

2005

Knowledge management through mobile networks in emergency situations

H. Pousti

University of Wollongong

Helen M. Hasan

University of Wollongong, hasan@uow.edu.au

Publication Details

Pousti, H. & Hasan, H. M. (2005). Knowledge management through mobile networks in emergency situations. Proceedings of the International Conference on Mobile Business (ICMB) 2005 (pp. 573-580). Los Almitos, CA: IEEE Computer Soc. Copyright IEEE 2005.

Knowledge management through mobile networks in emergency situations

Abstract

This paper concerns public emergency situations, which are the responsibility of a select set of organisations in the public, private and community sectors. It reports on an analysis of the knowledge management implications of mobile networks, using wireless technology designed for such situations. This follows the path of a research project concerning the need to integrate technological, logistical and organisational knowledge management issues within and between organisations with regard to their response to emergency situations. The analysis of a secondary case is used to illustrate and analyse the issue using a realistic and holistic approach.

Disciplines

Business | Social and Behavioral Sciences

Publication Details

Pousti, H. & Hasan, H. M. (2005). Knowledge management through mobile networks in emergency situations. *Proceedings of the International Conference on Mobile Business (ICMB) 2005* (pp. 573-580). Los Alamitos, CA: IEEE Computer Soc. Copyright IEEE 2005.

Knowledge Management through Mobile Networks in Emergency Situations

Hamidreza Pousti and Helen Hasan
Information Systems, University of Wollongong
hasan@uow.edu.au

Abstract

This paper concerns public emergency situations, which are the responsibility of a select set of organisations in the public, private and community sectors. It reports on an analysis of the knowledge management implications of mobile networks, using wireless technology designed for such situations. This follows the path of a research project concerning the need to integrate technological, logistical and organisational knowledge management issues within and between organisations with regard to their response to emergency situations. The analysis of a secondary case is used to illustrate and analyse the issue using a realistic and holistic approach.

1. Introduction

Now, more than ever, security and safety issues are of importance and relevance to every organisation. This paper addresses the direct preparation for, and response to, public emergency situations, which are the responsibility of a select set of organisations in the public, private and community sectors. However it has broad lessons for all businesses.

Within the set of frontline organisations there is a need for cooperation combining complementary knowledge, skills and capability in dynamically changing environments that threaten life, property and business. Critical decisions, which could have dire consequences, are made moment by moment by various, often uncoordinated, individuals and groups; based on incomplete and conflicting information. There is rarely time to make rational assessments or prioritise problems, which are continually changing in any case, so that there is little chance of reaching optimal solutions. However, it is imperative that an effective course of action is taken, the direction of which is dictated as events unfold.

This paper results from an analysis of the knowledge management (KM) implications of wireless technology being designed for critical public safety situations. It

follows the path of a research project into the need to consider and integrate technological, logistical and organisational KM issues within and between organisations with regard to their response to emergency situations. KM is important for the deliberate activities of planning and preparing for such unwanted eventualities as well the reviews that occur afterwards to determine the lessons learnt. However, the focus here is on the capability to act during catastrophic events, which have their own particular needs and characteristics when normal competitive business activity is suspended and there is the urgency to unite in facing a common threat.

2. Background Issues and Concepts

The news in recent years has been full of natural disasters, terrorist/criminal attacks, wars and accidents, many of which occur suddenly, are unexpected and often unanticipated and result in untold damage, suffering and grief. Whether at a local, national or international level, these events require a rapid response involving the instant co-ordination of people, teams and equipment from many different organisations. These include various police forces, fire brigades, medical personnel, government and non-government agencies and so on. While the emergency response organisations are trained and prepare for such contingencies, every catastrophe has its own unique set of circumstances and conditions that challenge the response. Other groups of people are also involved, such as the media, local authorities and the public at large. Decisions on appropriate courses of action have to be made under stress, in real time and often with incomplete and conflicting information.

Following a major emergency involving threats to public safety, enquiries are conducted through which lessons are learnt. This results in improvements both to technologies that can assist in these situations and in knowledge on how people make decisions and act. This study aims to add to the understanding of the technologies, human issues and whole socio-technical systems formed in emergency situations.

