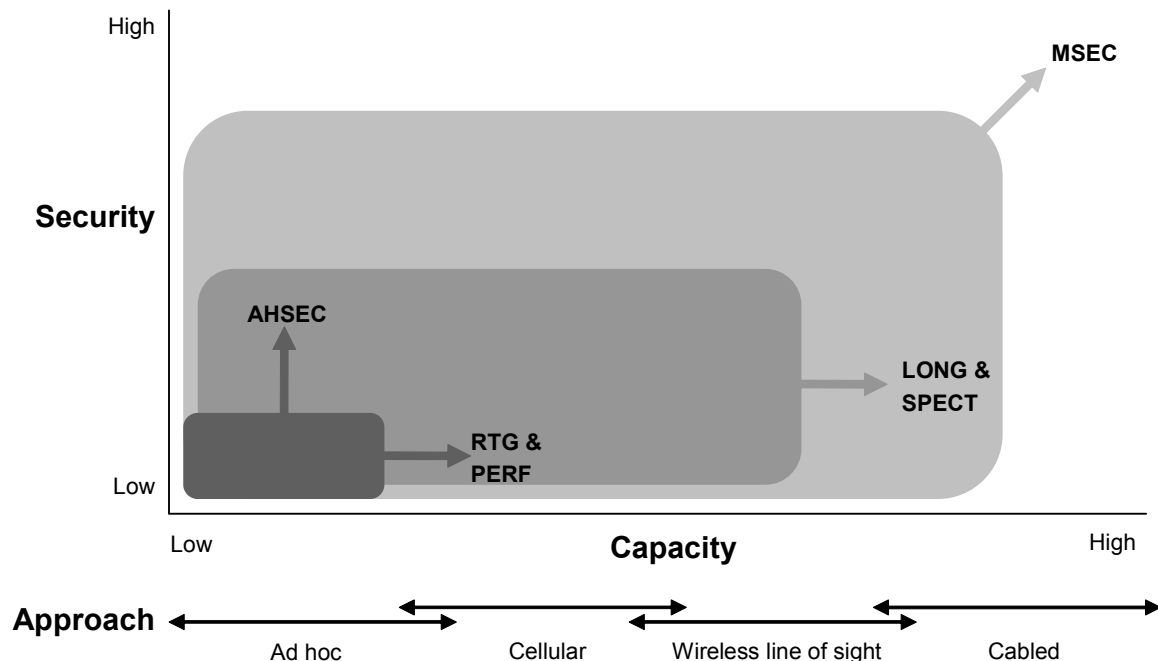


Figure 1. Relationship between 2005/6 research topics

Figure 1 is a qualitative diagram showing the spectrum of how capacity may be deployed:

- Ad hoc networks: Rapidly deployed and support mobility
- Cellular networks: Require planning and support mobility
- Line of sight links: Require planning, static, moderate capacity
- Cabled bearers: Require planning, slow to deploy, substantial capacity

The studies on ad hoc networks cover novel routing protocols that improve performance (RTG), a study of WLAN configuration that also improves performance (PERF) and a study of a security building block (AHSEC). Both the LONG and SPECT studies are primarily concerned with greater capacities from emerging wireless networking standards. Finally MSEC is concerned with security for multicast protocols that efficiently deliver information from a single source to a group of destinations and, as such, facilitate both security and additional effective capacity.

The six studies are summarised in sections 2 to 7 of this document and each have the following subsection structure: introduction, relevance to OASIS, and findings of the study including maturity and insertion opportunities. Then overall conclusions are drawn in section 8 and the recommendations are summarised in section 9.

2 STUDY OF ROUTING POLICIES AND PROTOCOLS IN HETEROGENEOUS NETWORKS

This report was produced by BAE Systems, document reference OASIS-2.4-RPT-094-BAE.

2.1 Introduction

An ad hoc network is a self-organising network that requires no planning, central control or prior infrastructure. Nodes may be mobile, with a dynamically changing topology.

The report is an overview of developments in ad hoc routing protocols. These are protocols that run between cooperating nodes in ad hoc networks, sharing topology information so that

nodes can forward traffic on behalf of each other. Protocols are essential for correct operation, but are an overhead in that they consume network capacity and power for their transmissions etc. Many protocols have been proposed over the last decade, each employing a “trick” that is intended to minimise overheads, typically making some assumption about network operation, whilst routing as accurately and efficiently as possible.

