The UK government's Critical National Infrastructure policy for emergency services communications platforms: Vulnerabilities in the TETRA Architecture

Devon Bennett, Hamid Jahankhani, Hossein Jahankhani

University of East London, School of Computing & Technology, UK
{D. Bennett, Hamid.Jahankhani, H.jahankhani}@uel.ac.uk

Abstract: In this era of global communications individual communities and entire cities rely heavily on the public telecommunication platforms to support the emergency services workers to provide a professional service in extreme situations, such as natural disasters - floods, earthquakes and hurricanes etc; or terrorist / political attacks, such as London, New York and Madrid. Previous experiences have demonstrated that in such situations entire cities find their general communication platforms such as the Public Switched Telephone Networks and Cellular systems are overwhelmed with emergency communication traffic, as huge number of calls are made locally and internationally to the disaster area to determine if love ones are injured or safe. Until recently under these extreme conditions the emergency services would have to rely solely on the available telecommunications bandwidth and any contingency bandwidth that has been allocated for such situations. However the UK government has a part of its Critical National Infrastructure as deployed a TETRA based private mobile radio (PMR) system to separate critical emergency communication from the general communication platforms. This paper analyzes whether this new system is resilient or could the use of MANET's be utilised to operate in extreme situations to provide a crucial short/mid-term communication platform.

Keywords: CNI, TETRA, MANET, global Communications, natural disaster

1. Introduction

Today the emergency services are looking to the telecommunications and IT industries to provide them with the technological resource to function effectively in situations of man-made or natural disasters. In such situations the public voice and data communication infrastructure can be severely compromised, one such situation is the 9/11 terrorist incident, in the United States. Where research as shown that the inadequacies of the emergency radio communications infrastructure, was a major contributing factor to the loss of 120 New York fire-fighters (BWCS, 2002). Similar research both in the UK and Europe has found the old analogue radio networks demonstrated the same bandwidth inadequacies with congested airwaves, bad reception, and loss of signal (BBC News, 2002), during similar situations.

In Manchester in 2004 a tunnel fire occurred 30 metres below ground damaging two main BT telecommunications supply cables, resulting in severing voice and data communications to over 130,000 customers and affecting telecommunications service in a vast geographical area covering Cheshire, Merseyside, Lancashire and North Derbyshire (BBC News, 2004). One of the worst affected emergency services was the Manchester ambulance service, which found itself under extreme operational pressures as the tunnel fire had damaged its radio network; in this situation the Manchester ambulance service resorted to using mobile phones to communicate with ambulance staff in the field, but were unable to receive any public 999 emergency calls until the fire was extinguished and communications could be rerouted to other switching stations.

Over the last few years we have seen a number of natural disasters, where such incidents as; the devastating floods in Worcestershire, UK in both 1998 and 2007, the Sichuan earthquake in China and the recent earthquake in the Italian city of L'Aquila. These disasters not only severely tested the national and international telecommunication structures , but in some cases completely destroyed the communication infrastructure in the affected areas. Resulting in the inability of the emergency services to react and organise themselves; whilst managing the sense of panic and anxiety, which is commonplace amongst the general population in the disaster zone; in addition to getting badly hurt survivors to medical help as soon as possible.

The ability for the emergency services to mobilise and organise efficient cross communication procedures is crucial and in such cases mobile ad-hoc networking can be critical to the delivery of a high quality service that is capable of coordinating the incident / rescue effort in the most cost effective and efficient manner possible. This implies that the emergency services must be capable, under these circumstances, of quickly achieving a high-level of inter-services communications without the assurance of a fully operational telecommunications platform.

The governments of both Europe and the UK have taken these natural and man-made threats to the national security communications infrastructure seriously and have developed systems to combat these types of threats; by introducing a policy of transferring all emergency communication from the PSTN services to a digital TETRA based private mobile radio network and public access mobile radio network (ETSI, 2000).

In Europe the emergency services network is called the C2000 (Motorola, 2001) and in the UK the system is called the 02 airwave (Cable & Wireless, 2004). In the UK the 02 airwave system forms part of the UK governments strategic Critical National Infrastructure policy, which was developed after the 2001 terrorist incidents to provide a comprehensive solution to combat terrorist attacks on the countries electronic communications infrastructure.

