Emergency Communication Challenges and Privacy

R. B. Dilmaghani, B. S. Manoj, and R. R. Rao
Department of Electrical and Computer Engineering
University of California, San Diego
La Jolla, CA 92093-0436
{rdilmagh, bsmanoj, and rrao}@ucsd.edu

ABSTRACT

Communication and interoperability between different organizations of first responders has been a problem for a long time. There have been examples of failure in communication between different organizations at World Trade Center on 9/11, for example some of the police warnings were not heard by fire fighters that resulted in several lives lost. In most cases, network unavailability or incapability of coordination among networks causes much damage. Therefore, we present a highly reliable communication infrastructure that is suitable at ground zero where the existing communication network is damaged or unavailable. We used Hybrid Wireless Mesh Network (HWMN) as a candidate for communication infrastructure with the capability of working in a heterogeneous environment with different available backhaul technologies. In addition to the use of WMNs, we also present some special requirements for a cellular networks generated by simulation models investigating different scenarios that occur at ground zero. For example, when hurricane Katrina hit New Orleans, people outside the ground zero area could place a call, but were not able to receive phone calls. This happened because the cellular network elsewhere was not able to contact the Home Location Register (HLR), located at New Orleans. We, in this paper, propose a solution in which the important user or network information databases such as HLR and VLR (Visitor Location Register) are replicated to provide a sufficient amount of fault tolerance.

Keywords

Disaster categories, Katrina, World Trade Center, wireless mesh network, cellular infrastructure, and privacy.

INTRODUCTION

This work studies and identifies the category and nature of disasters that need to be considered to design a reliable communication infrastructure. These are very important factors which differ from one another in different scenarios depending on the nature of disaster and play crucial role in designing warning systems. Examples of such factors include degrees of urbanization, scale of disaster, spatial breadth, time length, and the successful predictability of the disaster. It is quite clear that for sudden natural or man-made disasters there is very limited actions can be taken to warn people. Some disasters like hurricane by nature may give a very short time to warn people and disseminate data. Others might give a longer time window to warn people. Another important factor in warning people in sociology is the age and the ability of people who are addressed and their preference on how to be warned which may vary depending on the time of day. Another issue that we would like to address here is the special requirements of communication infrastructure for emergency response and future communication infrastructure. We propose a hybrid wireless mesh network (Dhilmaghani et. al., 2005) as communication infrastructure at ground zero, for a natural or man-made disaster where the existing network is fully/partially unavailable. This work additionally addresses some special requirements of cellular networks and suggests a few improvements that can be applied to the existing systems in order to provide a better and more reliable service.

For a long time, communication at system level between different organizations of first responders has been a problem. The issue, most of the times, is that they cannot really talk to each other, i.e. there is no effective communication (Morentz, 2000). This might be either due to unavailability of network or incapability of coordination or interoperation. After World Trade center, and hurricane Katrina, there has been more attention on continuous availability of a landline communication infrastructure and cellular networks. When a disaster like Katrina happens, people who own a cell phone lose access and are not able to call their family and friends.

In today's communication enabled society, many people communicate with each other using our cell phones from anywhere. Citizens have become a lot more dependent on a reliable communication infrastructure. Although they may not use the service at all time but when a disaster happens, it is very comforting for one to call friends and family to let them know that he/she is safe. Unavailability of cellular systems not only impacts the people who own cellular phones, but also first responders who are working on affected areas and they loose contact with other members of rescue team and the command and control center. Though most responders have their own communication systems, they use civilian communication networks such as cellular phones. People in need for help have been unable to use their cell phones due to unavailability of communication infrastructure which might have occurred because of physical damage, power failure, or both. In a disaster event, communication towers that transmit and receive wireless signals are prone to damage. Additionally, power may go down, and media communication becomes unavailable. Also an important part of the communication infrastructure, cellular phones fail to work when they get wet. The weak point of a communication system is determined by the most vulnerable part of it. However, the scale of the problem matters, for example, cell phones are not water proof but this affects one or a few individuals while a communication tower affects hundreds of people.