The report introduces the main protocols developed by the IETF (Internet Engineering Task Force) MANET (Mobile Ad hoc Network) group together with many other protocols in the literature. It covers the major categorisation of protocols as reactive (finds routes on demand, the trick being an assumption that only a few of the many possible routes are required) or proactive (maintains all routes as efficiently as possible, the benefit being no delay when a new route is required), or a hybrid combination of both. The report also covers hierarchical protocols, which depend upon some natural clustering in the network, and position-based protocols, that exploit additional knowledge of where nodes are in order to simplify routing decisions.

In addition to introducing a number of routing protocols, the report considers two aspects of quality of service (QoS). First the importance of link quality is explained; routing protocols discover links by handshakes between neighbouring nodes and these are poor at ensuring that link quality is high, the risk being that a low quality link will either lose a lot of traffic or waste energy in retransmissions. Then the report considers measures of capacity so that QoS-sensitive traffic can be carried.

Link quality sensing is important, especially since most routing protocols select minimum hop count paths and therefore favour the longest and consequently the poorest quality links. This can be achieved by signal to noise measurements and enhanced by a number of techniques identified in the report, e.g. optimising packet fragment lengths.

QoS for applications is only mentioned briefly. No solutions to the problem of oscillation have been identified, i.e. a protocol identifies spare capacity and traffic moves in that direction, freeing capacity elsewhere, ... Moreover it is obviously difficult to provide any quality guarantees when the network topology can be changed at any time. It is concluded that there are no general solutions for QoS in ad hoc networks at the time of writing.

2.2 Relevance to OASIS

Ad hoc networks are ideal for crisis management scenarios, where there may not be a dependable network infrastructure, possibly because it has been damaged by the cause of the crisis or become congested by high demand from the general population, and the time penalty to set up a managed infrastructure is unacceptable. Sensor networks may also be required in these scenarios, and may employ ad hoc networking techniques for similar reasons.

Unfortunately the flexibility of ad hoc networks comes at the cost of non-optimal performance. There are a number of reasons for this:

- The self-forming nature requires each node to be able to communicate with its neighbours and consequently nodes normally use the same radio channel. In contrast cellular networks increase capacity by careful allocation of channels to cells.

- The self-forming nature also requires nodes to communicate in all directions and hence use omni-directional antennas. In contrast cellular networks use directional or cabled links to connect base stations to the main infrastructure.

Hence we regard ad hoc networks as part of the solution for crisis management, but recognise the need to exploit other techniques when feasible.

Clearly the capacity of an ad hoc networks is limited. This importance of this study is that it sets out to identify techniques that reduce the limitation without reducing the overall benefits of ad hoc networking.

2.3 Findings of the study

The IETF MANET protocols are becoming mature and many implementations are available.

Few other general purpose ad hoc routing protocol proposals are as mature as those on the standards track. Moreover, despite the creation of many proposals over the last decade, the majority appear no better or possibly inferior to the MANET protocols in anticipated scenarios.

Hybrid protocols, that combine proactive and reactive operation (see section 2.1), are immature but offer the prospect of improved scalability and/or the best of the contrasting modes of operation.

Geographic protocols have been proposed over the last 2-3 years but no clear favourite approach has emerged to date. There is notable work by a number of universities and an interesting paper by Rutgers University was found that supports self-positioning using landmarks rather than GPS.

Work on augmenting ad hoc network operation with wireless channel characteristics is ongoing at a number of organisations. Of note is work at BAES which supplements conventional beaconing with signal quality measurements and has been demonstrated out of doors, so can be considered to be approaching maturity.

It has already been concluded in section 2.1 that QoS for ad hoc networks is in its infancy. Moreover there are many different aspects of QoS, ranging from the traditional bandwidth/latency concerns to avoiding security hazards. Some of this work is within the framework of the MANET standards and therefore can be considered to be more mature than the rest, but it is felt that work is still in its infancy and future breakthroughs may not be compatible with the current standards.

Ad hoc networks have already been used in the POS1 trials, including the BAES wireless channel quality sensing techniques. We do not anticipate any of these other developments identified maturing in time for POS2.

To conclude, the basic operation of ad hoc networks is maturing but there are many enhancements such as hybrid routing, geographic assisted routing and QoS that remain immature.

3 REVIEW OF STANDARDS FOR LONG RANGE WIRELESS NETWORKS

This report was produced by BAE Systems, document reference OASIS_2.4_RPT_093_BAE.

