A Wireless Mesh Infrastructure Deployment with Application for Emergency Scenarios

R. B. Dilmaghani, and R. R. Rao*
Department of Electrical and Computer Engineering
University of California, San Diego
* Director of UCSD Division of Calit2
La Jolla, CA 92093-0436
{rdilmaghani, and rrao}@ucsd.edu

ABSTRACT

When a disaster or emergency occurs, one of the most pressing needs is to establish a communication network for the first responders at the scene. Establishing and accessing a reliable communication infrastructure at a crisis site is crucial in order to have accurate and real-time exchange of information. Failure in the exchange of timely and crucial information or delay in allocating resources impedes early response efforts, potentially resulting in loss of life and additional economic impact. At a disaster site, the existing communication infrastructure may be damaged and therefore partially or totally unavailable; or, there may not have been previously existing infrastructure (as in the case of remote areas). A communication infrastructure within the context of emergency applications should be reliable, easily configurable, robust, interoperable in a heterogeneous environment with minimum interdependencies, and quickly deployable at low cost.

A disaster scene is a chaotic environment which requires a systematic approach to abstract the system, study the flow of information and collaboration among different disciplines and jurisdictions to facilitate response and recovery efforts. We have deployed the wireless mesh infrastructure in several drills at the university campus and in the city as part of the California Institute for Telecommunications and Information Technology (Calit2) NSF-funded RESCUE project (Responding to Crises and Unexpected Events). To evaluate network performance and identify the source(s) of bottleneck, we have captured the network traffic. The lessons learned from test bed evaluations of the network based on real-world scenarios can be applied to future applications to enhance the network design and performance.

KEYWORDS

Mesh network, Emergency communication deployment, Real scenario measurements, Field data, and Performance evaluation.

INTRODUCTION

A robust communication infrastructure must consistently detect and dynamically adapt to the changing network circumstances. A reliable communication technology is necessary to transmit information at all stages of an emergency including disaster mitigation, preparation, response, and recovery. Additionally needs to provision enough resources and interoperability with the existing devices and technologies in a distributed system. The infrastructure at disaster site needs to be easily configurable and quickly deployable at low cost. The system is preferred to be designed in a modular fashion which is easily upgradeable with the technology evolvement without the need to replace the entire system. This leads to an economic deployment solution which is affordable for different public and private agencies.

Interoperability in a heterogeneous system is required to enable collaboration among different organizations where different devices use different technologies. Different organizations, public or private, may resist deploying new technology for different reasons such as cost and culture. This might attribute to the cost of replacing or upgrading the existing technology or the cost of training people to learn how to use new technology. There is a natural resistance to the unknown and the new technology needs to show high performance before being deployed in a large scale. Another important factor is the amount of training that is required to deploy a new technology. The system should be user friendly, easy to configure with minimal training requirements.

This work presents different key factors in designing a robust communication infrastructure with applications for emergency response scenarios and describes the infrastructure deployed at several drills. Different organizations might loose communications because either the network becomes unavailable at some point in time, or different devices are not able to cooperate. Considering the scale and frequency of the recent disasters such as World Trade Center and Hurricane Katrina, there has been more attention paid to the continuous availability of a robust communication infrastructure to assure the best and fastest service. Design of such system affects emergency response and recovery in addition to planning. 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.

In the rest of this paper we present the technical challenges in design and deployment of new communication technology. This is followed by description of the Mesh test bed and the infrastructure deployed for a drill on the UCSD campus. We also present the results obtained from field data during the exercise, followed by an analytical discussion of network performance, and proposing solutions to improve network performance and prevent bottlenecks in the network. Finally we conclude this chapter by a brief review of concerns surrounding rapid growth of communication technology and the Internet.

