An Ad Hoc Network Infrastructure: Communication and Information Sharing for Emergency Response

Raheleh B. Dilmaghani and Ramesh R. Rao*
University of California, San Diego, 9500 Gilman Dr., La Jolla, USA
rdilmaghani, rrao@ucsd.edu, * UCSD Division of Calit2

Abstract— During an emergency response, access to a reliable communication infrastructure is required to exchange accurate information in a timely manner. Various communication technologies have been deployed for emergency response; however communication between different first response organizations has always been a problem. This is due to either broken networks or lack of knowledge regarding the channel frequency in use for the same device. According to recent investigations, text messaging was shown to be more reliable than voice to exchange short messages carrying critical information. Additionally, posting and updating the information on an electronic webpage accessible to all is also very useful. In addition, we would also suggest that team leaders physically stand together, thus improving network resource utilization plus ensuring receipt of updates and information from peers in the event the higher ranked person in the hierarchy is not reachable.

In this paper, we present supporting arguments for the choice of a wireless mesh network as a candidate to provide communication infrastructure for emergency response. We also present a comprehensive set of technical, social and organizational challenges which we experienced first hand during several deployments, learned about in interviews with emergency responders and by examination of the after-incident reports. Many of these challenges become even more of a concern and have a greater impact on international disasters concerning multiple countries when traditionally different technologies are used often in conjunction with different languages. We also present the results of network performance analysis which identifies sources of bottleneck and overhead in communication. A distributed control hierarchical authority is necessary to prevent bottleneck and the need to cancel an already scheduled path due to resource unavailability or security breach.

Key Words- Wireless mesh test bed, interoperability, reliability, emergency response, text messaging, electronic update board, information sharing and resource management.

I. Introduction

The importance of communication in an emergency response scenario is well known throughout the world due to the frequency of recent incidents and the wide range of impacts. In this work we present the state-of-the-art of communication technologies used in emergency response. We also present various projects based on wireless communication technology deployed as part of several drills conducted on campus, city, and county levels with several research groups participating, including the Rescue, WIISARD, and Responsphere projects from the UCSD division of the California Institute for Telecommunications and Information Technology (Calit2) [1] [2] [3] [4]. We present an exhaustive list of technical challenges for communication networks at disaster sites, in addition to the social and organizational challenges of deploying a communication infrastructure at crisis sites, directly extracted from real case scenarios. We address the problem of efficient communication considering human involvement. In real emergency scenarios, humans' communication and the flow of information affect the response time, as well as the procedures. There are limited resources in the network and the network management needs to be aware of resource status, limitations and conflicts at all times in order to allocate them based on priorities.

The organization of the rest of the paper is as follows: in Section II we present the state-of-the-art of the communication technologies for disaster scenes. In Section III we present the technical, social and organizational challenges in the design and deployment of new communication technologies. Section IV describes the requirements of a communication network infrastructure with application for emergency response describing the supporting reasons for a wireless mesh network as a suitable candidate. This is followed by the description of the wireless mesh network deployed at several drills with performance evaluation results identifying sources of bottleneck and lessons learned. Section VII presents our findings and suggestions to improve information management and resource allocation. Finally, we conclude this work with a closing discussion on the main contributions of this paper in Section VIII.

II. State-of-The-art of communication infrastructure for emergency response

The National Institute of Standards and Technology (NIST) has a Distributed Test bed for First Responders (DTFR) which is a vehicle that provides wireless connection for first responders at a disaster site. The Advanced Network Technologies Communication for

public safety is a division within NIST whose contribution to DTFR is a wireless ad hoc network using 802.11 off-the-shelf devices to provide users with network connectivity. The users can work with several handheld communication devices equipped with an IEEE 802.11b WLAN card and uploaded with NIST software. These communication devices are easy to configure as they automatically form a network as long as they are within radio range of each other. This includes the transfer of voice communications, video streaming, data, short messaging, and access to Internet over wired and wireless networks with the legacy standards [5].