Each one of these large scale disasters affect the nation in many ways and will probably take years to rebuild and recover from. Typically, after each disaster, there are serious side effects such as death, health, refugees, social effects such as looting, or price gouging after Hurricane Katrina. Economy effects are another drawback which in particular has led to increase in gas price, and decrease in revenue generated by the industries such as tourism.

For the 9/11 case, based on an article in New York Times, when Police helicopters hovered near the remaining first tower minutes before it collapsed and there have been reports of pilots asking for evacuation of all people in the area of the second building. However, those warnings were not heard by fire departments (see reference [3]). The radio broadcast system failed many times during the 9/11 response, even, if it was working, it was not linked to the Police radio so that they can hear them. This has been an issue for a long time, and many references and articles exist on interoperability and coordination between different first responder organizations (Morentz, 2000). Considering the heterogeneity of devices in today's world, a flexible communication system should be able to send and receive messages over different networks. Also such systems should provide interface to other first responders' systems.

CHALLENGES IN EMERGENCY COMMUNICATION

To design a flexible communication infrastructure, there are a large number of factors to consider. Below we summarize some of these important factors:

SCALE OF DISASTER: Disasters can be categorized based on the following features: degree of urbanization/scale which is determined by the number of people in the area who are affected when a disaster occurs. On the other hand, spatial breadth is a factor that impacts the way to respond and recover from disasters as there might be fewer people involved, however, it is happening in a very wide area such as wild fires. These vast area disasters should be under control soon as possible because further spreading of such disasters may not only impact more people, but also leave a long lasting negative impact on the environment. One important goal of disaster response is to shorten the length of disaster as if not, it may turn to another disaster and therefore, may become less manageable. In all different kinds of natural or man-made disasters, we need to take into account the degree of early warning, whether it has been anticipated like hurricane or unexpected like wild fires. The effectiveness of early warning, however, may vary depending on the time they give to take preparatory measures and evacuate people from the area.

SPECIAL COMMUNICATION REQUIREMENTS: As another specific application for special communication requirements at ground zero, we can point at telemedicine communication which may include interactive real-time communication. To share information between the physicians and patients, there are many issues such as receive/deliver care protocols, bill, and liability issues. Transferring data, audio, and video require special bandwidth at low cost. In this paper, we address some other special requirements of communication systems for emergency response such as reliability and continuous availability of service, interoperability between different first responder organizations, and ability to work with heterogeneous devices and different technologies available. We communicate in a heterogeneous environment, which means different devices such as laptop, palmtop, cell phones, and different network technologies such as WLAN, WiMax, WWAN, Satellite, or wired networks.

WIRELESS INFORMATION TECHNOLOGY: The role of wireless information technology in disaster response/recovery, and homeland security, especially in rural areas is very critical. Given the growing importance and challenges of inter-agency collaboration, we will highlight some of the problems and propose a solution which is capable of working in heterogeneous environment with different technologies to facilitate communications

interoperability. We need to have gateways which are able to communicate with each other while they use different technologies. Future communication infrastructure is expected to have the ability to operate in a highly distributed and infrastructure-less manner, quickly deployable and reconfigurable, and use available resources efficiently.