The study began with a broad objective: to gain a better understanding of KM with wireless technologies, which are rapidly being taken up in organisations without concern for their implications for KM. After several attempts at finding a focus for the project, the researchers encountered an R&D team of a commercial organisation developing wireless technologies with the specific capabilities for critical public safety contexts. In this project, the attention was wholly on the technology and its capability with no consideration of its implications for use by people. We identified the need for a KM viewpoint that was not being addressed and where the human and social elements would be dealt with. In doing this, we adhere to these definitions of Standards Australia [1]:

Knowledge: A body of understanding and skills that is constructed by people. Knowledge is increased through interaction with other people and with information.

Knowledge Management: A trans-disciplinary approach to improving organisational outcomes and learning, through maximising the use of knowledge. It involves the design, implementation and review of social and technological activities and processes to improve the creating, sharing, and applying or using of knowledge.

3. Research Approach

This research required a holistic approach at different levels where the units of analysis would vary between individuals, teams, networks, organisations and critical emergency situations. It developed from a technology-centric view, where the emphasis was on high performance devices and networks, to a tool-centred view automating as much as possible to agent-oriented and network-centric considerations.

The following two sections of the paper give selected overviews of relevant technological and knowledge management concepts from the literature. These include mobile intelligent software agents and wireless networks on the technology side, and sense-making at levels of individual, team, organisational (business and government) and society (the general public) on the KM side. This is followed by a section describing the application of these concepts to a secondary case study, in order to advance the understanding of their integration in practice. This case is analysed interpretively.

A case method is deemed applicable to this type of research, which attempts to integrate diverse paradigms as it provides a rich yet pragmatic approach to data collection and analysis. The use of a secondary case is necessary for this topic as it provides a real scenario, which is not possible to access first hand since, by their nature, emergency situations are not planned. It would,

in any case, be unethical to be undertaking data collection during an event when all resources are needed to cope with the problem. Most big events are well researched through exhaustive data collection after the event and most reports are in the public domain as it is a public issue. While it is not suggested that it is possible to generalise the findings of a single case, as each is unique to its own context, there are common threads that enable learning to occur across cases. Walsham [2] contends that interpretive case methods are appropriate when the aim of research is to understand the context and the process of systems, rather than to establish any hypothesis for testing.

4. Mobile Agents, Wireless Technologies

The selection of relevant technologies to this research is strongly influenced by the work of the R&D team from a commercial organisation and details of the technology are commercial in confidence. Therefore only general characteristics are presented here of devices, which can perform in extreme, highly dynamic and unpredictable environments where they have:

- High levels of vibration and shock,
- Wide temperature ranges,
- Varying humidity,
- Electromagnetic interference, voltage/current transients.

The direct end-users of these devices will be the frontline emergency personnel (fire-fighters, police officers paramedics, rangers) who will be continually on the move with changing contexts and hostile environment. They need:

- Reliable services
- Reliable devices
- Timely information
- Location-based information

This leads us to consider mobile agents in wireless networks where from a technical standpoint an agent is a software entity that functions continuously and autonomously in a particular environment, often inhabited by other agents and processes. Russel and Norvig [3, p.32] define an agent as anything that can be viewed as perceiving its environment through the sensors and acting upon that environment through actuators. Their agent could be a human, a robot, a piece of software, or whatever else that could interact with its environment by sensing and acting upon its perception of the environment. They express an agent in its simplest form as a reflex agent who selects actions on the basis of the current view of its environment and condition-action rules.

Such agents exhibit the following attributes:

- **Autonomy:** operate without the direct intervention of humans or others
- **Reactivity:** the ability to selectively sense and act
- **Collaborative behaviour:** work in concert with other agents to achieve a common goal
- **Persistency / Temporal continuity:** persistence of identity and state over long periods of time
- **Adaptively / learning:** ability to learn and improve with experience
- **Pro-Activeness:** Exhibit goal-directed behaviour by taking the initiative
- **Social Ability / Knowledge-level communication ability:** interaction with other agents (and possibly humans) via some kind of agent-communication language and communication protocols.