Related Work

In most disaster scenarios in the past, different organizations have not been able to communicate efficiently with each other throughout the network (Morentz, 1994). The Fire department did not hear warnings issued by the Police department asking for evacuation of all people in the area of the second building (Slack et al., 2006). This incident confirms the necessity for a technology that is able to work with heterogeneous devices to send and receive messages across different systems. Some of the frequently observed, serious outcomes of disasters are loss of life, health issues, social effects such as looting, or the impacts on economy such as gas price increase and loss of the tourism industry (NSF, Katrina 2006). The architecture should support distributed command and control systems to enable different first responders including police, firefighters, and medical teams to work remotely and collaborate, which was missing at the 9/11 disaster (Turoff et al., 2004).

In (Raniwala et al., 2006), the authors describe Hyacinth architecture which is a multi-channel mesh network where non-overlapping radio channels are explored to improve the available bandwidth limitations. They describe the channel assignment and routing in Hyacinth mesh architecture in (Raniwala et al., 2005). In (Das. et al., 2006) the authors study the effect of multi-way interference in mesh network caused by simultaneous transmission of different nodes.

Lannone IEEE et al. (2005) present Mesh-DV routing protocol for wireless mesh networks and Lannone et al. (2006) discuss the importance of a cross-layer routing protocol and the gain enhancement in wireless mesh network is studied. In (Eriksson et al., 2006) real measurement results are presented studying the feasibility of mesh network for all-wireless offices. Another work by (Bianchi et al., 2006) presents measurements over an outdoor wireless mesh network. In (Pirzada et al., 2006) the authors address performance evaluation of AODV for multi-radio mesh network considering the limited capacity and scalability due to interference. The performance behavior related to the handoff between access points in an 802.11-based mesh infrastructure (iMesh) for community applications is presented in (Navda et al., 2005).

We address the overall problem with existing approaches to communication infrastructures to resolve issues such as interdependency, unreliability, interoperability, possibility of network unavailability due to partitioning (Klapwijk et al., 2006), efficient network resource allocation, and the ability of organizations to adopt new technology. Some of these shortcomings have been the main cause of existing communication infrastructure failure at many incidents (Goel et al., 2004). This is why the problem of designing a robust communication technology is becoming crucial. Our work focuses on the challenges of future communication technologies with emergency applications (Dilmaghani et al., 2005 and 2007). Wireless mesh networks have been used as a solution to extend wireless coverage in many cities (MIT Roofnet) (Bay area) (Champaigne-Urbana)(WiFi News)(Seattle)(Wireless Leiden), we investigate the particular application and challenges for emergency and crisis scenarios.

Technical Challenges In Design and deployment of new communication technology

To design a robust communication infrastructure, there are a large number of technical factors to be considered. Below we address some of the factors that have been the cause of failure in many previous disasters. Later, we will see how the deployment of a mesh network will meet the specific requirements of a robust communication infrastructure at a disaster site.

In the design of future communication technology, we need to reduce possible interdependencies to minimize the cost of loss (Zimmerman, R., 2001). This makes the system more robust and resilient to failures in other components of a communication system. For example, high dependency of communication infrastructure on power supply has been one main reason for cellular failure in many scenarios. There needs to be a stand-alone, emergency power source for each base station so that the system can survive a land line failure to provide uninterrupted service.

When a large scale disaster strikes, first responders are sent to the site immediately. Once the most pressing needs of the disaster are addressed, the next step is to establish a command and control center. To accommodate this need, a communication infrastructure is required to provide decision makers with data and information from the site to receive digital maps, data, and feedback from personnel in the field in a timely manner. Also, it should be able to provide a reliable connection with enough resources for a distributed command and control center (Turoff et al., 2004). Details on the future of command and control for disaster response along with the theory can be found in (Rosen et al., 2002).

While there are common requirements for all communications during emergency response (e.g., integrity, availability and reliability, quick reconfiguration, and interoperability), the other needs such as confidentiality and different quality of service depends upon the nature of disaster and the specific application. It is very challenging to design a system that accommodates all of these needs. For example, terrorist attacks or campus shootings require higher levels of privacy and security. Telemedicine applications may need to transfer interactive real-time data over a secure network. Transferring data, audio, and video require special bandwidth, different quality of service, and high network security to meet Health Insurance Portability and Accountability Act (HIPAA) requirements at low cost. There are practical challenges in a new technology deployment that is relevant and very important to be addressed when deploying a system at first stage. A communication infrastructure should have the capability of operating in a highly distributed architecture. The system should be designed in a modular fashion that is easily upgradeable with the technology evolvement without the need to replace the entire system. This leads to an economic deployment solution which is affordable for different public and private agencies. Furthermore, it is desirable to provision redundancy for an effective network management based on the trade-off between reliability and cost.