RESISTANCE TO ADOPT NEW TECHNOLOGY: It is helpful to notice that very little improvement has really been done for aging networks concerning Public safety vulnerability. Public safety agencies should be encouraged to replace their existing networks to select systems that support emergency response activities in addition to their operational requirements. It is also desired to support the existing systems with as much redundancy as possible such as back-up facilities, dispatch centers, infrastructure, and power. However, disasters such as Katrina may help speed up adopting new technologies that help managing disaster recovery. The significant enhancement in communication technology has raised the ability of first responders to communicate, exchange information, and make timely decisions (Tierney and Sutton, 2000). However, adoption and implementation of such new technologies is affected by social factors such as cost and culture (Tierney and Sutton, 2000). In the broad area of cost associated with deploying new technology, one can refer to staff training, compatibility with existing technology, complexity of new technology, and maintenance are some major factors. Furthermore, there is a difference between private and public companies on justifying technology infusion. Private companies typically justify adoption for competition and profit while public companies especially for large cities make the excuse for the sake of size and scale in addition to compatibility with legacy applications, technology lifecycle, reliability, flexibility, and facilitating cross-agency collaboration. On the other hand, the cultural side of the story includes the traditional standards and codes of conduct. It is imperative that the new technology should be simple, intuitive, reliable, secure, and interoperable with legacy applications. In addition, there is a strong requirement to improve interactive communications, coordination, and collective action among community organizations in the shared task of managing incidents in which populations are at risk. This task gets more challenging in large cities as the existing systems which already exist might not be able to communicate with each other.

INFORMATION PRIVACY: However, information sharing and privacy issues matter with technology infusion as we need to release information to the specific first responder organization in charge of that incident. Data manageability and collection, adaptability with different technologies, Internet repositories, bandwidth aggregation for network services, handoff protocols at service level are some other challenges in future communication systems.

WIRELESS MESH NETWORK INFRASTRUCTURE

Recently Wireless Mesh Networks (WMNs) have become very popular research area for the use of unlicensed spectrum and low cost of IEEE 802.11b/a/g-based devices. In the near future, wireless Internet provisioning will see the convergence of the Wireless Wide Area Networks (WWANs) and WMNs. This convergence between WWANs and WMNs demands new architectures and experiments on real network testbeds. We designed a novel Hybrid Wireless Network (HWN) architecture (Dhilmaghani, 2005) that integrates WMNs and WWANs which is primarily designed to provide an easily reconfigurable alternative for first responders handling emergency response. This architecture uses point-to-point and point-to-multipoint long haul wireless links in order to provide gateway functionality for multi-hop wireless networks. As part of this work, we present our hybrid wireless mesh network architecture which provides a quickly deployable and highly reliable WMN infrastructure that uses WWANs as backhaul links with no wired backhauls. The initial objective of this architecture is to aid first responders in emergency situations at ground zero where the main requirements are: a quick deployment with minimal configuration, simplicity of reconfiguration of network topology; fault tolerance in the case of failure of certain nodes and/or a part of network, quick rerouting in the case of failure of long haul uplinks, and above all a fully distributed architecture. The network should have resilience to failure of nodes, and links. There might be some important nodes which should be treated in a differentiated way compared to the regular nodes. In this network infrastructure, only gateways are connected through wireless long haul links. In this architecture, the nodes can transfer packets in a multi-hop fashion through each other to reach other users in the network or to the Internet. It also enables use of different wireless user devices, and does not require any expensive network infrastructure for a broadband peer-to-peer network service. The HWMN utilizes a higher tier network that forms a long haul wireless backhaul link to reach a wired network. The presence of the long haul wireless link brings faster and more cost-effective service, while providing faster data dissemination and higher reliability. The special requirements of an emergency communication infrastructure make the HWMN suitable for emergency response activities.

In our Rescue project (see website [5]), we use WiFi access points (see website [6], http://calmesh.calit2.net) to provide broadband systems to access Internet. These wireless access points operate on the same unlicensed spectrum that cordless phones and microwaves use, and are robust enough to provide broadband service when wired networks