Many existing communication infrastructures became unavailable after Hurricane Katrina hit New Orleans, LA including one of the 800 MHz communication towers. Therefore first responders did not have access to a reliable communication infrastructure to coordinate emergency response activities, transfer data and exchange information locally and to the offsite command centers [6]. FEMA provided the affected area with MERS (Mobile Emergency Response Support) to provide a communication network to enable first responders to exchange information via a video teleconference to the offsite command center. MERS includes trained personnel and a vehicle which provides mobile communication support for voice and data [7].

According to area Sniper investigations report in Washington DC, Montgomery County Police Department (MCPD) communicated to the county through available devices including radios working with different frequencies during the emergency response. Each organization (for the city or county) had a dedicated channel and they talk to their own dispatcher at all times. Federal agents and MSP (Maryland State Police) officers who were initially assigned to the task force were using their cell phone and portable radios on Very High Frequency (VHF) which was not interoperable with task force members. MCPD UHF system was also overloaded as the result of incoming traffic to respond to the citizens. A new 800 MHz voice radio system which was fully tested before but not installed at the time was placed into service earlier than planned to serve as a patch to provide interoperability with the UHF legacy system. MCPD distributed a few 800 MHz portable radios to be used by the other agencies to provide interoperability. Audio cross-connect switches were deployed in some counties and the City of Alexandria for sniper investigations. This switch provides interoperability between radio systems working on different frequencies in a heterogeneous environment. Therefore different organizations were able to communicate across systems by switching to the operating frequency [8].

The Wireless Emergency Response Team (WERT) was established after September 11, 2001 to provide wireless connectivity for first responders to facilitate emergency response and rescue efforts [9].

The Virginia Tech telecommunication network infrastructure is a fiber optic core IP-based data network which provides a reliable communication network for users (wireless or wired) throughout the campus. During the response to the Virginia Tech Massacre on campus in April 2007 which was comprised of two shootings, the load on the network was increased but the network was able to perform reasonably well with no significant breakdown under the high traffic circumstances. During the crisis, the network staff was responsible to support the infrastructure to ensure reliability for data transfer and voice. According to the report communication and exchange of information relying on the internal phone system, instant messaging, e-mail and cellular short message service worked fine during the response. However voice service provided by external vendors reached saturation levels at times making it unreliable communication tool for exchange of information. The network engineers quickly reconfigured a National LambdaRail [10] network connection on-the-fly to increase the network capacity by 1 Gbps to avoid potential bottleneck or congestion in the network and avoid delay or loss of information. According to the report the campus telephone system was able to receive and transfer calls without failure although some delay was experienced on the lines connecting the campus and the city of Blacksburg to the outside network.

There have been problems experienced with the radio coverage indoor for different first response organizations according to the report. The signal was attenuated or there was no coverage at some indoor locations. Mobile broadband Internet access was not used by Virginia Tech Police and Virginia Tech rescue Squad during the April 16th incident. Different first response organizations used radios working on different frequencies such as UHF, VHF, 800 MHz, etc. which caused interoperability problems [11].

In 2001, the Miami-Dade Fire Rescue (MDFR), FA began to utilize the initial VoIP which takes advantage of already existing infrastructure for data to transfer voice at a lower cost. This has enabled firefighters to talk to each station they need to which is very convenient as many of them are moved around and need to call other stations [12].

Push-to-talk systems have been used for emergency response for years. The problem with them is the lack of interoperability and incompatibility with the other existing communication technologies.

Text messaging or instant messaging are also beginning to be used for early warnings or exchanging information when a disaster happens. For example during the recent earthquake in Los Angeles, CA (July 2008), the data network for sending text was not as congested as voice. There was no outage but there was an increase in the volume of calls [19]. Text messaging is a good alternative to share critical information as short messages as it does not consume bandwidth resources and there is a better chance of successful transmission compared to the voice network which is often busy and unreachable due to sudden network load increase after crisis.