3.1 Introduction

This report carried out a technical review of the state of the art for current and emerging standards being developed within Europe and the US for long range high capacity wireless networks. The major emphasis was on the IEEE IEEE 802.16 (WiMAX) standard which is being promoted heavily in the commercial domain and is beginning to make some in-roads into military thinking and trials.

WiMAX operates in two modes, firstly as a back-haul link providing a high capacity throughput (~ 10 Mb/s) over ranges up to 10 km connecting base stations, and secondly as a short range non-line of sight system covering an area of up to 4 km radius from a base station and offering fixed or mobile users (at speeds up to 150 km/hr) a high capacity link (~ 2 Mb/s). These numbers are much reduced from the hype in the press from the WiMAX promoters but are still in excess of what is currently available. The WiMAX specification is for frequencies between 2 – 60 GHz, therefore following the trend of moving up the spectrum to provide higher bandwidth services.

The report notes the convergence of ETSI HiperACCESS / HiperMAN BRAN, WiBro and WiMAX, and in addition IEEE 802.20 (similar to 802.16 but offering high-speed mobility and using a slightly different modulation technology) and 802.22 (cognitive radio providing fixed broadband over UHF frequencies) are briefly discussed.

3.2 Relevance to OASIS

There have been considerable developments in COTS wireless systems over the last two decades, covering cellular systems, line of sight systems and wireless LANs. The technologies offer increasing capacities at relatively low costs due to volume manufacturing. This additional capacity facilitates better information to the front line responders and video back to control rooms which, subject to effective information management, is expected to increase overall effectiveness.

3.3 Findings of the study

WiMAX is the most mature of the IEEE standards studied and is likely to directly compete with 3.xG technologies in 2007/2008. A battle for dominance between the computing industries' WiMAX and the mobile industries' 3.xG services will determine which of these two formats will become most commonplace. At the time of writing the other standards identified seem unlikely to mature at a sufficient rate to challenge these two technologies in all but specialised areas.

As noted in section 3.1, the effective capacity of a WiMAX system is likely to be less than the hype, although the exact capacity will depend upon terrain, equipment quality, etc.

There are a number of suppliers of WiMAX, including Alvarion, Alcatel and Motorola. However the WiMAX standards are very broad (especially in spectrum covered and differing

operating modes) so it is unlikely that any single manufacturer will supply a complete product range. There are a number of trial services based upon WiMAX in Europe and the US.

The study report, completed in February 2006, recommended that the use of a pre-WiMAX standard bearer should be considered for the OASIS POS1 trials to provide experience with the use of the bearer within the OASIS context and paving the way to the use of a ratified WiMAX standard bearer within the POS2 trials. The POS1 recommendation was dropped primarily for cost reasons, covering technology, learning curves and integration. At the time of writing a similar argument will apply to POS2, where the primary focus for most of the partners is upon architectures and integration with legacy systems, but it is nevertheless recommended that WiMAX is tested for the emergency services in a future project.

4 REVIEW OF SECURE MULTICAST PROTOCOLS

This report was produced by BAE Systems, document reference OASIS_2.4_RPT_098_BAE.

4.1 Introduction

Multicast is a technique by which one-to-many and many-to-many communication can be achieved in an efficient manner. The sender transmits each packet once and intermediate routers make copies and forward packets as necessary to the receivers. The main benefit of multicast is that, when the same information is to be sent to many recipients, the technique reduces the computational load at the sender, the total amount of information sent over the network and congestion at hotspots in the network near the source.

Secure multicast is multicast with security, e.g. confidentiality and integrity of the information transmitted, authentication and non-repudiation of the source, avoidance of denial of service, etc. The scope of the report is secure multicast in the context of networks based upon the internet protocols.

The report begins by outlining the standards bodies that are involved in developing the building blocks that will facilitate the development of secure multicast solutions. These work in a framework that consists of the following areas:

- Secure multicast data handling
- Management of keying material
- Multicast security policies

The report then presents a high level overview of some of the published literature in the area.

IP multicast scales well due to its open model where senders can transmit data to a multicast group without any interaction with a centralised entity. However this model makes it difficult to enforce access control, e.g. confidentiality requires the sharing of a common key which may require interaction with a centralised entity. This is one of the major research issues in secure multicast.

In conclusion, although a lot of research has been undertaken in the area of secure multicast, it is still at a relatively low maturity level in terms of deployed systems and available products, although there are a number of initiatives underway to increase this maturity level.

