Abstract: Communication infrastructure has some specific requirements that need to be considered within the context of emergency response scenarios. A few examples are the reliability, robustness, and the ability to work with other existing technologies, namely the interoperability and compatibility of such implementations. There have been several examples of communication failures between different first responder organizations in different disaster scenarios. For example at the World Trade Center on 9/11 some of the police warnings were not heard by firefighters resulting in several lives lost [5]. To address this problem, we propose a Hybrid Wireless Mesh Network (HWMN) as a candidate for highly reliable communication infrastructure capable of working in a heterogeneous environment with different available backhaul technologies for Internet connectivity. Also, cellular technology, as a pre-existing infrastructure, can be taken advantage of when the service is available in an emergency situation. We are using cellular simulators to study the possibilities of integrating cellular systems with other systems to evacuate people more efficiently in case of emergency and present alternative routes to avoid traffic congestion.

Keywords— Disaster categories, interoperability, World Trade Center, social challenges, hybrid wireless mesh network, cellular infrastructure, redundancy, information sharing and privacy.

I. INTRODUCTION

This work studies different key factors in designing a robust communication infrastructure with applications to emergency response. One key factor to consider when developing warning systems is the category and nature of disasters. We will discuss different categories of disasters in next section of this paper in more details. Examples of factors that impact the development of warning systems include degree of urbanization, spatial breadth, time length, and whether the disaster had been anticipated or not. Clearly, sudden natural or man-made disasters will not give sufficient warning time. Wild fires by nature may not allow for warnings initially, however as they spread, there is a very short time to warn people and disseminate evacuation information. Other disasters may give a longer time window to warn people and take appropriate actions. There are important sociological factors which need to be considered in developing warning systems such as the age and physical ability of people and their preference for method of dissemination, which may vary depending on the time of day. There is ongoing research on these considerations and on what the content of these warning messages should be to make people take them seriously [8] and take appropriate action. Also the content of the warning is very important as it needs to convey the nature of disaster clearly and provide sufficient information to avoid the disaster or reduce loss.

A secondary set of issues that we would like to address here is the overall problem with existing communication infrastructures such as unreliability, interoperability, possibility of network partitioned [6], efficient network resource allocation, and the ability of organizations to adopt new technology. These are some of the special requirements of communication infrastructure for emergency response. Hence, we propose a hybrid wireless mesh network as a communication infrastructure to deploy at disaster site where the existing network is partially or fully unavailable [1]. In this architecture, only the gateway(s) needs to be wired physically to access outside world whereas all relaying nodes are able to find each other and form a mesh network as long as there is a line of sight between the nodes. The advantage of this architecture is that it is capable of using any available technology as backhaul and does not rely on any existing infrastructure to form a network. Furthermore, it allows for communication within the disaster site even if no backhauls

This work was supported by the National Science Foundation awards #0331690 and #0403433, Rescue and Responsphere projects.
are available.

Interoperability between different devices used by different organizations involved in an emergency situation has always been a problem. In most cases they have not been really able to communicate with each other [2]. This may happen either because the network is unavailable at some point of time or different devices have been incapable of working together and coordinating. Considering the scale and frequency of the recent disasters such as World Trade Center, and Hurricane Katrina, there has been more attention on the continuous availability of a communication service to assure the best and fastest possible actions at rescue and recovery stages. Also considering the different ways the nation is affected by each one of these large scale disasters shows the importance of developing research in such wide multi-disciplinary research areas. This requires electrical and computer engineers to work closely with social scientists, structural engineers, and researchers from many other disciplines to identify the vulnerabilities in the proposed communication infrastructure and improve system reliability. Some of the frequently observed, serious outcomes of disasters are: loss of lives, health issues, social effects such as looting, or economic pressures such as price gouging, more specifically gas price and loss of the tourism industry. Based on an article in the New York Times on the 9/11 disaster, Police helicopters hovered near the remaining first tower minutes after it collapsed, and there were reports of pilots asking for evacuation of all people in the area of the second building. However, fire department did not hear those warnings [6] [10]. The cross-organization radio broadcast system failed many times that morning, and even if the radio broadcast system was working properly, it was not linked to the Police radio so other response organizations could not hear them and take the appropriate actions. This confirms the necessity for a technology that is able to work with heterogeneous devices to be able to send and receive messages between different organizations. Therefore a robust communication technology needs to provide an interface to other first responder organizations’ systems as well.

Finally we briefly touch in this paper on the importance of sharing the right information with right people at the right time. At the homeland security level, this is very crucial, and privacy should be enabled in transmitting information.