We believe that the use of an electronic post-it board is a useful method to share information regardless of technologies used by individual organizations. Information can be accessed via a web-browser on a

computer or cellular-phone. There are several software tools available, one being WebEOC. However based on our understanding due to the high cost of software license, it is available to a very limited number of first responders at a few emergency organizations. Therefore creating and developing electronic pages such as wiki pages accessible to public will be very beneficial.

III. Technical, social and organizational challenges of communication technologies at crises

When an emergency occurs, usually the response process starts with the dispatch center receiving a call. First responders are called to the site immediately. The first attempts into the hot zone, usually by specialized forces such as Bomb squad or HAZMAT, aim to make the hot zone safe for other responders to enter, particularly and most urgently for emergency medical team to enter for triage needs. At the same time, the effort to establish a communication infrastructure is happening in the cold zone to exchange information with the dispatchers and incident command center. The communication infrastructure is to provide decision makers with real-time data and information to assist them with accurate decision for a fast and effective response. There are several technical, social and organizational challenges that responders face during an emergency response. Below we present the challenges that we have experienced during our involvements at several drills, as well as from interviewing team leaders from first response organizations before or after the response and careful examination of after-disaster reports.

a. Inter-organization communication

Interoperability in a heterogeneous environment is crucial for communication and coordination among different agencies where different technologies such as UHF/VHF radios, 800 MHZ radios, push-to-talks, wired and wireless devices are used. The interoperability becomes more of an issue at an international level as there would be different technologies used and even different languages and hierarchies. In an emergency response organizational chart, vertical communication typically refers to within an organization while horizontal communication refers to inter-organizational communication, among team leaders and across different jurisdictions. Based on our observation, in most scenarios horizontal communication is more of a concern as different groups are almost always able to communicate with their own team members but unable to talk to peers. Even when different groups have the same type of radio or technology, they may not be aware of the channel used by their peers therefore information does not flow thoroughly through the network.

b. Resource allocation

The term “resource” refers to network resources such as bandwidth, human resources and apparatus. The information on the status of resource requests, allocation and release must be available and updated in real-time to enable accurate decisions and efficient resources allocation.

c. Choice of backhaul

To establish communication between disaster site and outside world the infrastructure needs to get connected to Internet through a backhaul link. The choice of backhaul depends on available technologies and the amount of bandwidth or data transfer required.

d. Network reconfiguration

In an emergency response, there is often a strong need to move nodes and reconfigure the topology. If the signal strength through a relaying node falls below a threshold, the network establishes a new connection seamlessly through a different path providing a better signal strength. Additionally in a multi-hop ad hoc network, it is preferred to be connected through the paths that are not more than two hops away from the gateway. This is to keep the signal strength above a satisfactory threshold and ensure acceptable throughput.

e. Network reliability and message integrity

It is of highly importance to repeat or send information or messages intact throughout the network. Failure to transmit the message precisely has been the cause of broken communication in past.

f. Traffic management and quality of service

Network management can allow the network to provide different services for different priority tasks depending on resource availabilities. Different traffic types can be scheduled with respect to the constraints, quality of service requirements and availability of the resources.

g. Limited support for encryption or mobility

An emergency response depending on the application may require different levels of encryption or information privacy. The communication infrastructure also needs to support mobility for the users when it is needed. The network should support mobility as users or access nodes move around the site.

h. Minimize dependencies

Emergency response is an interdependent process by nature. It is desired to reduce the amount of dependencies in technical specifications like having a back up source of power or battery-operated for short-term deployments in case power infrastructure goes down. Similarly in an inter-organizational chart minimizing dependencies is desired. This can be interpreted as the functional cohesion corresponding with loose coupling. Naturally it is preferred to eliminate unnecessary dependencies and interactions to protect the system performance and achieve the overall objective in case of individual’s failure. We do not want to turn one organization to a bottleneck and a single point of failure in case of unpredictable disconnection in communication.

i. Scale and nature of disaster

Decision and resource allocation in a disaster response varies from one incident to another depending on the scale and the nature of the disaster. The degree of urbanization or the geographic spread may require different actions for a specific respond. When the incident(s) is geographically dispersed, it requires a lot of coordination.