4.2 Relevance to OASIS

Potential OASIS applications of multicast include conferencing, transmission of the operating picture, transmission of orders, distribution of sensor information, simulations, etc. Software updates is another potential application during longer term crises.

A major benefit of multicast is that it improves efficiency because information is transmitted just once rather than N times to reach N recipients. Hence multicast increases the effective network capacity when the information flows are suitable for multicasting or, viewed in a different way, multicast facilitates applications that are not otherwise feasible.

4.3 Findings of the study

Considerable research has been undertaken in the area of multicast and the area is becoming relatively mature but deployment of multicast for civilian applications has been slow, largely due to the current lack of support for traffic management, accounting and billing, and reliability and security.

Surprisingly few freely available implementations of secure multicast were found for download from academic institutions, the current research is focussed at a low maturity level. Moreover only one commercially advertised product for a secure multicast system was found, a system developed by Logica that supports both satellite and terrestrial multicast. As a commercially product this appears to be mature, but a detailed study would be required to confirm this.

Many of the applications of multicast will require reliability, this is especially important for distribution of orders and software. Reliable multicast is a separate standards activity from secure multicast, so there is a need to check the overall status of support for secure reliable multicast.

Multicast routing is still relatively new. Hence the combination of multicast and mobility is likely to be especially immature and is therefore worthy of further study.

5 AVAILABILITY OF SPECTRUM FOR WLANS

This report was produced by Ericsson Microwave Systems, document reference OASIS_2.4_RPT_110_EMW.

5.1 Introduction

The report set out to present an overview of the processes that control the use of the frequency spectrum and the consequences when developing new types of components, systems and standards for wireless communication.

The report covers the working of the ITU-R which produces international Radio Regulations covering 9 kHz to 1,000 GHz (i.e. the practical spectrum for over the air wireless communications). A special application of wireless, called a Safety Service, is reported as “Any radio communication service used permanently or temporarily for the safeguarding of human life and property”.

Demand for spectrum has grown in recent years, driven by the success of cellular communications. Hence spectrum has acquired a value, as evidenced by the phenomenal bids

by operators for 3G spectrum in several European countries earlier this decade. This, together with an observation that spectrum is not always used efficiently, has led to proposals for spectrum trading and also for cognitive radio, notably in the IEEE 802.22 group. The latter is initially focussed upon reuse of television bands (i.e. 54 to 862 MHz), currently driven by requests including location to a central server that is aware of the television broadcast schedule, but eventually leading to methods driven by spectrum sensing.

Recent years have also seen an increase in the popularity of unlicensed spectrum, most notably the 2.4GHz band used by WLAN and other low powered wireless systems. This has the benefit of convenience in that no licence is required, and frequency management is simple, but the spectrum is becoming increasingly congested and there are, of course, no guarantees of capacity.

5.2 Relevance to OASIS

Clearly the emergency services require radio spectrum for operations at the front line. The report indicates that commercial pressures will limit the spectrum available to the emergency services, at least in some countries, and they may therefore have to share spectrum with other users, either using unlicensed spectrum or in the future using cognitive radio techniques.

OASIS is concerned with interoperability, and a particular aspect of this in international crises is sharing particular parts of the spectrum and ensuring that there is no undesirable interference between portable equipment originally intended for national use.

5.3 Findings of the study

There is a conflict between the simplicity of unlicensed spectrum where there can be no guarantees and the complexity and increasing cost of licensed spectrum. The long term solution will be cognitive radio but that is very immature today.

Spectrum management is a key function in military coalition networks and will also be a requirement for crisis management when multiple organisations are involved. Further study is recommended. This should start by listing which frequency bands are in use today by the national rescue services (police, ambulance, fire brigade etc.) within Europe. Furthermore, the maturity level of the standards should be investigated.

6 TESTING PERFORMANCE IN AN OLSR-BASED MANET WITH QOS CAPABILITIES

This report was produced by Thales Norway AS, document reference OASIS_2.4_RPT_113_TNR.

6.1 Introduction

In a separate research project, Thales Norway together with Thales Italy built a research laboratory for mobile ad hoc networks (MANET). This is a test bed based on multi-band technology, combining low bandwidth high radio range UHF and high bandwidth with low radio range WLAN technologies.

This test bed was extended for OASIS work package SP2.4. The goal was to investigate the performance of an ad hoc network with QoS capabilities, i.e. both prioritisation and traffic shaping on the IP layer, and also IEEE 802.11e prioritisation in the MAC layer. The ad hoc routing protocol used was OLSR, one of the IETF proactive protocols.