fail. Their wireless antennas all talk to each other, which can allow users to access the service even if the nearest wired network is far away. In addition to this deployment, California Institute of Technology and Information Technology, Calit2 (see website [6]), have developed portable wireless access points in house. We recently deployed a HWMN at a full-scale homeland security drill organized by San Diego County and were able to collect real data from the medical first responders' communication over the network. Below, we present some of these results which help us to derive models for typical network Communication pattern at ground zero. For this particular drill, we have been able to extract the following results: Among 226 Ethernet conversation for this partial set of data, 904 applications was sent over TCP and 234 over UDP. Overall capture duration was about 15550 seconds. Total number of packets transmitted was 210727 with average throughput of 3653 Bytes per second approximately. The percentage of packets transmitted over TCP was 26.52%. Extracting and monitoring the communication pattern can help developing a more efficient communication system for emergency response. Figure 1 shows the communication pattern at a given node where the color represents the quantum of traffic from a particular node. Figure 2 presents the volume of communication at all nodes. From this figure, it is noted that more packets are addressed to a particular address (10.1.1.1) which is the default gateway address. Since the default gateway address, in our network, is assigned to every access point, this traffic is not aggregated at any single node in the network. On the other hand, the second biggest loaded node in the network, 10.1.16.1, is the node to which the central repository for the medical response application was attached. This node points to the fact that it may become a bandwidth bottleneck for the whole network. Therefore, distribution of central repositories instead of using a single centralized architecture is inevitable to improve the scalability of the network.

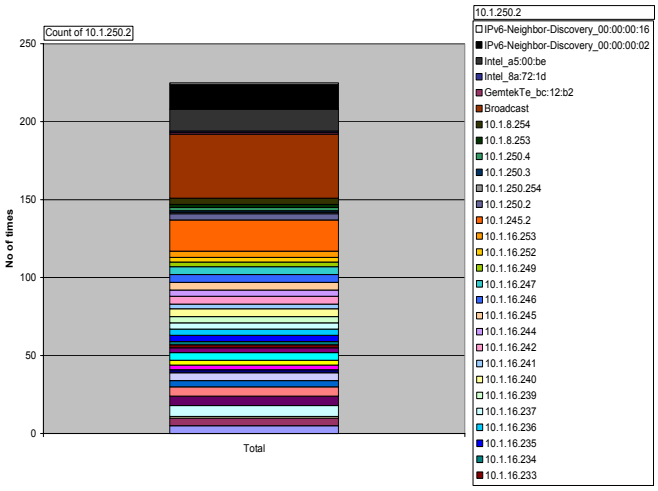

Figure 1. The Communication pattern at a given node

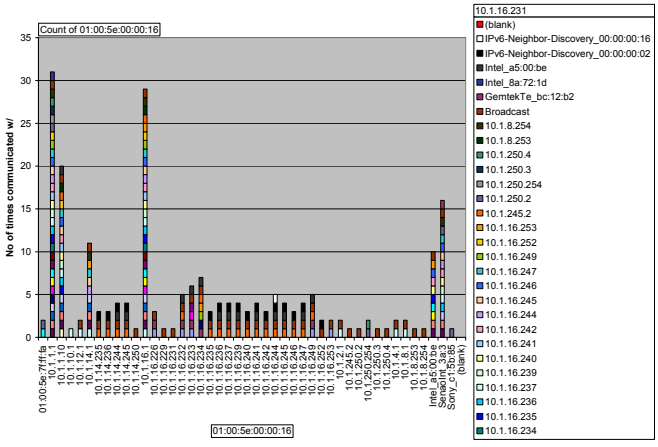

Figure 2. Typical communication pattern across all nodes

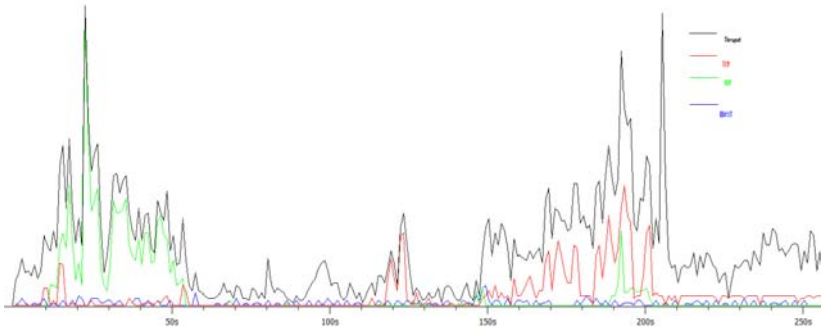

Figure 4. Total Throughput, TCP, UDP, and Broadcast

Figure 4 shows total throughput, the amount of bandwidth used to send UDP, TCP, and broadcast packets for duration of 200 seconds approximately. This figure shows the large deviation in the network traffic.