The organization of the rest of this paper is as following: in section II, briefly we discuss the social and technology challenges in emergency communication deployment. Section III presents the shortcomings of the existing communication technology, the solutions we propose, and the research in progress we are conducting in order to design a reliable robust communication infrastructure. Section IV provides a brief discussion on the concerns surrounding information sharing and privacy issues with the rapid growth of communication technology and Internet. Section V concludes this paper with a review of the important factors needed to be considered in a communication network design with particular application to emergency situations.

II. SOCIAL AND TECHNOLOGY CHALLENGES IN EMERGENCY SITUATIONS

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

Disaster Categories- Disasters differ from each other depending on their scale which is crucial to consider in designing an appropriate response/recovery system. This can be defined by the degree of urbanization or the geographic spread. Degree of urbanization is usually determined by the number of people in the affected area, which is very important in disaster handling as the impact of the event changes based on the number of people involved and the breadth of spatial dispersion, both of which impact response and recovery from disasters. Disasters such as wild fires may affect a very wide area in national parks at a first stage, however if they do not get under control in a timely manner, they may eventually lead to a second disaster and impact more people. We want to provide a robust communication infrastructure to transfer relevant information such as digital maps, etc to enable responders to make decisions in a timely manner to save lives. On the other hand, when a disaster happens, first responders are sent to the site immediately and require a communication infrastructure set up to provide them with data and transfer urgent information from them back to command and control center. As pointed in introduction, one key factor which makes a big difference in the response and recovery stage is whether the disasters have been predicted or not. If there is advance notification, we are potentially able to set up a better communication infrastructure and possibly even have a backup technology in place before the disaster occurs. Designing a robust communication infrastructure which is reliable with enough resources considering all the different factors is a demanding task.

Specific technology requirements- Sometimes depending on the nature of disaster, there are more specific communication needs. For example, telemedicine communication may require interactive real-time communication. Physicians and patients need to share particular types of information such as care protocols, symptoms, and medical background. Transferring data, audio, and video require special bandwidth requirements and high network security to meet HIPAA requirements at low cost. The service needs to be reliable and continuous and work with other different first responder organizations’ devices if necessary. Users may have different devices such as laptops, palms, or cell phones which may work with different network technologies such as WLAN, Wi-Max, WWAN, Satellite, or wired networks. Additionally a communication network needs to be easily configurable, and quickly deployable at low cost. In next section, we will address this problem by using our mesh nodes designed and developed in-house which are capable of using any available technology and are able to talk to each other and very easy to configure.

Resistance to adopt new technology- Communication
infrastructure should be able to operate in a highly distributed though infrastructure-less manner. However there are practical concerns in deploying new technology and factors such as cost and culture which resist to adopt new technology [7] [10]. We would like to have systems that are easily upgradeable as the technology evolves. It would be very costly to frequently pull out the old system and replace it with new technology. Currently, there is a strong need for public safety agencies to replace their existing networks [19]. When doing this, it is very important that they select systems that fulfill public safety operational requirements considering all possible natural hazards. We also would like to leave some redundancy as back-up to handle emergency situations more efficiently and quickly. However there is always a trade-off between cost and redundancy. This trade-off point varies between different scenarios considering the probability and risk of failure, and the degree and scale of possible outcomes. There have been studies providing insight into the ways in which institutions can proactively incorporate social factors into communication technology [12].

Interoperability- Communication technology provides the tool to send data; however when information is sent over different channels or systems, interoperability may not necessarily have been provided. In the next section we will see how this problem can be waived by using CalMesh boxes, each of which is capable of using different technology by choosing the appropriate interface card, and still they work together to from a mesh network and communicate data. Therefore regardless of what technology each individual might use, they are uniformly connected to the relaying mesh nodes and able to exchange data.

Interdependency- Another factor which needs to be considered in the design of future communication technology is minimizing possible interdependencies in a system [23]. This helps to design a more robust system which is resilient to failures in sub-components of the system.

Knowledge and training- An important factor to be considered as addressed is the lack of knowledge on exact capabilities of the new technology being deployed and lack of training [20]. The new technology needs to be installed and fully tested in drills and preparation exercises well before it is used in an actual disaster. It is also very important to consider who will be the users of this technology and what level of knowledge and technical background they have. We would like to design future emergency communication tools and public awareness systems to be user friendly with minimal training requirements, yet also secure. For example, a simple identification process to login into a system might require users to provide fingerprints as a credential.

Information Sharing and data dissemination- In some disaster scenarios when people have important information, there needs to be a motivation for them to share it across first responder organizations. When the information is provided, there needs to be some mechanism to verify the accuracy of the information provided. Privacy is a factor that needs to be considered in determining who should have access to this information.