The concept of a mobile agent is a contentious topic that has attracted some researchers and repels others. White [4] describes a mobile agent as a new way of communication between hosts, in which hosts not only call procedures in one another, but also supply the procedures to be performed there so that the interaction does not require ongoing communication and is a new way of communication between hosts.

While the use of IT networks is commonplace in business, the adoption of wireless networking technologies means that public safety workers can effectively access data resources and communicate more efficiently with their colleagues and the dispatch. According to Wireless Ready Alliance [5], there are many advantages of using new wireless technologies over the traditional two-way communication systems in emergencies: they are more secure, more accurate, provide visual information, support and transfer different formats of information, workers can operate in the extreme environments, their performance is higher in terms of the level of functionality, throughput and coverage. Walker [6] also notes that devices in such ad-hoc networks can be diverse (laptops, PDAs, camcorders, mobile phones, sensors, etc.) and have various characteristics like throughput, transmission power or size. Importantly, the common feature of all ad-hoc network devices is the capability to communicate using one or more wireless technologies (standards and protocols) and limited energy resources. Through ad-hoc networks, coupled with various sensors, information about the network's nodes such as their position, temperature, speed and so on, can be constantly monitored.

The term MANET is used by the R&D team that has inspired our research to stand for an autonomous collection of mobile users that communicate over

relatively bandwidth-constrained wireless links. Its challenges are:

- Since the nodes are mobile, the network topology may change rapidly and unpredictably over time.
- The network is decentralised; all network activities must be executed by the nodes themselves.
- Need efficient distributed algorithms to determine network organisation, link scheduling, and routing.
- Shortest path is not the best path.
- The network should be able to adaptively alter the routing paths to alleviate any of these effects.
- In many environments, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns.

Topology	Reliability	Adaptability	Scalability
Point to Point	High	Low	None (two end points)
Point-to-Multipoint	Low	Low	Moderate (7-30 endpoints)
Mesh Networks	High	High	Yes (thousands of endpoints)

As indicated in Table 1, in the preferred mesh topology a node can send and receive messages and can function as a router and can relay messages for its neighbours with:

- Self-Configuring and Self-Healing
- Redundancy and Scalability
- Easy installation in short period of time
- No requirement for sophisticated planning and site mapping to achieve reliability

If environmental conditions result in poor reliability, it is difficult or impossible to adapt a point-to-multipoint network to increase reliability. By contrast, mesh networks are inherently reliable, adapt easily to environmental or architectural constraints, and can scale to handle thousands of end points.

Among possible wireless radio technologies the preference is for Ultra Wide Band (UWB) which:

- Operates across a wide range of frequency spectrums by transmitting a series of very narrow and low power pulses.
- Immunes the multipath cancellation effects as observed in mobile and in-building environments.
- Has a quite low energy density which translates into a low probability of detection
- combines well with the mesh network topology

Mobile agents have the following advantages on a wireless network as they:

- reduce the network load
- overcome network latency

- encapsulate protocols
- execute asynchronously and autonomously
- adapt dynamically
- are naturally heterogeneous
- are robust and fault-tolerant

5. The Knowledge Management Issues

KM concerns getting the right information and knowledge to the right people at the right time in the right form. In emergency situations is a need for rapid decision making under pressured dynamic conditions where information is partial, conflicting and often overloaded. Effective choice from a range of actions must be enabled by making appropriate knowledge available to many players. In addition to the on-site emergency personnel there are off-site commanders, representatives from governments and other agencies as well as the public media and those members of the public inadvertently caught up in the situation.

Public safety service providers typically have bureaucratic structures. Members are trained to follow a rigid tree-like communication hierarchy in every crisis. These have advantages in pre-technology eras but are not suited to a mesh network environment.