The communication infrastructure needs to be reliable and continuous, and it must work with existing responder organizations’ devices if necessary. Users may have different devices such as laptops, PDAs (Personal Digital Assistants), or cell phones, which may work with different network technologies such as WLAN (Wireless Local Area Network), Wi-Max (Worldwide Interoperability for Microwave Access), WWAN (Wireless Wide Area Network), satellite, or wired networks. Additionally, a communication network needs to be easily configurable and quickly deployable at low cost.

Interoperability of heterogeneous systems is required to enable collaboration among different organizations and across various departments of the same organization (Gerst et al., 2005). At a disaster site, different response organizations show up with a variety of devices using different technologies. Since there is not one single standard communication technology with application for emergency response and different organizations use different available technologies, we need to plan and provision interoperability among different devices in a heterogeneous environment. This has been addressed in our Mesh test bed, where wireless mesh nodes are capable of interconnecting different technologies using different interface cards. Regardless of the technology that each individual system uses, different systems are uniformly connected to the relaying mesh nodes and are able to exchange data. Local connectivity is more urgent as failure to hear others’ communication at disaster site has caused loss of life in the past.

Cross-Tier diversity effect is inevitable in a heterogeneous environment. Ideally different devices operating over different physical layers should not interfere. Real measurements over the network show that the network performance and application response time in a heterogeneous environment are not merely affected by one source.

This has been observed in the drills conducted by San Diego County in addition to the comments after Katrina and similar disasters (Wirbel, 06).

In a heterogeneous environment where all users share the same network resources, recovery mechanisms from congested network is not trivial. While network congestion, resource allocation and meeting minimum quality of service are resolved in the established and mature standard such as 802.11, they continue to be highly challenging problems where all different devices and technologies interfere in a non-traditional model. IEEE 802.11b medium access protocol resolves the problem of interference by only allowing nodes to transmit when there is no other transmitting node within the interfering distance using carrier sense Distributed Coordination Function (DCF). DCF function employs Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA) or Collision Detection (CD) (Walke et al. 2006). Regardless of the technology that each individual system uses, different systems are uniformly connected to the relaying mesh nodes and will be able to exchange data. Mesh boxes with multiple interface cards provision interoperability in a heterogeneous environment as different devices are able to uniformly connect to the network through the appropriate interface cards.

Applying test bed captured network traces is a cost-effective tool to re-configure the network topology for a more efficient network performance and dynamic adaptation. It enables network designer to repeat the real world scenarios in a simulation environment to re-configure and evaluate alternative topologies to recover from component failures or to meet QoS requirements by selectively turning nodes on/off.

Network performance can be optimized by tuning the relevant traffic parameters based on real measurements. Traffic management and resource allocation is achieved by changing network topology (turning nodes on or off) and selectively allowing particular types of traffic. This allows the network to adapt to the critical conditions that are at the core of the infrastructure. We modify the network load at the operating network, partition the functionality of the network over the components of the infrastructure, and re-schedule activities considering the constraints.

Maintaining the network connectivity after initial setup is another challenge as the network load gradually increases during recovery stage. Mesh network provides reliability in a sense that there are always alternate routes in case of a component failure (node or link). Based on real measurements we find the conditions and topologies that facilitate establishing a reliable network at disaster site to speedup recovery, manage traffic, and allocate network resources towards an efficient and reliable network.

Another important point to consider is the level of knowledge of future operators/users of the system and the amount of training that is required to deploy a new technology (Zimmerman, 2006). The system should be user friendly, easy to configure with minimal training requirements while maintaining security and privacy in specific applications as required. Finally, it is significant to have the new technology fully tested before final deployment.