These new emergency services communications platforms are generally called Public Safety Networks and their initial objective is to achieve signal coverage across a country, homogenising the regional communications of that country, between the ambulance services, police services and the fire brigade. These systems are digital radio systems that are a vast improvement on the old analogue radio networks previously used by the emergency services.

In the UK and Europe the private mobile radio networks are based upon the TETRA standard, the TETRA standard is a European wide standard for radio communications of the public safety and emergency services networks (ETSI, 1995), like GSM is the standard for mobile voice communication systems; TETRA is the equivalent standard and was developed by the European Telecommunications Standards Institute (ETSI, 2000).

2. The TETRA Private Mobile Radio network architecture

The acronym TETRA means the TErrestrial Trunked RAdio system and is a modern digital private mobile radio (PMR) and Public Access Mobile Radio (PAMR) technology used exclusively for the police, ambulance and fire service and other national and public safety organisations (ETSI, 2007). The service was first deployed in 1997, but it was not until 2006 that the PMR and PAMR systems took an increased share of the market, this increased share can be directly attributed to the UK Critical National Infrastructure policy and the EU equivalent European Programme for Critical Infrastructure Protection (EPCIP), which adopted the TETRA standard for the rollout of the emergency services private mobile radio network (PMR) for all police, fire and ambulance services communications. Now the TETRA standard and services have been adopted by numerous countries outside the EU and is presently deployed in 88 countries around the world. Interestingly the TETRA standard is not used in North America, but discussions are taking place to license the technology in the near future (Pandata Corp, 2009).

In Europe two of the best examples of public safety networks are the Motorola C2000 system in the Netherlands and the 02 Airwave system in the United Kingdom.

The 02 network is a secure digital radio network that supports intelligent networking, via Telsis® fastSSP intelligent switches installed in secured locations throughout the United Kingdom. They support QSIG signalling to route traffic via private circuits to airwave handsets anywhere in the UK (Telsis, 2004).

The 02 airwave intelligent networking platforms is one of the biggest emergency and public safety networks in Europe. It forms part of the United Kingdom's HMG Critical National Infrastructure, which is the largest of its kind in Europe. The UK's HMG Critical National Infrastructure was designed to cope with the excessive loads experienced during major incidents, where the conventional cellular and fixed wired telecommunication systems may fail due to traffic overloads.

In the UK the 02 airwave communications platform is owned by mm02 plc, which have out-sourced the core transmission network infrastructure to Cable & Wireless, for provision of its Ground Based Network (GBN). The Cable & wireless /02 airwave network is a fixed line backbone core network, that consists of a mesh STM-4 link at 622Mbps, connecting seven core switching sites, that in turn connect over 100 police control rooms across the UK. Because this structure is a mesh it is highly resilient; if a switching site goes down then all the circuits to that site can be re-routed within minutes (Cable &wireless, 2004), via the mesh structure. Other benefits provided by this network are:

- The network is based on the TETRA standard

- The radio network operates on the 380MHz to 400MHz band.
- It caters for speech, data, and image communications on the same infrastructure.
- All the radio sites are connected via an extensive ground based network, using Kilostream links.
- mmO2 , as the service provider, procures, installs, maintains and manages the entire network via a number of network and service centres.

The 02 airwave network was originally rolled out to the police forces in the UK, and in March 2005 this process was completed. Allowing all the police forces in the UK to move from their outdated analogue radio systems, which were generally procured 'bespoke' for each force. To a fully digital and integrated state-of-the-art public safety network, that provides a wealth of new facilities:-

- Access to local and national databases leading to better and faster provision of information to Officers.
- Secure communications, contributing to combating crime and safeguarding information from unauthorised access (analogue scanners operated by some criminals, will not be able to listen into police radio traffic).
- Digital voice quality, reducing any possible misunderstandings in messages.
- One terminal acting as a radio, mobile telephone, and data terminal leading to time savings (certain facilities are generally available to all users but the system is tailored to suit the Forces needs).
- Automatic Vehicle and Person location leading to quicker responses, more efficient use of resources and improved Officer Safety.
- Comprehensive Management Information enabling the best management of our limited operational resources.
- Interoperability providing seamless voice, data and image communications, across the country and across organisational & geographical boundaries

(Taken from Fife Constabulary - http://www.fife.police.uk/)

Although the 02 airwave network was initially rolled out to the police forces and the military police; a number of ambulance trusts, fire brigades, and county councils have moved to the 02 airwave network. This has become more crucial as the UK government will withdraw support of all of existing analogue VHF radio frequencies used by the emergency services, by the end of 2009.