Warnings and alerts- Warning messages should be provided with the consideration that some people may disregard the warnings, therefore even the well-designed warning system must consider human error or resistance. People may not evacuate to safe areas even if asked or ordered to do so for different reasons such as family, belongings, and pets, or they may not trust the accuracy or source of the warning. They may not take the warning serious if they hear different messages from different sources, or if the source of the warning has not proven to be accurate or reliable in the past. The warning should provide a clear explanation of the nature of the disaster and appropriate actions to be taken.

III. COMMUNICATION TECHNOLOGY

There are four different stages in a disaster management based on US Federal Emergency Management Agency (FEMA): mitigation, preparation, response, and recovery. A reliable robust communication technology is necessary to transmit information at all stages. However for disaster response and recovery there is a more specific need to deploy an infrastructure which is quick and easy to configure and reconfigure. These two stages can be considered more time-sensitive while the first two usually have a longer planning time.

In emergency communications, we need to transmit relevant information from the disaster site to the decision makers and send feedback from first responders regarding potential dangers or decision [22]. Another important consideration for the networks is that network load changes rapidly, so that we may need to include different service support in order to assure transmission of high priority data. We need to make sure that the data is transmitted in a timely manner and network overload is avoided.

In this section, we discuss our solution for a network that is quickly deployable in an emergency situation. Our research in progress is working towards avoiding network congestion and large number of call drops in cellular networks in affected areas.

Hybrid Wireless Mesh Network- Wireless Mesh Networks (WMNs) have become very popular for the use of free unlicensed spectrum and low cost of IEEE 802.11b/a/g off-the-shelf devices. We have proposed a Hybrid Wireless Mesh Network (HWMN) for emergency situations which uses point-to-point and point-to-multipoint long haul wireless links in order to provide gateway functionality for multi-hop wireless networks [1]. We have also deployed the infrastructure in several drills at the university campus and city levels, and in exercises of the San Diego Metropolitan Medical Strike Team (MMST), a group of local, state, and federal response agencies that work together in planning and preparation for large-scale disasters. The architecture of the HWMN provides a quickly deployable and highly reliable WMN infrastructure with minimal configuration using Wireless Wide Area Networks (WWANs) as backhaul links with no necessity for wired backhauls. The mesh architecture
of this network is resilient to the failure of nodes, as there are alternate paths to take in case a link or an intermediate node becomes unavailable. In this architecture only gateways are connected through wireless long haul links which is considered as an advantage as fewer nodes (only gateway(s)) need to be configured/re-configured and it is easier to deploy at emergency situations. The packets are forwarded in a multi-hop fashion throughout the network to reach their destination. We are currently working on routing algorithms to improve network throughput based on special requirements and features of the network. It allows use of any wireless user device, and does not require an 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 existence of long haul wireless link facilitates faster and more cost-effective service, while providing faster data dissemination and higher reliability.

This infrastructure has been developed and deployed as part of the RESCUE project [3]. We use Wi-Fi access points to provide broadband systems to access Internet. These wireless access points operate on the free unlicensed spectrum to provide broadband service when the wired network fails. Their wireless antennas are able to find each other and talk to each other which allow users to access the service when there is no wired network available. In addition to this deployment, the California Institute for Telecommunications and Information Technology (Calit2) [4] has designed and developed CalMesh nodes, a portable wireless access points. We recently deployed a HWMN with CalMesh nodes at an event in downtown San Diego and were able to put sensors on the network and collect real data over the network.

We have also deployed a wireless mesh network at a MMST drill with medical applications. Patients were tagged with wireless devices which were connected to Internet through the Mesh nodes, communicating patient health status and vitals information to medical personnel at the site of the disaster. In this drill, there were three gateways which connected to the Internet by different available backhaul technologies including 1xEVDO, 1xRTT, and satellite.

Figure 1 shows the mesh network architecture discussed above. Different user end devices with multiple interface cards can use different available technologies such as Bluetooth, CDMA2000, GSM, etc while still able to connect to the CalMesh nodes which are able to from a local network and communicate to the outside world through Internet as well.

Figure 2 shows the architecture of the network deployed at the site for a HWMN deployment at a full-scale homeland security drill organized by the MMST where we were able to collect real data from the medical first responders’ communication over the network. Below, we present some of the statistical network data gathered from this drill which helps us derive models for typical network communication patterns in emergency situations. Figure 3 shows the number of bytes broadcast over the network for a partial set of data.