CELLULAR INFRASTRUCTURE FOR EMERGENCY RESPONSE

When a disaster occurs, cellular phone users might face different scenarios some of which are presented here:

i) The users at Ground Zero are not able to receive a call or make a phone call.

ii) People elsewhere may not be able to make or receive calls from people at Ground Zero.

iii) Users elsewhere may be able to make phone calls, however not able to receive calls though they are not at Ground Zero.

On third scenario, some cell phone users who are out of the area, will be able to make phone calls but not able to receive any calls. This can be justified as cellular providers might have arranged the network elements among themselves so that it can automatically connect any calls dialed from those cell phones on other areas without checking back with Home Location Register (HLR). HLR is a centralized database repository with detail information on each authorized subscriber. However, to receive a call, the wireless network has to check back with a HLR server known as home agent to verify account information and let the service provider know where to route the calls. The ultimate goal is to design and build a cellular infrastructure which survives all natural and man-made disasters. This means it should be able to provide continuous service which can happen by minimizing the number of calls to be dropped or blocked. Deriving traffic pattern and monitoring resource usage helps to minimize network congestion. Below we summarize some of potential reasons that may lead to cellular infrastructure failure:

LOSS OF HLR: In the case of destruction of HLR, for the called cell phones outside the Ground Zero region whose HLRs were located at Ground Zero, the cell phone network may not be able to contact HLR in order to locate the destination user. Therefore, the cell phone network may not be able to locate a large number of users whose HLRs may have been located at Ground Zero. As one solution to this problem we suggest that we make replica copies of information contained in the HLR at different strategically identified locations. This makes the network deployment, operation, and maintenance, more expensive; however, the network reliability requirement is met in case we lose one agent during a disaster. It is very important to notice that there is a tradeoff between reliability and cost. With the decreasing prices for communication equipments, such a provisioning of redundancy on HLRs is essential.

NATURAL DISASTER SUCH AS FLOOD/HURRICANE: In the areas which are prone to floods, the design of the central telephone building is done such that it withstands floods. Therefore in such areas, the central telephone buildings remain operational throughout the hurricane with a good chance, receiving calls and Internet traffic to and from outside the affected area. The physical damage may lead to the base station failure or loss of switching center. Additionally, there may not be sufficient network resources such as lines for most calls and bits

of data to be forwarded to upon arrival as local lines might have got cut off either by flooding. Towers need to be able to continue to work even when their base and core electronics are submerged under water, and also be able to work after being removed from water.

POWER FAILURE: Cellular towers need to have their own automatic power supply that can last for a while, and must be able to route calls without depending on land lines.

NEW STANDARDS AND REGULAR INSPECTION: Nationwide standards need to be developed indicating the conditions that wireless phone towers need to continue to work even when surrounding infrastructure fails. In this regard, the existing towers need to be inspected regularly to see if they can continue to work during disasters. For hurricane Katrina case, some of the server computers which were used to route and connect calls were wiped out by flooding. In other disasters, the phone lines may get cut or damaged by the storm or flood. Both wired and wireless networks are affected when the backup generators running their switching systems stopped working either for want of power or fuel. Above all, at ground zero, even if there is no physical damage, the networks get overloaded due to the sudden surge in call traffic and users may experience a high call blocking rate.