One such example is the Shropshire Fire & Rescue service (Sepura, 2005), which migrated its old analogue radio communications system for the 02 airwave TETRA secured digital radio communication system, using the TETRA enabled Sepura in-vehicle mounted terminals and Sepura mobile handsets for mobile fire and rescue personnel. The Shropshire Fire & Rescue service (SFRS) is situated in the largest landlocked county in the UK and has approximately 550 fire fighters, officers, and control room staff set across 33 fire stations in the county (Sepura, 2005). In addition the SFRS has over 80 fire and rescue vehicles each one has the Sepura in-vehicle TETRA terminals, with direct communication to one or other incident control room.

Because the SFRS has adopted the 02 airwave system, they have found that in addition to the increased voice communication clarity of the digital system, when compared to the problems of the old analogue system. The 02 airwave system provides the facility for the Shropshire Fire & Rescue Service to talk directly to the police service, as all police forces in the UK have rolled out the 02 airwave system for their services use.

This is achieved by the Sepura handsets and terminals used across both services and the ability to define and setup 'talk-groups'. Talk-groups are used to provide inter-agency communication between the services and the secured nature of the 02 airwave TETRA platform means that the possibility of unauthorised persons eavesdropping is eliminated. In Shropshire these talk-groups have now been setup for specific fire-to-police communications, which are used in emergency incidents for emergency situation management and cooperation between the fire and police services.

Another advantage provided to the SFRS is the TETRA handset that has integrated in it the Global Positioning System (GPS), which provides both the police and emergency services the ability to locate their personnel in adverse and emergency situations. One such good example of the use of GPS in the SFRS is the water rescue service which has began to use the handsets GPS to monitor their personnel's positions in dangerous rescue operations.

With this increase in intercommunications and the ability of the emergency services to construct cross-services talk-groups etc, it would seem the use of MANETs would be unnecessary as the 02 airwave systems appears to provide all the necessary facilities to support the emergency services in any situation. This would be a short-sighted approach as the 02 airwave system is a still primarily a fixed line backbone core network, which does provide resilience in its ability to reroute circuits via its mesh architecture to one of the seven core switching site across the country. However as we see from the tunnel fire experienced in Manchester in 2004, or in Hampshire in 2002 where vast areas experienced a major communication problems, simply because the network infrastructure experienced a fault these land line based systems are vulnerable to outages and loss of facilities, no matter how short.

In the case of a major terrorist or national disaster, as the recent earthquakes in Italy and China, the telecommunications industry would not simply be in the process of trying to correct a fault, but could be in the midst of having to rebuild part or all of their entire infrastructure. A dynamic mobile communications platform such as the MANET could be one of the few methods of providing localised mission critical data communications, on the ground, in such situations.

3. Mobile Ad-Hoc Networks and Multi-hop Routing

A MANET environment is not the tried and test environment of the Wireless Local Area Network (WLAN), where the WLAN provides a point-to-point connection from the client to the network infrastructure via a network access point; a MANET consists of a dynamically organised network, with a constantly changing topology or shape (Murthy & Manoj, 2004); within a defined geographical area. This is because a MANET environment leaves all the routing and authentication responsibilities to the

client workstations in the network. A wireless local area network (WLAN) does provide mobility but differs from a Mobile Ad-hoc Network in that it is primarily connected to a network access point that provides all the routing and authentication responsibilities of the network (Stallings, 2002) . The AP is responsible for testing the connection status and signal quality and will handover to another AP as the device moving from one AP range into another; this is not true of a mobile ad-hoc network.

Mobile Networks (MANET) has been around for some time but was exclusively used in the past for military uses (DARPA, 1973). The roots of the mobile network technology can be traced back to the 1970's when the Defence Advanced Research Project (DARPA) introduced the Packet Radio Network (PRNet), and in the 1980's the Survivable Adaptive Network (SURAN). These networks were designed for use in military situations under battle conditions and it was therefore necessary that these networks were resilient and would not share information with unauthorised personnel (Kahn, 1978).