The test bed consists of four nodes each with two radios, i.e. IEEE 802.11g WLAN and UHF slotted TDMA. There is a network emulator for the WLAN interface, such that the connectivity can be controlled by adjusting the signal levels between each node pair.

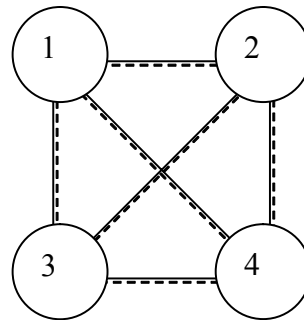


Figure 2. Topology of ad hoc network test bed. Links may be broken in a controlled manner.

Each node consists of a local network with a router using OLSR to select the available radio interface based on the information received from the other OLSR nodes in the network. Traffic shaping is applied to the router in order prevent flooding the low capacity UHF network with data streams that require high data capacity such as video. Each node has a prioritization scheme on the IP-layer, for making sure that the control traffic (such as OLSR) is prioritized before other traffic, in order to provide a stable network.

6.2 Relevance to OASIS

The relevance of ad hoc networks to OASIS scenarios has already been explained in section 2.2. This study is focussed upon the effective capacity of an ad hoc network when there are hidden node problems (i.e. some nodes cannot hear transmissions from other nodes and may therefore cause collisions at intermediate nodes) and the overall capacity of the network is limited by the operating characteristics of the Wireless LAN protocol. This is important to ensure that applications are designed to operate within the constraints of the bearers available.

6.3 Findings of the study

The laboratory test found that the capacity of the WLAN is around 4.8Mb/s when all nodes can hear each other but this drops to about 1.89Mb/s in a hidden node scenario. The traffic limitations for the UHF radio network stopped all broadband traffic but prevented failure in the routing protocol, which would occur if the network were overloaded and cause unstable operation.

The 1.89Mb/s WLAN performance is achieved when the network is configured to use the RTS/CTS handshake, which makes nodes aware when their neighbours are receiving transmissions from hidden nodes. Without the handshake the throughput drops to around 0.4Mb/s.

The importance of not losing routing protocol traffic has already been noted. However it is noted that the challenge is particularly serious because broadcast transmissions are not

acknowledged over WLAN and consequently there are no retransmissions if the first attempt is lost.

The work also observed the importance of signal strength testing, adding further weight to the conclusions about the importance of this topic in section 2.3.

The network cards used in these tests failed to perform QoS prioritizing of the wireless transmission when running in ad hoc mode. This might be related to limited implementation of the 802.11e protocol in the devices that have been used, suggesting that WLAN is less mature in ad hoc mode than in the more common access point mode.

To conclude, the performance of an ad hoc network is a complex combination of the behaviour of the routing protocol, the wireless protocol and the wireless propagation conditions. Even when well configured, the performance of WLAN with hidden nodes which are inevitable in multiple hop topologies is less than half that in a fully connected network.

7 ANALYSING SECURITY SERVICES IN A MANET CONNECTED TO OTHER INFRASTRUCTURE

This report was produced by Thales Norway AS, document reference OASIS_2.4_RPT_114_TNR.

7.1 Introduction

Security is still an unresolved and challenging research topic in mobile ad hoc networks. Security spans a wide range of topics, from encrypting data traffic to ensure confidentiality, to key management systems, to firewalls and access control, to authentication mechanisms for new entities joining and leaving networks, etc.

This study investigates the traditional security services, security threats and basic security functionality as applied to ad hoc networks. In particular the new IEEE 802.11i standard is considered for use as part of a 2-level authentication mechanism. One scheme is used for node to node authentication, a second is used for authentication to an internet gateway when available, bearing in mind that an ad hoc network may become isolated with no connection to fixed infrastructure.

In ad hoc networks there is a debate about whether security should be centralised or distributed. From a security point of view, a centralized approach is preferred for simplicity, for instance regarding key management. However, this introduces a single point of failure and breaks the distributed nature of the network itself. This proposal introduces a combination of a centralized and a distributed system.

7.2 Relevance to OASIS

The case for ad hoc networks in OASIS scenarios was made in section 2.2. This 2-level authentication mechanism adds security capability to the network. The importance of the security objectives below is self evident:

- Confidentiality: the protection of data from unauthorized disclosure.
- Integrity: the assurance that the data sent has not been modified, inserted, deleted or replayed.