j. Training and Financial obstacles

There is a natural resistance to try out the new technology while the old system works. This might attribute to the cost of replacing or upgrading the existing technology and the cost of training people to learn how to work with new technology.

k. Cultural barriers

Different organizations may resist deploying new technology for different traditional and cultural reasons. Additionally each organization has a pride in their departments and there is a tendency to be self-sufficient rather than cooperating with others. This slows down the effectiveness of a response as it creates delay in sharing resources and coordination which are vital to an efficient response. To address this, a higher authority (like MMST Task Force Leader) is responsible to set the overall objective and ensure that all organizations work together to achieve that goal for an efficient response.

l. Precise personnel accountability

Another practical issue in an emergency response is to obtain accountability of personnel attending the response. Responders arrive at different times and before the mobile check-in staff gets to them, the special protection force might have their sealed-out uniform on which does not allow scanning the magnetic badge. When there is not an exact list of who attends the site, the communication is seriously affected. It is difficult to carry-on a well-planned and well-organized response if there is not precise knowledge on the list of personnel attending the crisis site! We believe that an electronic check-in check-out system will assist with the problem so that every one entering the site or leaving the system has to go through it prior to attendance or departure. This solution is similar to the accountability check-in process in use by cruise lines. A unique magnetic ID card can be activated upon an emergency which can be retrieved upon departure and demagnetized to be re-used. This may take us to financial obstacles in item j but it is a one-time cost.

IV. Choice of Wireless Mesh Communication Network

A communication infrastructure within the context of emergency applications should be reliable, robust, easily configurable, quickly deployable at low cost and interoperable in a heterogeneous environment with minimum interdependencies.

Based on the study of literature and state of art presented in section II, we see the need to have a solution that addresses interoperability between different communication technologies in a heterogeneous environment. If different organizations use different radios operating on different frequencies, interoperability is the main common problem as different responders cannot talk to each other. Lack or limited support of encryption, mobility, coverage (indoor), and geographic situational awareness are the other common aspects that need to be developed. However in the most recent crises, there has been a better use of recent existing technologies in the sense that they have been able to establish patches quickly to enable different first responders to talk to each other which has been a problem throughout different disasters.

Wireless mesh infrastructure is a candidate to be deployed at crisis site for the following reasons: in mesh architecture, only gateway(s) is connected through wireless long haul links, which is considered advantageous, as fewer nodes need to be configured. Wireless access nodes form a network when there is a line of sight. The mesh architecture is resilient to the failure of nodes or links as there are alternate paths to take if any one link fails. Similarly, a node can communicate through other nodes when a neighboring node fails. This characteristic improves reliability, as unavailability or failure of sub-components of the system does not affect the overall performance of the system and the service will be continuously available. This architecture is robust in the sense that it is able to operate in a heterogeneous environment with a variety of technologies. Additional wireless access nodes can join the network without causing a service interruption by finding the closest node with best signal strength and connecting to expand the existing network. Therefore this infrastructure provides a robust deployment solution for organizations as changes are transparent to the rest of network nodes.

Finally, at a disaster site, if we need to move the nodes at some point in time, reconfiguration is trivial since these wireless access nodes will automatically form a network. These wireless access nodes allow users to communicate with each other when there is no wired configuration.

The wireless mesh nodes developed in house which has been used in several drill are presented in next section. Each wireless access node has two interface cards to provide interoperability and redundancy through the use of different channels for communication. Users using different technology such as CDMA or 802.11 can get connected and talk to each other through these nodes. VoIP can be deployed over wireless mesh network to provide an opportunity to call other responders regardless of their location. This allows responders to utilize their human and network resources efficiently with a smaller connection waiting time suitable for short-term deployments (like crisis cite) or at rural areas.

V. RESCUE Wireless Mesh Deployment and Lessons Learned

We have deployed the mesh infrastructure in several drills at the university campus and city levels as part of the NSF-funded RESCUE project (Responding to Crises and Unexpected Events), and in exercises of the San Diego Metropolitan Medical Strike Team (MMST) [14].