This type of network was expected to be rapidly deployed without relying on a pre-existing fixed network infrastructure, under extreme conditions. This in practice meant that these relatively high-speed networks were integrating communications between different command levels, from the division to the brigades, on the move and in extremely short periods of time (Murthy & Manoj, 2004).

The modern/commercial term for this type of platform is the Mobile Ad-Hoc Network (MANET), where the commercial definition is such that a wireless ad-hoc network is a group of dynamic client nodes that has no infrastructure and are responsible for providing routing, authentication and security functions amongst themselves and within a given coverage area. The nodes in a MANET can dynamically join and leave a network frequently, and without warning, but should aim not to interfere with the other clients in the network. Finally the nodes in a MANET can be highly mobile and because of this a MANET environment has a continuously changing topology as links are constructed or broken dynamically (Haas et., 2001). This definition becomes cloudy when the wireless device interacts with a fixed infrastructure / environment either via RF frequency, cellular, or Satellite interface as all these facilities could be considered as providing wireless interfaces to a fixed environment and not the dynamically constructed network of an ad-hoc environment. The crucial objective of an ad-hoc network is the ability for client devices to take on trust and routing responsibilities with the ability to exchange information with other client devices when there is a complete absence of a client/server infrastructure has defined in a fixed environment.

As stated the nodes in a MANET exhibit nomadic behaviour by freely migrating within a coverage area and dynamically creating and tearing down associations with other nodes. It is these characteristics that differentiate a MANET from any other type of network, by rapidly and continuously changing its shape. In some cases nodes that have a common goal create formations together called clusters, where they are able to migrate together (Haas et, 2001). A MANET is a peer-to-peer network that allows direct communications between any two or more nodes, when there is adequate radio signal to send information between each other and there are no power limitations. This is very different to the WLAN architecture that is a point-to-point network where the client connects to the network via a P-T-P link to the access

control point (AP). In a MANET network if there is no direct link between the source and destination nodes a process called multi-hop routing is used.

3.1 Multi-hop Routing

Multi-hop routing is where packets are sent from one node to another; even in the case where a source node cannot directly connect to a destination node a packet can still be sent via the multi-hop process (Stallings, 2002). In figure 1, we can see that source 'A' wants to send a packet to destination 'C', 'A' can communicate with 'B' but cannot communicate with 'C' directly. Source 'A' simply sends its packet to device 'B', which in turn forwards the packet on to its destination 'C'

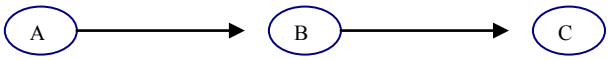

Figure 1: Multi-hop packet forwarding

The most difficult aspect of developing a MANET environment is the operation of the network when compared to the traditional wireless network, this is because there is no centralized entity in a MANET (Murthy & Manoj, 2004); and therefore there is no central component that can be used for routing and authentication. The potential for constant and rapid movement of the client nodes and the main weakness is that all communication – ie. Data, authentication, or encryption transmission – is carried over the wireless medium. The lack of these entities mean that MANET's require distributed algorithms for routing and authentication function, as opposed to the traditional algorithms used on traditional WLAN's.

3.2 Routing Protocols for MANET's

In traditional networks routing protocols can be divided into two categories either proactive or reactive. Proactive routing protocols such as the traditional link-state or proactive distance-vector protocols learn the topology of the network by continuously exchanging topological information among the network nodes (Murthy & Manoj, 2004). With this process all nodes are constantly updated with the routing topology and when a route is required by a node it is immediately available. Because of this process of constantly updating the routing tables these protocols are sometimes referred to as table-driven routing protocols. The early proactive protocols that were used for ad-hoc networks were distance vector protocols based on the Distributed Bellman-Ford (DBF) algorithm (Perkins & Bhagwat, 2001). This did not work out very well as distance vector protocols produce convergence and excessive control traffic overheads, resulting in slow transmission rates.

On the other side of the spectrum are the reactive routing protocols which are based upon a query / reply procedure. Reactive protocols do not attempt to continuously maintain the current topology of the network; instead when there is a requirement for a route a reactive protocol will invoke a procedure to find a route to its eventual destination. This procedure involves the protocol flooding the network

with a route query, because of its operational manner these types of protocols are referred to as 'on-demand' protocols. There are numerous routing protocols in the market for ad-hoc networks, but for the purposes of this paper we will discuss the Proactive (Table-driven) protocol.