Communication Infrastructure at disaster site

A reliable robust communication technology is necessary to transmit information at all stages of an emergency situation to handle disasters more efficiently. This includes disaster mitigation, preparation, response, and recovery. Emergency response and recovery have a more specific need for quick deployment and easy reconfiguration of a communication infrastructure. These are more time-sensitive applications, while mitigation and preparation usually allow a longer planning time.

At a disaster site, there may not be any communication infrastructure available. A mesh network infrastructure can be deployed quickly to provide a network for local communication. If there is any kind of Wide Area Network (WAN) or communication technology available, the local network at a disaster site can communicate to the outside world through this link. The infrastructure consists of three-tiers considering the connectivity of the local mesh network to Internet: the first tier-level consists of clients using different devices and technologies such as PDA, laptop and iTAGs (iTAG). The second level tier consists of wireless mesh nodes and the third layer is the backhaul link(s) provides connectivity to Internet. The mesh network is a decentralized architecture is resilient to the failure of nodes or links as there are alternate paths to take if any one link fails. Each node in the network transmits to the neighboring nodes therefore each node is connected to several nodes. In case of a hardware failure or loss of the line of sight (LoS), the neighboring node can fine another route. 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. In this architecture nodes act as repeaters to transfer data from the source to the far destinations. The architecture is easily expandable by adding more nodes. In this architecture, only gateways are connected through wireless or wired long haul links, which is considered advantageous, as only gateways need to be configured/re-configured and all the wireless access nodes will automatically form a network as long as there is a line of sight among them. It is important to notice that the network throughput drops if the maximum number of hops exceeds a limit therefore depending on the terrain and signal strength, we configure another gateway for a given number of access nodes (or repeaters). The wireless mesh infrastructure is quickly deployable with minimal configuration and has multiple interface cards to communicate in a heterogeneous environment with different technologies.

We proposed a Hybrid Wireless Mesh Network (HWMN) for emergency situations which is a non-expensive deployable infrastructure for the use of free unlicensed spectrum and IEEE 802.11b/a/g off-the-shelf devices in (Dilmaghani et al. 2005). It is different from other mesh deployments in cities because of its application for emergency scenarios, portability, flexible infrastructure, and independence from power lines by being battery operated.

The wireless mesh nodes in our test bed use Soekris net4521 boards running on minimal Debian Etch Linux distribution with Linux-2.6.18 kernel. Modifications were made to the Linux kernel bridging code and the brtcl application to enable additional functionalities for bridging and spanning Tree protocol (STP) (CalMesh) (brtcl).