For this particular set of data, the percentage of the number of bytes transmitted over TCP was approximately 50% of the total number of bytes.
Figure 4 shows total number of bytes transmitted over TCP, and UDP in addition to the total number of bytes broadcast over the network. In this partial dataset, more bytes are transmitted over reliable TCP, but this varies depending on different applications. Generally to transmit small amount of data, UDP introduces a smaller delay compared to TCP with its three-phase handshake mechanism. To transmit video and digital maps over wireless links with a high link error and propagation delay, UDP outperforms TCP again in terms of data rate and congestion avoidance. In this particular application, there was more data that needed to have a reliable transmission therefore the major part of data was sent over TCP. Different protocols are used to transmit data with best quality and reliability depending on the application type and sensitivity of the information being transmitted. For the scenarios which may need to send data to a large number of people i.e. to broadcast larger amount of data, we could take advantage of cellular infrastructure if the service is available.

**Cellular Infrastructure** - Cellular network is a pre-existing infrastructure and it is of very high value to take advantage of this service if it is available at disaster sites. However, in some disaster scenarios the service becomes unavailable due to power outage, physical damage to the tower [10], or unexpected load increase in the network. There has to be an alternative plan to call people. That is where we setup our evacuation simulators in order to route traffic more efficiently and run real scenarios with the data on the network. There will feed these results into other simulators to route traffic more efficiently and run real scenarios with the data on ground zero to find out where the cell user is located. As one solution to this problem we suggest that replica copies of home agent information should be placed at different locations. This causes some redundancy to insure network reliability in case we lose one agent during a disaster. It is very important to notice that there is a tradeoff between redundancy and cost.

In order to design a cellular infrastructure which survives all natural and man-made disasters we need to minimize the number of calls to be dropped or blocked. In case we need to send a message to a big group of people, broadcasting may be a better option which might already exist. Broadcasting to a group of users prevents network overload and congestion.

In near future, we will extend our work to integrate cellular simulations with other simulators such as transportation and evacuation simulators in order to route traffic more efficiently at the affected areas to insure that cellular infrastructures are not overloaded so that broadcast warnings and messages are still received. This integration can mutually benefit social scientists and other researchers with interests in crowd behavior dynamic in emergency scenarios. As mentioned earlier, it is understood that there might be some resistance to using cell phones to communicate with work colleagues in an emergency, though it has been widely used to talk to friends and family.

**Deriving traffic pattern and monitoring resource usage helps minimize network congestion.** When a disaster like Katrina happens, because of loss of base stations, frequency of call volume, and other factors that influence cellular network traffic, people who own a cell phone lose access and are not able to call their family and friends just like those with access to wired telephone networks. We will present some of the simulation results using a UMTS module with W-CDMA technology. This is a work in progress and in the future we will feed these results into other simulators to route traffic more efficiently and run real scenarios with the data on the failure of affected base stations. When a disaster happens, users’ mobility pattern changes as some bridges and paths...
become unavailable. We try to extract traffic patterns based on these data to be able to manage cellular network resources more efficiently after a disaster. Here we present the results obtained from the following two scenarios: one with all base stations active and running and the second set of results with one base station out of service (Base station number 1).

Figure 5. Cellular Network Topology

In this scenario, 23 User Ends (UEs) send large data files to the server with Poisson arrival time distribution with mean 120 seconds throughout the simulation. Four users are mobile for this scenario and handover is defined for them. However further investigations in their mobility will be presented in our future work. Traffic is considered interactive and Quality of Service is of priority level 3 correspondingly. Figure 5 shows the simulation project discussed above, and figure 6 presents the results for total uplink throughput for base station number two in packets per second with the average maximum of 145/140 packets per seconds for scenario 1 and 2 respectively.

Figure 6. Average total uplink throughput (packets/sec)

Figure 7. Handover: Cells added to active set for UE 1

Figure 7 presents the results for total downlink throughput for base station number two in packets per second with the average maximum of 45 packets per seconds.

Figure 8. Average total transmit load (Pckt/sec)

Figure 8 presents the results for average total transmit load for radio network controller number one in packets per second with the average and maximum of 22/12 packets per seconds for scenario 1 and 2 respectively.

Figure 9. Average total received throughput (Pckt/sec)

Figure 9 presents the results for average total received throughput for radio network controller number one in packets per second with the average and maximum of 180/105 packets per seconds for scenario 1 and 2 respectively.

The throughput of the network is dropped for scenario two where one base station becomes unavailable. Lower throughput occurs because the network load exceeds the capacity of the network. Therefore, the server is not able to meet all clients’ requests. The goal is to extend these investigations and design redundancy in the network capacity so that a sudden increase in load can be accommodated.