4. Proactive Routing Protocol for MANETs

Proactive or table-driven routing protocols are simply protocols that are extensions of the traditional wired network protocols, such as Link-State routing protocols. As in wired networks, proactive protocols maintain a global topology of the network in the form of routing tables, at each and every node. These routing tables are updated frequently in order to maintain accurate and consistent network state information (Haas et., 2001).

4.1 Destination Sequenced Distance-Vector routing protocol

The Destination Sequenced Distance-Vector (DSDV) routing protocol was one of the first routing protocols used for ad-hoc networks. It was an enhanced version of the Distributed Bellman-Ford (DBF) Distance Vector routing protocol, where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node on the network (Murthy & Manoj, 2004). DSDV combines incremental sequence numbers with table updates to prevent loops and to counter the count-to-infinity problem. Because DSDV is a table-driven protocol, every node on the network has a view on all routes to all destinations; as during regular intervals routing tables are exchanged between neighbours, by a process of flooding the network with routing updates (Perkins & Bhagwat, 2001).

DSDV provides two types of routing updates either an event-driven incremental update or a periodic full-table update. An incremental routing update consists of the protocol sending a single network data packet unit (NDPU), whereas a full-table update may contain multiple NDPUs. Generally an incremental update is used by a node when there are little or no changes to the topology; a full update is used when a node is aware that the local topology has changed significantly.

Routing table updates are initiated by a destination node that transmits an update next-hop table with a new sequenced number that is greater than the previous update. When a node receives this new next-hop table update from its neighbour it can perform two actions either to update its table to show the new destination, if the sequence number of the update is higher then the previous update. Or store the update to compare it against the multiple versions of the same updates from the neighbouring nodes, to determine the best metric – which could be the shortest number of hops or cheaper cost route. In addition to reduce the control message overheads DSDV provides a time-to-settle metric, which is an estimated settling time for each route to complete (Perkins & Bhagwat, 2001). Therefore a node will only send an update of a route to its neighbour if the settling time of the new route has expired and the route is the best option.

DSDV protocols require each node in an ad-hoc network to advertise to each of its neighbours its own routing tables by broadcasting its entries. Because of the nature of MANETs the entry lists may change quite dramatically, so it is important

that the broadcasts are made often enough so that every mobile node can almost always locate every other node in the network (Murthy &Manoj, 2004). In addition each node in a DSDV enabled mobile network, must agree to relay data packets on request; this is extremely important in terms of determining the shortest path for a source route to its destination. DSDV also has the ability not to disturb mobile nodes that are in the 'sleep' mode and if a node is asleep then DSDV will still exchange information with all the other mobile nodes in the coverage area, even if the destination for the data is not within range for direct communication.

A DSDV broadcast packet consists of the ;

- Destination address,
- Number of hop require to reach the destination
- A Sequence number

A routing table update consists of the hardware address and the network address of the transmitting node within the header of the packet, plus a sequence number transmitted by the source node. As stated above routes with the more recent or higher sequence number are always preferred as the basis for updating the routing tables and making forwarding decisions. With the above mechanisms DSDV provides a vast improvement over the Bellman-Ford Distance Vector protocol, by eliminating route-looping, by reducing control message overheads and increasing the speed of convergence.

4.2 The Cluster-Head Gateway Switch Routing Protocol

The Cluster-Head Gateway Switch Routing Protocol (CGSR) organises differently to the DSDV routing protocol as it employs the use of a hierarchical network topology as opposed to the flat network topology of the other table-driven routing protocols. In CGSR structure nodes in a given coverage area forms themselves into clusters. Each cluster provides coordination functionality between all nodes in the cluster via a management node called a 'Cluster-head'. A cluster-head node is elected dynamically by employing a 'least cluster change' (LLC) algorithm (Murthy & Manoj, 2004). The LCC algorithm determines that a cluster-head node will only change its status if it comes into range of another cluster-head node that has a higher node ID or a higher connectivity algorithm, as shown in fig 2.