San Diego MMST is a team of local responders who work together to develop and implement response plans for major urban crises and disasters. The most recent drill in San Diego county CA simulates a bomb explosion inside the Coors amphitheater followed by gas spill in the city of Chula Vista and National City. In this drill several organizations participated including (San Diego city,

county and several other neighboring cities) Police, Sheriff, fire department, Emergency Medical Service (EMS) paramedics from multiple agencies, HAZMAT, bomb squads, SWAT, FBI, and the Metropolitan Medical Response Service, etc. The MMST large-scale drill took place at Coors Amphitheater and the neighboring Knott's Soak City water park in Chula Vista. Several first responder organizations attended the site to practice their rapid response and adaptability and resource allocation. An Area Command was activated to oversee the management of multiple incidents that are each being managed by a separate incident command center [15]. There were about 100 victims/patients consisting of volunteers who received instructions on their mock injuries and what they need to do in advance. The measurements have been conducted during the drills over the test bed to capture real network traffic to identify sources of bottleneck.

Figure 1 shows a wireless mesh network infrastructure deployed at a disaster scene which provides connectivity throughout the disaster site and to the outside world through Internet. The gateway can get connected to Internet through any available technology such as wired, wireless or satellite. During several drills that we have been involved we have deployed different technologies as backhaul to connect hot-zone with outside area. We have used satellite link as backhaul link in downtown San Diego, wired link on campus and EVDO at Silver Bullet drill. At Silver Bullet Drill, the infrastructure deployed at the site consisted of two independent networks at each site. Considering the small geographic spread of each incident site, it was sufficient to deploy a small network. Each site had a network consisting of one gateway and three access nodes where gateways were connected to Internet via EVDO technology. The default choice for CalMesh boxes is EVDO where it is not possible to connect through Ethernet or WiFi for faster speed or higher bandwidth. We have observed that the choice of EVDO decrease the network throughput as it is sharing the bandwidth with cellular phones and other devices deploying EVDO technology.

With CalMesh access nodes with multiple interface cards, different systems are uniformly connected to the relaying mesh nodes and will be able to exchange data regardless of their individual technology. CalMesh is an ad-hoc network device consisting of reconfigurable wireless access nodes which can be quickly configured to form a mesh network. The operating range of each access node is about 300m outdoors. Figure 2 shows a picture of the wireless mesh access node with an opened case [16].

Gizmo is another wireless mesh node as a remote-controlled truck developed in house by researchers [17]. It provides broadband coverage and situational awareness via its video and audio outputs. This device is equipped with a GPS module that allows the device to record location-based measurements. The integrated environmental sensors allow the truck to collect data on gas sensor and send measurements via SMS to a designated cell phone. During the drills, patients were tagged with wireless devices (iTAG) connecting them to Internet over the wireless mesh network. This device is used to communicate and transfer patients' medical status, treatment record, and vital information to medical personnel at the site of the disaster [18].

Figure 1. Mesh Test bed deployment at a disaster site

Figure 2- CalMesh wireless node

Real measurements obtained directly over the test bed are studied for analysis and network performance evaluation. It can particularly be used to identify all sources of bottleneck. Additionally applying the real life scenario data allows to study what if scenarios for future deployments. Here we briefly present sample results obtained from the drills in past. For this set of data, the total response time is 456 seconds. 137.6 KB of application data and 328.7KB of network data were transferred. The difference between these two values shows the amount of protocol overhead. The large number of small packets traveling over the network is the main source of bottleneck in this capture. Node 2 has a large number of application turns indicating the number of times the direction of communication changes between source and destination.

Sending large number of small packets cause potential bottleneck in the network which can be optimized by sending fewer larger packets instead. This will reduce the number of request/respond set of messages. The cause of these bottlenecks seems to be protocol overhead, chattiness and retransmission. Table 1 shows the amount of application data and network throughput between the server and mesh nodes. Application throughput is approximately the same between server and all mesh

nodes as they run similar applications. Network throughput includes all application data and network protocol overhead which is similar for all mesh nodes except node 2. Table 2 shows the total number of retransmission for each node. Node 2 has a large number of retransmission which is due to existence of error-prone links in this case (network congestion is not the cause in this scenario) and as a result the network throughput varies drastically from other nodes.