We can categorize the above scenarios based on the affected network layer as the following (Tipper et.al., 2000, Brass and Fuhrmann, 1994):

i) Access-Radio level which includes damage to base station or mobile unit

ii) Access-Link level which includes Base Stations (BS) and BS controllers (BSC)

iii) Transport layer failure including BS, BSC, Mobile Service Switching Center (MSC), and signaling network

iv) Intelligent layer such as MSC, HLR, VLR, Equipment Identity Register (EIR), and signaling network

As an alternative for the cellular network at Ground Zero, we can deploy Voice over IP (VoIP) technique with portable wireless mesh nodes such as that developed by Calit2 (see http://calmesh.calit2.net). For such a VoIP system, users elsewhere simply need to access a broadband network in order to make and receive calls even if they are away and no longer at their home area. In this scenario, an IP address, possibly supported by MobileIP, is assigned to each user independent of their location. It is quite simple to redirect traffic over switches remotely to send traffic onto working networks overriding the damaged lines. When a couple of towers fail, switching to a lower bit encoding in cellular networks, may provide a minimum service at the cost of degrade quality of voice.

On simulation side of this project [9], we plan to integrate our network simulator with an earthquake simulator with complete information of the location of towers and bridges. When an earthquake is simulated, users' mobility pattern changes as some bridges and paths might not be available. The goal is to provide a continuous reliable service in emergency situations. We are trying to extract some traffic patterns based on this data to be able to manage cellular networks after a disaster. Here we present some simulation results for a network and we will extend our work for further studies.

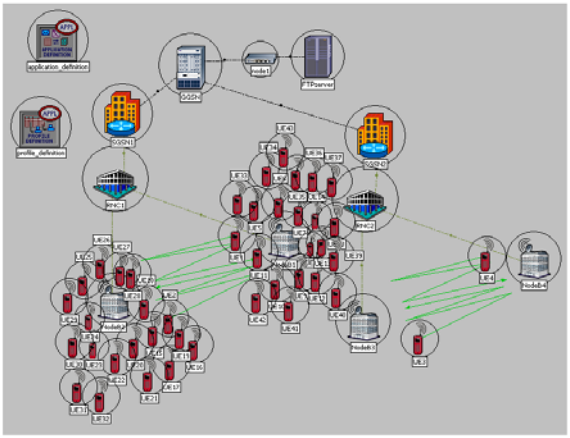

Figure 5. Cellular Network Topology

In this scenario (depicted in Figure 5), 23 User Ends (UEs) upload large FTP files to the server with Poisson arrival

time distribution with mean 120 seconds throughout the simulation. Handover is defined for user number 1 through 4 between corresponding BSs. QoS traffic is considered of priority level 3 for interactive traffic. Figures 6, 7, and 8 show the important parameters, for a given node (say node 14), such as traffic sent and received, total transmission load and throughput achieved, and the end-to-end delay, respectively.

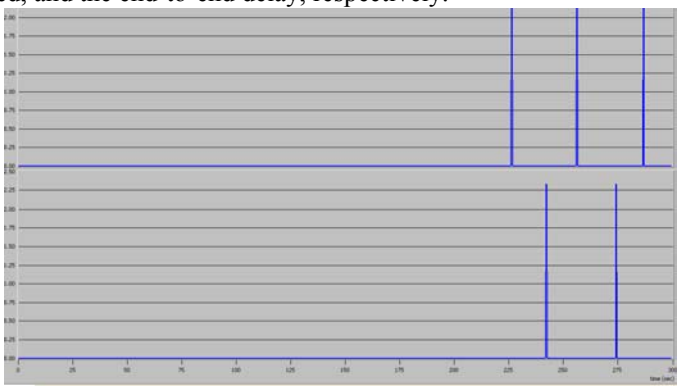

Figure 6. Traffic sent and received by node number 14 (packets/sec)