There is currently considerable interest among military organisations in network-centric configurations. The concept of “network-centric” has been defined by Standards Australia in their recently released vocabulary [1] as “Reaping the potential benefits of linking together, or networking, organisational entities to achieve synergistic effects. Networking-centrism has two related and mutually reinforcing dimensions:

- the human dimension: the way people collaborate to share their awareness, knowledge and expertise so that they can operate more effectively as a whole;
- the network dimension: the connection of information, applications and infrastructures to permit rapid dissemination of knowledge.

Network-centrism is about how social and technical capital can enable the flexible and synergistic linking of the capabilities of people and technologies in networks of self-adapting teams that fulfil the broader purpose or goals of an organisation. It is particularly relevant to operations of interest to our research where there are critical issues of human-computer interaction involving socio-technical systems. Research into the use of technology such as networks of mobile devices to sense and communicate a variety of relevant data involves multiple interacting agents, both technical and human.

This research deals with knowledge enabling action within a broad context of sense-making in organisations

as understood by Weick [7]. According to Cecez-Kecmanovic et al [8] knowledge can be considered as both a subject where what we know enables us to act, and as a product of sense-making by individuals, groups and organisations leading to learning from those acts. A sense-making approach to knowledge in situations demonstrates how it can be applied to gain deep insights into complex knowledge management phenomena in real life situations. Weick and Cecez-Kecmanovic regard sense-making as occurring at four different levels:

- Individuals –professional actions, decision-making, tacit knowledge/experience
- Groups/teams – activities, trust, combinations of knowledge and skills, informal/agile networks
- Organisations – allocation of resources, funding, lessons-learnt, discipline, co-ordinating, authority,
- Society/community – amateurs, focus of danger, culture, motivation, panic

Nosek [9] echoes the idea that sense-making leading to action occurs at different levels which interact in complex ways as depicted in Figure 1. He describes sense-making as incomplete discovery, inaccurate interpretation and imperfect action demanding deep collaboration between participating agents. He applies this to organisations in general, but it is particularly relevant to those involved in emergency situations.

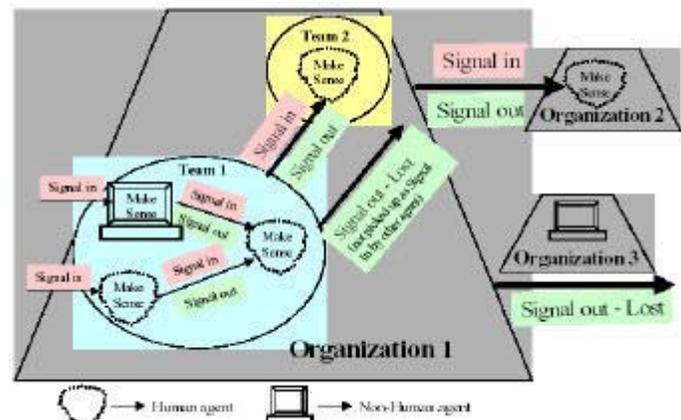


Figure 1 Sensemaking Cycles and Linkages within and between organisations [9]

6. The Secondary Case Description

The secondary case chosen for the study was the attack on the World Trade Centre on September 11, 2001. This case is suitable for two reasons:

1. It was an unexpected catastrophic event that typified the conditions where advanced technology together with multiple teams of people from different

organisations had to rapidly coordinate activities under extreme pressure, and

2. There are extensive reviews and reports of this event in the public domain which can be used as sources for the study [10.11].

At 8.46am on September 11, 2001 the first plane hit the North Tower. An American Airline Boeing 767, having been deliberately flown into the North Tower, striking it across floors 93 to 98. The aircraft was swallowed up as it hit the building, and had a massive impact on the North Tower. Jet fuel spread a huge fire across all six floors where the plane had hit. For the 6000 people below where the plane had hit, the staircases still offered the means of escape, but for the 950 people caught above the point of impact, there was no way out.