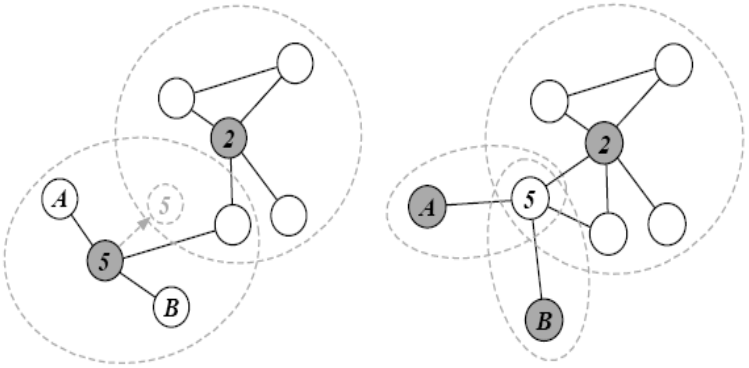

Fig2: Cluster-head status change (Taken from Krishna et, 1997).

In the cluster all routing between nodes in the cluster is managed by the cluster-head, therefore all member nodes in the cluster are able to be reached by the cluster-head node in a single hop. When routing information between clusters it is a node called a cluster gateway (Krishna, et, 1997) that provides this facility; a gateway is a node that is simultaneously a member of two clusters (as in Fig 3).

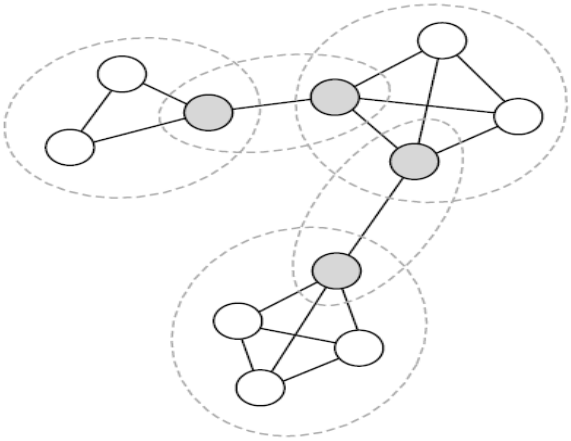

Fig 3: Gateway for CGSR routing (Taken from Krishna et,).

Clustering provides a mechanism for the allocation of bandwidth between clusters, which is a limited resource in ad-hoc networks; it achieves this by allowing different clusters to operate at different spreading codes (channels) on a CDMA system (Hollerung, 2004). Within a cluster it is the cluster-heads responsibility to coordinate the channel access via the use of a 'token-based' protocol. This token-based scheduling is used within the cluster to manage access to the shared bandwidth, by all the members in the cluster. This bandwidth sharing is achieved by assigning access tokens to all member nodes in the cluster.

The CGSR routing protocol assumes all communications within a cluster passes through the cluster-head and any communication between clusters are routed via the cluster-gateways. A gateway could be considered to be a more sophisticated device has it is required to listen to multiple spreading codes that are in operation in the clusters to which the gateway is a member. Conflict at this stage can happen when a cluster-head node sends a token to a gateway over a spreading code when the gateway is tuned to another code. To avoid this situation gateways were developed to communicate simultaneously over two interfaces to avoid these types on inter cluster communication conflicts (Krishna, et, 1997).

CGSR routing is based upon the DSDV routing protocol, where every member node maintains a routing table containing the destination cluster-head for every node in the network (Murthy & Manoj, 2004). In addition each member node maintains a routing table containing a list of next hop nodes for reaching every destination cluster. When a node has packets to transmit it must first be issued with a token from the cluster-head, then obtain the destination cluster-head and the next-hop node from its cluster member routing table and the destination routing table, before it can transmit.

With its hierarchical routing capabilities CGSR provides many improvements to the flat network topology employed by other protocols. It enables a level of coordination between the clusters by electing Cluster-Head nodes and provides an increase in the utilisation of the available bandwidth. It also suffers from the problems of WRP and DSDV when used in a highly mobile environment, where the rate of change of cluster-heads increases greatly as the network grows (Murthy & Manoj, 2004). Also to elevate the problems of excessive gateway conflicts it is necessary to increase the number of interfaces which in term will increase the resource costs and finally because the power consumption at the cluster-head nodes are far higher than at the ordinary member nodes. There is a tendency for frequent changes of cluster-head nodes as these nodes are drained of power, which could result in a high level of

Conclusion

The UK government has vastly improved its ability to protect the countries communication infrastructure by the introduction of the critical national infrastructure policy; the main objective was to protect the strategic IT and telecommunication architecture under extreme conditions from such major national disasters as flooding, tornados, hurricanes and earthquakes. In addition to man made disasters such as terrorist attacks experienced by numerous countries since 9/11 in New York and 7/7 in London.