There has been several observations during these drills including first responders' communication and technical and social challenges which was presented in section III. Among other results we observed the interference among different devices employing various communication technologies which does not quite agree with theory. Additional practical observation was the effect of network partitioned due to some physical obstructions. This was experienced when a truck blocked the line of sight between two access nodes. To overcome this problem, the nodes were moved around to re-establish the connection where there was a good line of sight.

Table 1- Application and Network Data from server to the mesh access nodes (bytes-directional)

	Network Data	Application Data
Server to Node1	41.3	21.6
Server to Node2	60.2	21.7
Server to Node3	40.5	20.7
Server to Node4	42.5	20.9
Server to Node5	41.8	21.4

Table 2- Total number of retransmission from server to the mesh access nodes

Time (sec)	Node 1	Node 2	Node 3	Node 4	Node 5
0	1	1	3	4	2
50	0	0	0	0	1
100	0	0	0	0	1
150	1	2	1	6	3
200	1	12	0	1	2
250	1	15	4	0	0
300	1	9	2	3	1
350	1	14	0	1	0
400	0	22	0	2	1
450	0	1	0	0	0

VII. INFORMATION MANAGEMENT AND RESOURCE ALLOCATION

At a disaster site, communication is critical to facilitate situational awareness and interactions among different responders. Incident management should collect information and share them on a need-to know basis for an efficient communication and information sharing.

We have investigated the flow of information during the drill. Most first responders use radio technologies to talk to the people they communicate with. However some have their preference on face-to-face talks. This can have the advantage that the messages and information are not abbreviated and there is no ambiguity about the content. However as the responders get interrupted with radio or other people, there will be unnecessary repeat and some delays as it may take some time to reach the responder in person. We believe that if different team leaders physically stand together, there is no need to repeat information or wait unlimited time causing a deadlock in case the person higher in hierarchy is not reachable. The information can be obtained through a peer who has the information already. In case of a security threat, the message needs to be transmitted via a different channel (due to information breach) or take an alternate path (due to physical obstacles causing network partition or new resources). In this scenario a higher authority may need to cancel an already scheduled path or procedure. The authorities may need to get to the same site physically to exchange information securely in a timely manner.

Resource allocation is particularly important as additional resource can cause deadlock in the network. An aggressive request or organization can take over the resource in a selection and blocks fairness. This creates a deadlock in the network as the other organization never gets access to the resources. A cancelation from higher authority may be necessary in this scenario as well.

In emergency medical applications including admission to hospital emergency department or field hospitals, there is limited number of resources such as beds and doctors available. If for any reason, the manager or decision making authority does not provision redundancy and does not hold back on some resources, in case of an emergency like an urgent patient coming in, it may need to cancel an already schedule resource allocation to accommodate the new incoming request. This can be interpreted as Pre-emptive tasks entering the system. This is similar to task scheduling in a multi-task or multi-thread operating system. The pre-emptive task needs to be carried out in the system, interrupting the on-going process (resuming upon completion of pre-emptive task). This is usually decided and implemented by a privileged individual ranked higher in the hierarchy who is certified to interrupt the current state to avoid deadlock in an urgent matter.

Finally we need to maintain a distributed control and management architecture. The concept of establishing a supervisor and local controllers and articulating the roles and communication plan is of crucial importance so that one higher ranked authority does not turn into a single point of failure in case of unreachability causing bottleneck.

VIII. CONCLUSION

A wireless mesh network provides a reliable infrastructure to share data and exchange information.

Several technical, social and organizational challenges concerning developing and deploying new communication technologies such as interoperability, network reconfiguration, resource management, financial and cultural barriers have been presented. Considering the importance of knowing the personnel attendance, we propose deploying an electronic check-in check-out system upon joining or leaving the system to ensure intact accountability.