After the first tower was hit, many firefighters, police officers and other rescue units got to the scene as soon as they could. But unpredictable problems arose making it extremely difficult for them to cope with the huge magnitude of the disaster. Any attempt to establish a unified command was further frustrated by the lack of communication and coordination among responding agencies, including the Fire Department (FDNY), city police (NYPD) and Port Authority Police Department (PAPD). Information critical to informed decision-making was not shared among these agencies. For example FDNY chiefs later stated that their decision-making capability on that morning was hampered by lack of information from the NYPD helicopter. The FDNY chiefs, facing the crowd in the North Tower lobby, confronted critical choices with little to no information.

At 9.02am the second airplane hit the South Tower, impacting between floors 78 to 84. The plane sliced into the South Tower. About 2000 people were left alive in the South Tower, some 1500 below where the plane had crashed. Just as in the North Tower, these 1500 people still could make their way down. The 500 left above the impact line had no way to get out.

At that time, of particular concern to the FDNY chiefs was communications capability. Earlier, one button on the communication repeater system activation console in the North Tower was pressed at 8:54 a.m. As a result, communication became possible between FDNY portable radios on the repeater channel. There was a second button that needed to be pressed for the activation of transmission on the master handset. That second button was never activated that morning.

At 9:51 a.m., a helicopter pilot cautioned that "large pieces" of the South Tower appeared to be about to fall, and posed a danger to those below. Immediately after the collapse, another helicopter pilot radioed the news. The FDNY chiefs would have benefited greatly if they had been able to communicate with the helicopter pilot. 57

minutes after the second attack, at 9.59 a.m. the South Tower collapsed. It took only 30 seconds for the tower to collapse entirely. 600 people died in this tower, 500 of them were those trapped above the point of impact.

At 10.03 a.m., four minutes after the first tower collapse, there was a terrible realisation that if the South Tower had fallen, the other one was likely to follow. An urgent message was radioed to all firefighters and policemen in the North Tower. The South Tower's total collapse was immediately communicated on the dispatch channel by an FDNY boat on the Hudson River; but no one at the site received this information. Despite his lack of knowledge of what had happened to the South Tower, a chief in the process of evacuating the North Tower lobby sent out an order within a minute of the collapse.

Many FDNY personnel in the North Tower who received the evacuation orders did not respond uniformly for several reasons. According to Bock [12], many of the firefighters got the message before it started to collapse and didn't pay any attention because it didn't come from a source they trusted, their own commander, but rather from the police. Many of these firefighters didn't leave.

25 minutes later at 10.28 a.m. nearly 1000 people were still trapped in the upper 20 floors of the North Tower, together with many firemen unaware of the evacuation order and still inside the tower trying to save people. At this moment the North Tower came down. The theory for the collapse is that the tense fire had weakened the bare steel of the core columns and this had caused the building to start pancaking down similar to a situation in controlled structure demolishing. In total 2800 people died in the attack, 479 of them were from the emergency services including 343 firefighters.

7. The Secondary Case Review

There was considerable impact on the firefighters' lives on September 11 due to the inconsistency of vital information among different groups. The primary reason of this inconsistency goes back to the lack of interoperability among the different agencies and its consequences on the senior commanders' decisions. The US 9/11 Commission Report (2002) made a point of the discrepancy between the number of NYPD and FDNY casualties and deaths. The report clearly states that the success of NYPD instruction is credited to:

- The strength of the radios they were using
- The relatively small numbers of individuals involved
- Use of the correct communication channel by all

The report says that the same three factors worked against communication among FDNY personnel.

- First, the radios' effectiveness was drastically reduced in the high-rise environment.
- Second, initially, all the FDNY units were using the tactical channel 1 for the communications purposes, so this channel was simply overwhelmed by the number of units attempting to communicate
- Third, some firefighters were on the wrong channel or they simply lacked radios.

There was a significant impact on the firefighters' communications when those in the North Tower were redirected to the repeater channel after 10:00 to resolve the congestion problem. This repeater was considered as the focal system, which would handle all the communications throughout the North Tower. For others the type of wireless equipment in use did not provide reliable communication because many public safety personnel regularly use cellular phones, personal digital assistants, and other commercial wireless devices.