The introduction of the TETRA communication network provided the government with an answer to the extremely congested PSTN and mobile cellular network, as experienced under extreme conditions, where both in the UK and USA the emergency services were unable to communicate with their respective HQ and in some cases each other; with a parallel TETRA based private mobile radio system.

The TETRA system provides the emergency services with numerous benefits such as clear digital communication, digital integrated handsets, location awareness, digital images and seamless voice / data communications across the country with other emergency services. This was not possible with the old analogue services as the majority was procured as 'bespoke' systems for individual emergency services.

However even with these major improvements the government has still based its policy on a system that is still a fixed backbone cellular infrastructure, that controls and manages its main connections and transmission of data via a number of switching station located on (under) the ground across the country. This does provide some systems integrity by having the ability to rerouted communications to sites that are not affected. But in situations where underground switching stations have been damaged, as demonstrated in Manchester, Lancashire and North Derbyshire in 2004 (BBC News, 2004). These switching stations can be made inoperable for hours and in some cases days, before services are effectively rerouted to other functioning switching stations.

In the situation of major flooding incidents as experienced in Gloucestershire July 2007 (BBC News, 2007), The ability for the emergency services to mobilise and organise efficient cross communication procedures is crucial to saving life and managing hysteria; in such cases mobile ad-hoc networking can be critical to the delivery of a high quality service that is capable of coordinating the incident / rescue effort in the most cost effective and efficient manner possible. The ability to utilise a number of laptops, PDA's and handheld devices to implement a dynamic network without the need for a fixed network infrastructure, to share biometric, database and medical record would be invaluable in such situations. With the use of multi-hop routing protocols such as the cluster-head protocol; these short-term dynamically generated networks could be organised in a h ierarchical structure to enable information sharing amongst emergency services personnel, in entirely flooded areas where the TETRA switching stations would be inoperable.

In addition MANET's are able to utilise what little available cellular / GPS bandwidth that is present by bridging a connection to a cluster-head node and the (available) telecommunications interface; enabling data transfer between the EMS HQ and the rest of the nodes in a MANET network. There is still a great deal of work that needs to be undertaken before MANET's are seen as a viable addition to the emergency services communication platform, but as a short-term dynamic communication platform there is no better alternative.

References

Bhagyavati, Summers, W. DeJoie, A. (2004) Wireless Security Techniques: An Overview InfoSecCD Conference '04, September 17-18, 2004, Kennessaw, GA, USA. Copyright 2004 ACM 1-58113-000-0/00/0004.

BWCS Consulting – Press Release (2002)

UK Emergency Services Voice Concerns Over Radio Systems in Face of September 11th Scale Disaster. (17/09/2002, BWCS Staff)Cable & Wireless – Press Release http://www.bwcs.com/news_detail.cfm, Viewed 15/08/2007

O2 AIRWAVE APPOINTS CABLE & WIRELESS FOR BANDWIDTH PROVISION
http://www.cw.com/media_events/media_centre/releases/2004/06_01_2004_59.html
Veiwed 23/09/2007

Corson, M.S. and Ephremides, A. - A Distributed Routing Algorithm for Mobile Wireless Networks, ACM/Baltzer Wireless Networks, Vol. 1, pp61-81, February 1995.