We presented the available state-of-the-art of the communication technologies for emergency response applications such as UHF/VHF and 800 MHz radios. Text messaging is a suitable alternative to exchange short messages during or after a disaster when there is a sudden increase in voice traffic over the network. Additionally public web-based pages can update and inform public. Inter-organization communication has always been a problem due to network failure, loss of the source of information or lack of a shared detailed communication plan. We presented the characteristics of mesh infrastructure such as reliability and robustness which makes it a suitable candidate for emergency response. Then we presented some results obtained over the test bed deployment along with a discussion on sources of bottleneck. Finally we presented the concerns and proposed solutions surrounding information sharing and resource management in the network for an efficient flow of information and resource utilization.

ACKNOWLEDGMENT

Work described in this paper was funded by the RESCUE project at the California Institute for Telecommunications and Information Technology (Calit2), NSF award #0331690. The authors would like to thank Anthony Nwokafor, Karen Riggs-Saberton and other project researchers at the UCSD division of Calit2 (Gizmo, Rescue, and WIISARD projects). The authors would also like to acknowledge Maureen Curran's help with special thanks for her editorial review. Finally we acknowledge Art Botterell and Dr. Sassan Sheedvash for his review comments.

REFERENCES

[1] California Institute for Telecommunications and Information Technology (Calit2), http://www.calit2.net/, August 2008.
[2] ITR-RESCUE: Responding to Crises and Unexpected Events, http://www.itr-rescue.org/, May 2008.
[3] WIISARD, http://health.ucsd.edu/news/2003/10_23_WIISARD.html, Calit2, UCSD, May 2008.
[4] Responsphere, http://www.responsphere.org/, May 2008.
[5] Advanced Network Technologies Division Communication and Networking Technologies for Public Safety, National Institute of Standards and Technology (NIST).
[6] The Federal Response to Hurricane Katrina, Lessons Learned, February 2006, http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf, May 2008.
[7] http://www.fema.gov/media/archives/2007/061207.shtm, May 2008.
[8] Washington, DC, Area Sniper Investigation-Communications After-Action Report, SAFECOM, September 2003.
[9] Wireless Emergency Response Team (WERT), Final Report for the September 11, 2001 NEW York City World Trade Center Terrorist Attack, October 2001, http://www.wert-help.org/index.php, January 2008.
[10] National LambdaRail, http://www.nlr.net/, January 2008.
[11] Information and Communications Infrastructure, Virginia Tech, Confidential Presidential Working Paper: Telecommunications Working Group, August 17, 2007, Copyright Virginia Tech, 2007, http://www.vtnews.vt.edu/documents/2007-08-22_communications_infrastructure.pdf, January 2008.
[12] Disaster Preparedness and Service Using Communication Technology, 2005 Computer World Honors Case Study, http://www.cwhonors.org/laureates/government/20055426.pdf, January 2008.
[13] [1] Los Angeles earthquake chokes phone calls, not Twitter, http://alpha.news.yahoo.com/s/cnet/830110353100019129 4, Yahoo! News, August 2008.
[14] R.B. Dilmaghani, B.S. Manoj, B. Jafarian, R.R. Rao, "Performance Evaluation of RescueMesh: A metro-Scale Hybrid Wireless Network", *Proceedings* of WiMesh Workshop, IEEE Workshop on Wireless Mesh Networks, held in conjunction with SECON, Santa Clara, Sep. 2005.
[15] National Incident Management System (NIMS), http://www.nimsonline.com/, May 2008.
[16] CalMesh, http://calmesh.calit2.net, May 2008.
[17] GIZMO, http://gizmo.calit2.net, May 2008.
[18] iTAG, Wiisard project , "UCSD Tests Intelligent Triage, Other Technologies in San Diego Disaster Drill", http://www.calit2.net/, Nov. 2006.
[19] EDRAW software, http://www.edrawsoft.com/, July 2008.
[20] WebEOC Community Site, http://www.webeoc.com/webeoc_community/, July 2008.