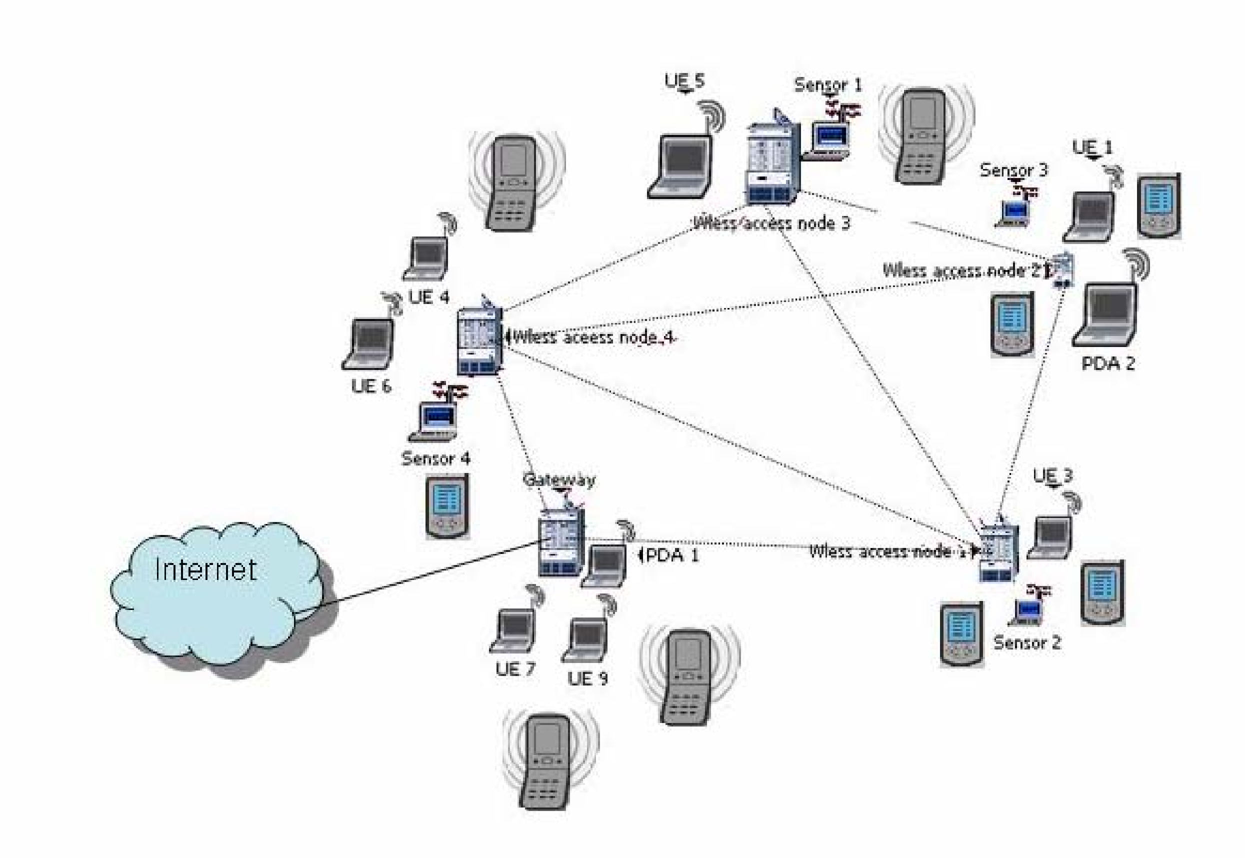

Figure 1. Mesh test bed deployment at a disaster site

We have deployed a 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) (Rescue project, Calit2), and in exercises of the San Diego Metropolitan Medical Strike Team (MMST). San Diego's MMST, which coordinates the city and county's medical response to a disaster, staged a drill based on a scenario involving a terrorist attack and gas spill at the Calit2 (California Institute for Telecommunications and Information Technology) building on the UCSD campus. Figure 1 shows the infrastructure of the mesh network deployed at the disaster scene during this exercise on campus which provided connectivity to the command center and throughout the disaster site. The site included Atkinson hall and a nearby parking structure mainly. The test bed consists of a gateway which was connected to the

Internet through a wired backhaul link, four wireless access points, sensors and iTAGs (handheld electronic devices that patients are equipped with to transfer vital information over the network) and laptop clients. Based on the total geographic distribution of this exercise and the coverage of the nodes, it turned out that one gateway and four nodes provide a reasonably well coverage. In larger scale scenarios there is more than one gateway to provide reliability and redundancy. Any access point can quickly be configured as a gateway when required.

The importance of developing a robust communication infrastructure to support transmission of critical health related data to on-site medical response organizations has initiated considerable investments (Popovich et al., 2002). We have captured traffic data using opnet capture agent during this drill to develop network performance studies and improve network resource usage for similar scenarios (Opnet).

At a disaster site, all different response organizations need to communicate to the decision-makers off-site including the Emergency Operations Center (EOC), occasionally transferring large amounts of data such as digital maps or video information. We need to analyze the large amount of data obtained during the drill to ensure that the mesh network infrastructure is capable of providing the best service possible for both data and voice applications in a timely manner such that network congestion is avoided. We will discuss some of these findings in next section. System performance analysis enables us to determine the level of coverage, efficient network management, and resource allocation. Additionally, it provides us with a method of collecting and measuring data on crowd behavior dynamics, mobility and traffic patterns in emergency scenarios for later analysis by engineers, social scientists and computer vision researchers.

performance evaluation and analytical discussion

In this section we present the results obtained from the field data conducted over the Mesh test bed during the drill. The opnet capture agent was installed on a laptop which was in capture mode at different locations during the exercise (Opnet). The gateway was directly connected to the Internet via a wired network. For this particular work, we study the network behavior within the local mesh network.