- Non-repudiation: protection against denial of involvement by one of the communicating parties that was involved.
- Access control: the prevention of unauthorized use of a resource.
- Authentication: the assurance that the communicating party is the one it claims to be.
- Availability: the property of a system or a resource being accessible and usable upon demand.

These security requirements are generic in that they are required by the majority of OASIS applications. However the open nature of an ad hoc network makes the threat greater and the solution more complex, e.g. if communication is over a physically protected cable then there is no threat of interception and encryption is not required.

7.3 Findings of the study

The proposed 2-level authentication mechanism is divided in two parts; one centralized function using 802.11i, and one distributed using a proprietary mechanism:

- Level 1 (mandatory): Whenever a new mobile node enters the network, a level 1 authentication needs to be completed. The new node broadcasts (one-hop only) a request to join the network. Every node hearing this broadcast will answer with an authentication challenge. The new node chooses one of the answers and completes the authentication procedure. After completion, the new node receives the current group session key and is then member of the network.
- Level 2 (for communication via Internet gateway only): The mobile nodes first complete a level 1 authentication before starting at level 2. The gateway must be deployed with a RADIUS server. After detecting a gateway, the mobile nodes start an 802.11i authentication session by tunnelling their 802.11i messages (EAP messages) to the gateway. This authenticates the new mobile nodes and returns the session key to them.

This proposal requires pre-configuration of security material in both the ad hoc nodes and the gateway, so reduces the speed of deployment, but this is regarded as part of the inevitable cost of security in ad hoc networks.

The ad hoc network nodes communicate using a group session key. This solution is desirable for its simplicity but has problems if the network should split and merge.

The denial of service requirement is particularly difficult to satisfy in an ad hoc network. WLAN is prone to simple low layer attacks such as jamming, and at higher layers attackers can starve networks of resource by repeated security challenges. Jamming has previously been regarded primarily as a threat to military networks, but recent evidence shows that terrorists launch multiple attacks so an atrocity followed by jamming to disrupt the emergency services can be envisaged.

To conclude, security in ad hoc networks is a significant challenge and solutions are currently immature. Widespread use of ad hoc networks in OASIS scenarios is not envisaged until the solutions become more mature.

8 CONCLUSIONS

This document is a summary of six communications research activities that have been carried out in OASIS work package SP2.4 over the period 2005/6. All work has been focussed upon increasing the network capacity and/or improving the security, and the majority of the work has been targeted at responders and sensors at/near the front line. The conclusions in this section should be interpreted whilst bearing this scope in mind.

The original intention was to insert the findings of this report into the POS1 and/or the POS2 demonstration/trials systems. In most cases this has proved impractical due to the timescales of maturing and/or the development budgets. However work by TNR on optimising WLAN configuration is practical if ad hoc networks are deployed in POS2.

Half of the research activities have been concerned with aspects of ad hoc networks. Their basic operation is maturing, but there are many enhancements such as hybrid routing protocols, geographic assisted routing and QoS that remain immature. Their performance is a complex combination of the behaviour of the routing protocol, the wireless protocol and the wireless propagation conditions, and more work is required to characterise their performance in order that they are used effectively. Moreover security in ad hoc network is a major issue and may prove to be a barrier to their adoption in the short term.

Secure multicast was also found to be at a relatively low maturity level in terms of deployed systems and available products, although there are a number of initiatives underway to increase this maturity level. Crisis management applications also require reliable multicast and multicast routing that accommodates mobility.

There have been substantial developments in wireless systems over the last two decades. Price/capacity ratios continue to improve with new technologies such as WiMAX and experiments are recommended to increase the maturity for emergency scenarios.

There is a conflict between the simplicity of unlicensed spectrum where there can be no guarantees and the complexity and increasing cost of licensed spectrum. The long term solution is expected to be cognitive radio but that is very immature today.

Spectrum management is a requirement for crisis management when multiple organisations are involved with their own equipment. Further study is recommended, including listing which frequency bands are in use today by the national rescue services within Europe and assessing the maturity levels of the standards used.

9 SUMMARY OF RECOMMENDATIONS

- Ensure that the POS2 WLANs are configured as recommended by PERF
- Develop a route map in ad hoc network security and develop new solutions if necessary
- A new project (or subproject) focussed upon spectrum management issues in crisis management
- Develop a “cook book” to help predict ad hoc network performance under a broad range of operating conditions
- Arrange WiMAX trials for emergency scenarios
- Develop a route map for reliable multicast and multicast routing with mobility support