IV. INFORMATION SHARING AND PRIVACY

We discussed earlier that in an emergency situation if there is no network available, we deploy our hybrid wireless mesh network. This is probably the common infrastructure in many deployments where multiple different organizations communicate over the same network. For security concerns, it is desired that each individual organization receives only the data relevant to them. In a typical emergency situation, people from Red Cross, Fire department, Police, Media, etc. communicate over the same network. In medical applications,
one’s medical file should be visible only to the medical team as part of personal privacy requirements established by HIPAA (Health Insurance Portability and Accountability Act). Media are always at a disaster site but are not supposed to have direct access to much of the data being communicated over the shared network, as they should not have access to data which is not meant for the public.

To a certain extent, in emergency scenarios, violation of one’s privacy is inevitable as life-saving measures tend to supersede desires to maintain privacy. However, privacy breaches can be limited to certain types of data or to a minimal number of people. In many cases, to assure that the right information reaches only the right people, data should be encrypted. We need to design an encryption system such that each type of data is encrypted by a different key so that only the designated party is able to decrypt and access that information. There are many different protocols in traditional security systems to provide this type of privacy. In order to have a secure communication between different organizations, we need to choose the most appropriate and straightforward group communication protocol to have the communication up and running in a very short time. In many scenarios, we want to have the infrastructure operational immediately as it is one of the primary concerns in rescue and response stages. Therefore a feature should be implemented in the network enabling users to turn encryption on or off by pressing a knob or. Authenticating people to make sure that the information they provide is trustworthy or to authenticate them for access to data is another challenge which needs to be addressed carefully. Fingerprints are suggested as a means for identification as it does not require any special knowledge and thus might be useful for untrained people at the site. Message integrity is another concern as when data flows in a network it may be collected with error and lead to wrong decisions being made. There should be mechanisms to verify the accuracy of information.

Location detection by cellular phones can be very useful in emergency situations however may be considered an invasion of privacy, but depending on the scenario and the application, it may be a price individuals are willing to pay to insure their safety [16].

In order to encrypt messages in group communication, there have been different protocols discussed [11]. If the server encrypts the data object and broadcasts it, the broadcasted message will consist of the concatenation of the same object data encrypted by each individual’s public key. Therefore, the same message is inefficiently encrypted multiple times and broadcasted. Whereas with a session key protocol, each broadcast is considered a session. There is one session key assigned to each session, which is discarded after the end of the session. In this protocol, there is an encryption/decryption pair per object per session. The server encrypts the data with the session encryption key and broadcasts it. The length of the message will depend on the number of subscribers for each data item, and the customer subscribing to more than one data object will receive multiple decryption keys [10]. Therefore, key management can become a concern, but since each key lasts only for the duration of the session and is discarded when the session is over, it is a minor concern. However, for multiple data objects to be transmitted, key distribution remains a major problem because all session keys need to be distributed to all subscribers within a session. Another approach which utilizes a group key concept is when 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. Data items will be encrypted and broadcast with the new group key. The new group key will be encrypted by customers’ public key and transported to new members of group. For the case a customer subscribes to multiple data objects, their device has to manage multiple group keys, and since group keys are used multiple times, managing and storing multiple group keys is not trivial. In the above approaches, the size of the broadcast data increases as the number of consumers increase and key distribution or key management can become an issue which needs to be addressed in future research.

V. CONCLUSION AND FUTURE WORK

We studied the special requirements of a communication infrastructure in emergency situations and discussed some of the social and technical challenges existing in designing and deploying a robust and reliable communication infrastructure. A Hybrid Wireless Mesh Network has been proposed as a well-suited candidate capable of working in a heterogeneous environment where different technologies might be available as backhaul. We also reviewed a few reasons why some public agencies may resist deploying new technologies. Interoperability between different organizations has always been a concern which has been addressed here and can be improved by deploying Calit2’s CalMesh boxes with multiple interface cards. We also need to eliminate unnecessary interdependencies between different components of a system. We would like to take advantage of pre-existing cellular infrastructure therefore developing real scenarios and trying to integrate this with other simulators in order to be able to allocate network resources more efficiently and route traffic effectively to reach a survivable network in an emergency. This study can be of mutual benefit to social scientists and other researchers with interest in crowd behavior dynamics in emergency scenarios.

And finally, as technology develops, information sharing and privacy concerns grow and data manageability becomes more crucial. We will address potential and possible design aspects in our future work.

ACKNOWLEDGEMENTS

Work described in this paper was funded by the RESCUE and ResponSphere projects at UCSD, NSF awards #0331690 and #0403433. I would like to also thank our project team members at Calit2 with special thanks to S.H. Bristow for help with readability of the paper.
REFERENCES