From an organizational perspective there was no adequate and reliable interoperability among the different groups involved in the rescue operation and civilian evacuation. As a result, information sharing was extremely limited, so there was much redundancy and conflict in the tasks undertaken by different parties. These parties suffered from the disparity and inconsistency of the critical information. These problems seriously impacted the overall performance of the rescue operations since commanders couldn't make united decisions and coordinated actions.

Furthermore, in this case, the technical issues linked to the communication network remarkably affected the reliability of the network that was responsible for disseminating the critical information. It seems that communications networks were unable to operate in the high pressure environment. For example, US 9/11 Commission [11] reveals that firefighters did not receive the evacuation transmissions, for one of four reasons:

- First, some FDNY radios did not pick up the transmission because of the difficulties of radio communications in high-rises.
- Second, the numbers trying to use the one channel may have drowned out some evacuation instructions. According to one FDNY lieutenant who was on the 31st floor of the North Tower at the time, "[Tactical] channel 1 was so bogged down that it may have been impossible to get that order through."
- Third, some firefighters in the North Tower were off-duty and did not have radios.
- Fourth, some firefighters in the North Tower had been dispatched to the South Tower and most likely were on a different tactical channel.

8. Case Discussion

In this case, and probably many others, the communications systems' ability to facilitate the process of transferring data is critical to enabling local decisions to be made based upon the local data travelling throughout the system. This facilitates human decisions making in a more reliable and timely fashion particularly in the highly dynamic environment. The human process should be enhanced if there is a degree of intelligence and autonomy embedded into the systems by the mobile agents and the wireless networks, which support them.

Optimal public safety radio communication systems require satisfying five primary criteria [13]:

- 1- Dedicated channels and priority access that is available at all times
- 2- Reliable one-to-many broadcast capability
- 3- Highly reliable and redundant networks that are engineered and maintained to withstand natural disasters and other emergencies.
- 4- The best possible coverage within a given geographic area, with a minimum of dead zones.
- 5- Unique equipment designed for quick response in emergency situations since in critical events seconds can mean the difference between life and death.

One promising solution to this issue is mesh networking technology. Initially designed and exploited for military purposes it has shown significant advantages over many other networking topologies for the on field communications[14]. These advantages include the capacity and the number of users who can communicate with each other at the same time. Broersma [15] explains that each device on a mesh network receives and transmits its own traffic, while acting as a router for other devices; intelligence in each device allows it to automatically configure an efficient network, and to adjust if, for example, a node becomes overloaded or unavailable. According to Broersma, the advantages include ease of setup, the ability to spread wireless access over a wide area from a single central wired connection, and the inherent toughness of such networks, since they are self-healing and self-configuring. In many public safety rescue tasks, especially in a specific geographical area where a large number of crew are involved in rescue operations, high bandwidth, ad hoc mesh networking is promising because it can handle the one-to-many and many-to-many communications by reliable and flexible means. Mesh technology gives networks the ability to adapt with dynamic environment changes such as the number of the mobile users and coverage area. This can help public safety communications to avoid the tradeoffs

between the number of mobile users and the network capacity.

Mobile agents can add new values and considerable competencies to the wireless networks i.e. the ability of networks to deliver data to the appropriate place and to deal with the interoperability issues. The term interoperability to address the ability of networks to transmit all types of communications electronically, including voice, data, and images [16]. However, today the diversity and incompatibility of the contemporary network devices used has considerable impacts on public safety interoperability. This means that different hardware or software platforms used in public safety are the main reasons that devices cannot talk to each other. Mobile agents are generally independent of any computer platform and network transport layer, and their performance only depends on their execution environment [17]. This means that they can provide optimal condition for seamless system integration, which could significantly help to make reliable inter-links between the different communications systems used. Pham and Karmouch [18] report that the mobile agent paradigm has two general goals: reduction of the network traffic and asynchronous interaction. Mobile agents can sense the users' environment through the sensors interface between agents and environment. In fact, a sensor network could sense some critical elements of the physical environment [19] such as body temperature, blood pressure, or speed and direction of the wind, and pass this data to waiting agents. Sensor networks could be setup as mesh configuration and cover a broad geographical environment, resulting in improved 'situation awareness' [20].