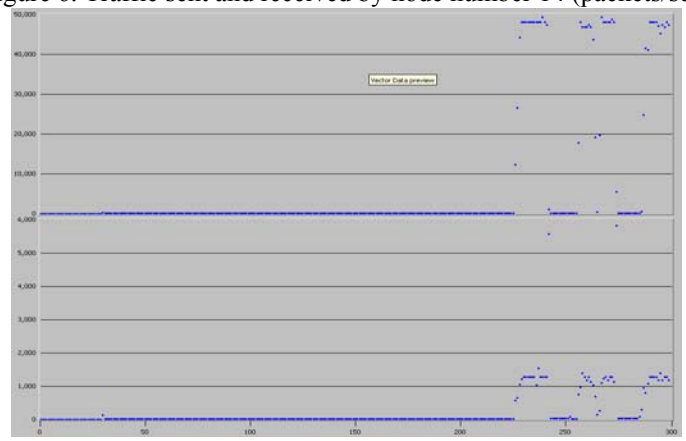

Figure 7. Total transmit load and total received throughput for node 14 (bits/sec)

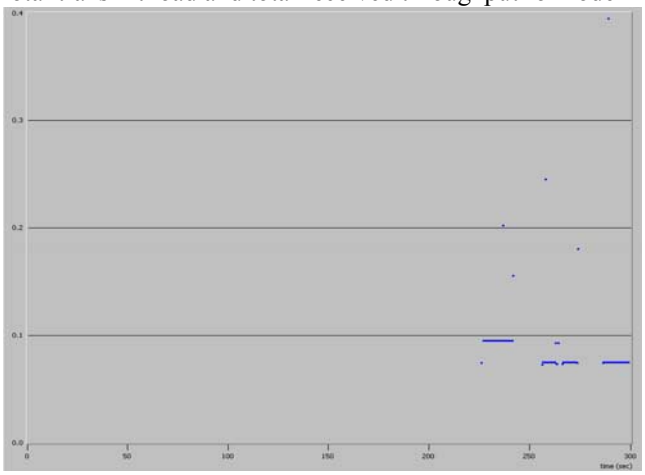

Figure 8. End-to-end delay for node 14 (sec)

PRIVACY ISSUES

The ultimate goal in a network designed for emergency response is that all different organizations should be able to use the same network. However, it is very important that each individual organization receives its own data only and

others should not be able to access the data which is not originally designated to reach them. As one particular application consider the following scenario: in an emergency situation it is very typical to have people from Red Cross, Fire department, Police, and Media. As far as security concerns, police might access the data that is not allowed for any other organization. One's medical file should be visible to medical team only as it concerns one's privacy. Media eventually gets the information however, what they should be told might be different from what they may get from the network. The last case shows the importance of voice being encrypted. In emergency scenarios, violation of one's privacy is almost inevitable. However it can be limited to certain subset of the authorized people. As one solution to this problem, we can design an encryption system such that each type of data is encrypted using the public key of recipients. Therefore they would be the only people who can decrypt the message and access data. Traditional security systems are able to provide this privacy in many different ways. In order to have a secure communication between different organizations, we need to choose the most appropriate group communication protocol based on special needs of emergency communication. We briefly discuss a few existing algorithms in this paper and extend our work in future. One of the earlier works in secure broadcasting is due to Gopal and Jaffe where they proposed a point-to-point approach to broadcasting (Dilmaghani, 2003). For each customer, the server encrypts the data object and broadcasts it. Suppose there are N consumers C1, C2, .,CN. Having public keys P1, P2,., PN respectively. These N consumers subscribe to the data item Di. Then the broadcast message will consist of the concatenation of [Di, P1], [Di, P2], [Di, P3],., [Di, PN] where [Di, Pj] refers to encryption of Di with the public key Pj. Thus, the same message is inefficiently encrypted multiple times and broadcasted. Chiou and Chen proposed a session key approach to broadcasting in which each broadcast is considered as a session. There is one session key per session, which will be discarded after the session is over. In this protocol, there is a pair of encryption or decryption per session for each object Di (SessEncKeyi, SessDecKeyi). The server encrypts the data item Di with the SessEncKeyi and broadcasts it. The corresponding subscribers use SessEncKeyi to decrypt the data. For each customer Cj subscribing to the data item Di, the server encrypts SessEncKeyi with the public key of the consumer Pj. The encrypted SessDecKeyi for all the subscribers for Di, are concatenated together with the data item Di and broadcasted. Therefore, for consumers C1, C2, .,CN subscribing to the data item Di, the following message will be broadcasted: concatenation of [Di, SessEncKeyi], [SessDecKeyi, P1], [SessDecKeyi, P2], .,[SessDecKeyi, PN]. Clearly, the length of the message will depend on the number of subscribers for each data item. In this protocol, the customer subscribing to more than one data object will receive multiple decryption keys in order to decrypt the subscribed objects. Therefore, the customer has multiple keys but key management is simplified because each session key is used for one session only and will be discarded when the session is over. However, key distribution remains a major problem because all session keys need to be distributed to all subscribers within a session. Another protocol was proposed by Ingemarsson et al. which utilizes a group key concept. All subscribers of an object share a group key, which stays the same until one customer joins or leaves the group. When a customer leaves the group, a new group key should be generated and distributed to current subscribers. Then the data item will be encrypted by new group key and broadcast. The new group key will be encrypted by customers public key and transported to new members of group. For the case where the consumers C1, C2, .,CN have subscribed to the same data object Di, the following encryptions are concatenated and broadcast:[Di, Gx], [Gx, P1], [Gx, P2],., [Gx, PN] where Gx is the group key. For the case a customer subscribes to multiple data objects, it has to manage multiple group keys and since group keys are used multiple times, managing and storing multiple group keys is not trivial. However, key distribution is less expensive than session key approach since it is done when a customer leaves the group. In all the above approaches, the size of the broadcast data increases as the number of consumer increase.