DARPA (1973) Packet Radio Networks

ESTI (1995) – European Standards Telecommunications Institute - Terrestrial Trunked Radio (TETRA), http://www.etsi.org/WebSite/Technologies/TETRA

ESTI (2002) – European Standards Telecommunications Institute - Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2
http://www.etsi.org/WebSite/Technologies/TETRA, Viewed 16/11/07

ESTI (2007) – ETSI TETRA (Terrestrial Trunked Radio) technology
http://www.etsi.org/WebSite/Technologies/TETRA, Viewed 16/11/07

Gafni, E. & Bertsekas, D. – Distributed Algorithms for Generating Loop-free Routes in Networks with Frequently Changing Topology, IEEE Transactions on Communications, vol.29, no.1, pp. 11-15, January 1981

Geier, Jim (1999) Wireless LANs: Implementing Interoperable Networks, Macmillan Technical Publishing

Hansen, John (2002) 802.11a/b A Physical Medium Comparison, RFDESIGN : RF and Microwave Technology for Design Engineers

Hollerung, T.D. (2004) The Cluster-Based Routing Protocol: University of Paderborn

Haas Z.J, Deng.J, Liang. B, Papadimitratos. P, and Sajama. S (2001) Wireless Ad-Hoc Networking, http://www.ece.cornell.edu/~haas/wnl/html / Viewed 17/08/2007

Haas et al., The Interzone Routing Protocol (IERP) for Ad Hoc Networks, Internet Engineering Task Force (IETF) MANET Working Group, Internet Draft, Jun. 2001.

IEEE Standard 802.1x – Port Based Network Access Control
http://www.ieee802.org/1/pages/802.1x.html, Viewed on 21/6/2007

IEEE standard 802.15.4, IEEE standard 802.15.4-2006, http://www.ieee.org/getieee/download/802.15.4-2006.pdf, Viewed 10/09/2007

ISFL.org.uk, Information Security for London – Warning, Advice and Reporting Point (WARP), http://www.lcwarp.org/

Johnson, D.B. and Maltz, (1996) Dynamic Source Routing in Ad-Hoc Networks in Mobile Computing, Kluwer Academic Publishers, 1996

Kahn, R. (1978) Kahn, R. Advances in Packet Radio Technology. Proceedings of the IEEE 66:1468-1496,

Krishna, P., V aidya, N.H., Chatterjee M., and Pradhan, D.K. A cluster-based approach for routing in dynamic networks, ACM SIGCOMM Computer Communications Review 27:49-65, 1997

Manoj, B.S. & Baker, H. (2007) Communications Challenges in Emergency Response, Communications of the ACM

Motorola, (2001) C2000 The Netherlands Digital Radio Networks for Public Safety www.motorola.com/governmentandenterprise/contentdir/en_GB/Files/CaseStudies/c2000.pdf, Viewed 10/09/2007

Murthy, C.S.R & Manoj, B.S (2004) Ad Hoc Wireless Networks: Architecture and Protocols, Pearson Education: Prentice Hall Publications

Murthy, S & Garcia-Luna-Aceves, J.J. (1996) An efficient Routing Protocol for Wireless Networks - Baltzer Journals.

Proxim Corporation: (2003) White Paper – Wireless Network Security, http://www.openxtra.co.uk/articles/wep-weakness.php

Schiller, Jochen (2003) 2nd Ed. Mobile Communications, Addison Wesley Publications

Stallngs, William (2002) Wireless Communications and Networks, Prentice-Hall, USA

Stallings, William (2003) Cryptography and Network security, Prnetice-Hall, Pearson Education inc. USA

Sepura.com, Sepura Case Studies – West Yorkshire Police (2005), http://www.sepura.com/case-studies-detail.php?caseid=12

Sepura.com, Sepura Case studies - Lancashire Fire and Rescue (2005), http://www.sepura.com/case-studies-detail.php?caseid=9

Sepura.com, Sepura Case studies - Shropshire Fire and Rescue Service (2005) http://www.sepura.com/case-studies-detail.php?caseid=11

Tijssens, M. (2003) Implementation of GRN's in Europe, www.euro-police.com/pdf/tijssens.pdf, Viewed 08/11/07

Telsis.com, Press release (2004) Critical Role for Telsis in 02 Airwave Network, http://www.telsis.com/0218.htm Viewed 04/07/2007

Telsis.com, Press release (2005) Telsis wins emergency services network expansion contract, http://www.telsis.com/0297.htm Viewed 04/07/2007

Walker, J. Cam-Winget, M. Housley, R. Wagner, D. (2003): Security flaws in 802.11 data link protocols. Communications of the ACM46(5):35-39 (2003)

Wilson, J. (2005) The Next Generation of Wireless LAN Emerges with 802.11n, Intel Publications – Technology @Intel Magazine