This range of sophisticated and high performance technologies is being developed through a growing awareness of the needs of catastrophic emergency situations. However, it must support the sense-making of the complex human social systems involved in these situations, leading to an ability to act at various levels from individual through coherent teams in rigid hierarchical organisations.

In the highly pressured environment of emergency operations, changes happen fast. Having a communication network that could handle crucial information with less possibility of a congestion problem is vital. Mobile agents and new wireless technologies show encouraging capacity to handle in emergency situations. Access to both primary information of the current status and complementary information, building plans for example, in a comprehensible form is critical to the success of a rescue operation and to the lives of the crews involved. This involves not only technological specifications but an understanding of the human

usability issues and the broad view of the interoperability within the whole socio-technical system.

Research in this area must be multidisciplinary, as no one discipline has the breadth of understanding of all facets of the problem let alone how they interact and integrate. Many of the requirements for the complete system are contradictory and knowledge in each domain is incomplete. The work of Nosek [9] depicted in Figure 1 gives a broad perspective and yet this work only deals with organisations under normal conditions. The interoperability of the problem is magnified many times in an emergency situation. The following are some specific examples of the interaction between the technology and the human elements of the system.

The individuals that are relied on in military or civilian emergency situations must have completely unhindered mobility [21]. On the other hand, they should be armed with as much information and data as they can effectively utilise. A combination of mobile agents and new wireless technologies with networked wearable computing devices could offer a good solution in order to help crews have access to more valuable information about their environment and then make local decisions or relay that information in a reliable way to other places in the network where they are needed. Mobile agents can handle network disconnections by storing their state and data delivering these to a destination after the connection is established again [22], making communications robust against network breakages

Intelligent communication systems have the autonomy not only to assist local situation awareness, but also to help decision makers have broader sense of the overall picture of the operations on the field. Essential for these systems is the ability to perform local processing and making decisions where individuals and teams are authorised to act autonomously. This system could have a degree of intelligence in order to integrate and transfer some of the human tasks to the systems. In such a system, many decisions would be made locally where the data are generated. As Lang and Oshima [17] spell out, in many situations it is more efficient to move the small computation and required processing to the place of the large volume of the data rather than the data to the computation. This then supports the ideal of a network-centric configuration as described earlier.

9. Conclusion

In complex situations, such as emergencies, the sense-making of individuals and various groups of people is inevitably incomplete which leads to imperfect action. For the successful resolution of such a situation as well as the saving of lives and property it is imperative that

decisions made are the best possible in the circumstance with the resources and information available. This study suggests that as much as possible should be learnt from each occurrence of such events so that this knowledge be shared with those investigating human behaviour in such conditions at all levels as well as whose develop technologies that can be used to both support and relieve some of the human activity.

The authors of this paper have determined that mobile agents with wireless mesh networking provide technology that could bring a degree of intelligence to the communication systems in the work of public safety organisations. This is highly flexible technology which can adapt to changing network environments, making communication systems more adoptive and intelligently responsive to the needs of those with decision-making responsibilities in the situation.

Classes of problems that emerge from this study involving technical and human issues are.

1. Numbers and heterogeneity – individuals/teams from various emergency service organisations
2. Interoperability between services, communications issues and problems under stress
3. Network congestion, information overload
4. Lack of Meta Data – support for intelligent and dynamic sense-making for decision makers
5. Network volatility – communications breakdown, incomplete access to resources
6. Right equipment, skills, training, capability available as needed

Applications of mobile agents and new wireless technologies can help to overcome or alleviate the discussed problems, and give a degree of intelligence to the communication systems enabling them to interact with their environment to gain the best performance in the timely and reliable fashion. They must however be developed in conjunction with improved understanding of the way people, teams, organisation and the public need to act in uncertain and threatening environments.