CONCLUSION

We studied special requirements of a communication infrastructure which is suitable for emergency situations. We presented our hybrid wireless mesh network performance figures and a distributed wireless mesh network is a well suited candidate which is capable of working in a heterogeneous environment where different technologies might be available as backhaul. We saw some reasons of resistance to deploy new technology by first responders and emphasized the importance of interoperation between different organizations. On cellular infrastructure, the goal is to derive traffic models so that we can allocate network resources to reach survivability. Finally, as technology grows so fast, privacy concern in information sharing and data manageability becomes crucial. In our hybrid wireless mesh network, all public safety personnel communicate over the same system, however, data should be secured for each specific organization so that others which have not been originally assigned to this specific task, will not be able to access that data.

ACKNOWLEDGMENTS

Work described in this paper was funded by the RESCUE project at UCSD, NSF award #0331690, and the Responsphere project, NSF award #0403433.

REFERENCES

1. Dilmaghani, R. B., Manoj, B. S., Jafarian, B., R.R. Rao, (2005) Performance Evaluation of RescueMesh: A Metro-Scale Hybrid Wireless Network, *Proceedings of IEEE WiMesh 2005.*
2. Morentz, J. W., (1994) Can We talk*, Proceedings 1994.*Rockville, Maryland, 1994.
3. http://www.firehouse.com/terrorist/911/11_NYTregroup.html
4. Tierney, K., Sutton, J., (2005) Cost and Culture: Barriers to the Adoption of Technology in Emergency Management, *Proceedings of Natural Hazard Workshop 2005*.
5. http://www.itr-rescue.org/
6. http://www.calit2.net/
7. Tipper, D., Dahlberg, T., Shin, H., Charnsripinyo, C., (2002) Providing fault tolerance in wireless access networks, *IEEE Communications Magazine,* 1, 40, 58-64.
8. Brass, V., Fuhrmann, W. F., (1994) Traffic Engineering Experience from Operating Cellular Networks, 8, 38, 66-71.
9. http://www.opnet.com/services/university
10. Raheleh B. Dilmaghani, (2003) MS Thesis, An Investigation to Fast Modular Multiplication and Exponentiation Techniques to Speed-up RSA-Like Crypto Systems, Department of Electrical and Computer Engineering, Colorado State University.