Although attention during an emergency is on the task at hand, there is also awareness that, after the event, there will be detailed scrutiny of decision-making and performance by both the media and those in authority. Lessons are being learnt and thereby technology and human systems be developed to meet the challenges presented in various types of emergency situations.

10. References

[1] AS5037 2005 *Knowledge management – a guide*, A Business Standard from Standards Australia.
 [2] Walsham, G. 1995 Interpretive case studies in IS Research:nature and method. *Eur. J. Inf Systems* 4: 74-81.

[3] Russell, S. and Norvig, P. 2003, *Artificial intelligence: a modern approach* Prentice Hall, New Jersey.
 [4] White, J. 1996 *Mobile Agents White Paper*, General Magic.
 [5] Why Wireless for Public Safety? Wireless Ready Alliance, URL<<http://www.wirelessready.org/safety.asp>>
 [6] Walker, J. 2004, *Mesh Networks References*, Technical paper, Applied Wireless Local Area Network Inc., Viewed 23 December 2004, <http://www.wi-fitechnology.com/Wi-Fi_Reports_and_Papers/Mesh_Networks_References.html>
 [7] Weick, K.E. (1995). *Sensemaking in Organisations*. Sage.
 [8] Cecez-Kecmanovic, D. Jerram C. & Treleaven L (2003) A Sense-Making View of Knowledge in Organisations: The Insiders' Tale in H. Hasan & M. Handzic eds *Australian Studies in Knowledge Management*, UoW Press 92-135
 [9] Nosck J. (2005) Collaborative Sensemaking Support:Progressing from Portals and Tools to Collaboration Envelopes, *Int Journal of e-Collaboration*, 1/2 26-39.
 [10] The fall of the World Trade Center 2002 video recording, BBC, UK.
 [11] US National Commission on the Terrorists Attack Upon the United States 2004, *The 9/11 Commission Report*, Special Report, Washington, USA.
 [12] Bock, W (2003), *Lessons from September 11*, media release, The digital age storyteller, USA, viewed 3 January 2005, URL<http://www.mondaymemo.net/020909feature.htm>
 [13] Commtech 2003, *Can't We Talk? Interoperability, Working Together To Bridge the Communications Gap To Save Lives A Guide for Public Officials*, National Task Force Publication under the Agile Project Programme, USA.
 [14] Schoen, R. 2002, *Interoperable Communications: Is Mesh Technology the Answer?*, Technical Paper, Police Futurists International , Oregon, Viewed 1 February 2005, <http://www.policefuturists.org/newsletter/webarticles/interoperable.htm>
 [15] Broersma, M. 2004, *Mesh: The next step for wireless, technical report*, ZDNet UK, viewed 10 January 2005, <<http://insight.zdnet.co.uk/communications/wireless/0,39020430,39149930,00.htm>>
 [16] Smith, B. and Tolman, T. 2000, 'Can We Talk? Public Safety and the Interoperability', *National Institute of Justice Journal*, April, pp.17-21, USA.
 [17] Lange, D. and Oshima, M. 1999, Seven Good Reasons for Mobile Agents', *Communications of the ACM*, 42/ 3, pp 87-89.
 [18] Pham, V. A. and Karmouch, A. 1998, Mobile Software Agents: An Overview, *IEEE Communications Mag*, 26-36.
 [19] Boukerche, A. Nelem, P. R. W. and Araujo, R. B. 2004, A Fast and Reliable Protocol for Wireless Sensor Networks in Critical Conditions Monitoring Applications, *ACM* 157-164.
 [20] Huhns, M. N. and Seshadri, S. 2000, Sensors+Agent +Network=Aware Agen', *IEEE Internet Comp* May, 84-86.
 [21] Evan, N. M. R., Chandler, M., Nobel, K. R. 2002, Threat Response: a Compelling Application for Wearable Computing', *Proceedings of the 6th International Symposium on Wearable Computers*, IEEE Computer Society, Seattle, Washington.
 [22] Kotz, D. and Gray, R. 1999, Mobile Agents and the Future of the Internet, *ACM Operating Systems Review*, 33(3), August, pp. 7-13. A