Data has been captured at several intervals during the drill. The total capture time is 456 seconds for this particular set of data. The overall performance was similar among several data traces. 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. All network data is sent over Transport Control Protocol (TCP) which retransmits packets if they are lost or experience a long delay (retransmission timeout occurs or 3 duplicate ACKs received). This leads to a longer application response time. Based on this measurement, server and node 2 are communicating over the network by sending a large number of small packets for RSRB messages (Remote Source Route Bridging) creating overhead (RSRB). In this scenario network resources can be utilized by sending fewer larger application messages. Another source of bottleneck is the large number of retransmissions over the network. This may occur for two main reasons: either the network is heavily congested, or there exist some error-prone links. 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. Network throughput statistic includes all application data and network protocol overhead which is similar for all mesh nodes except node 2. Figure 2 shows the amount of application data transmitted between the server and mesh node which is similar for all nodes as they run similar applications. Later in this paper we see the amount of overhead and the fact that the network data is similar between server and all nodes except node 2.

Analyzing the results identifies bottlenecks and potential bottlenecks in the network. We see the nodes in which

The main causes for the bottlenecks seem to be protocol overhead, chattiness, retransmission, and very occasionally out-of-sequence packets. It is interesting to notice that in the set of data collected in this drill, TCP windowing and Nagle’s algorithm are not causing any bottlenecks.

Figure 3 shows the network throughput transmitted between the server and all mesh nodes except node 2. Network throughput statistic includes all application data and network protocol overhead.

Figure 4 show the network throughput from server to node 2. Figure 5 shows the number of retransmission each node experiences. We see that 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 (a large number of small control packets, about 42% of total packets; RSRB messages).

Finally figure 6 shows the total amount of application and network data exchanged between server and mesh nodes. The network behaved differently between server and node 2 because of an error-prone link which was verified by the signal strength measured during the drill.

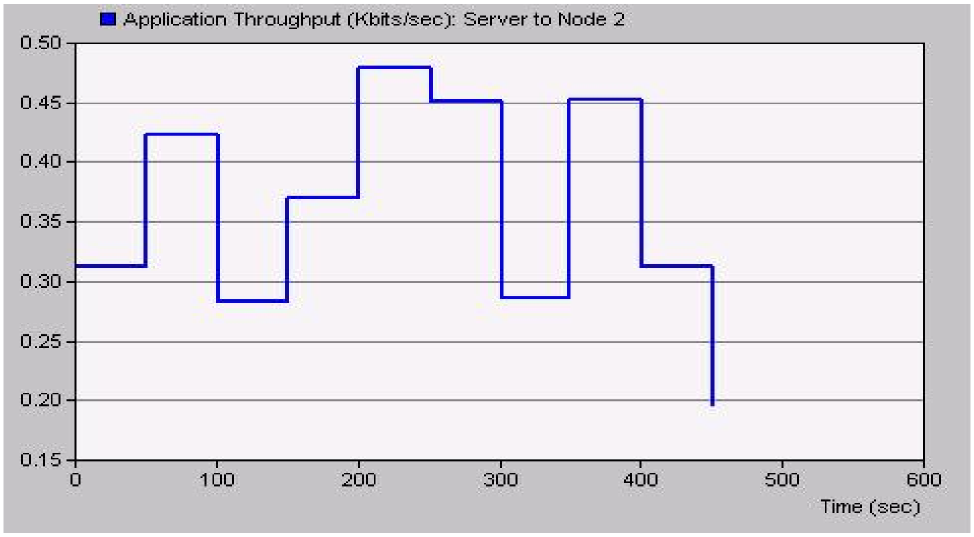

Figure 2. Application throughput from server to a mesh access node

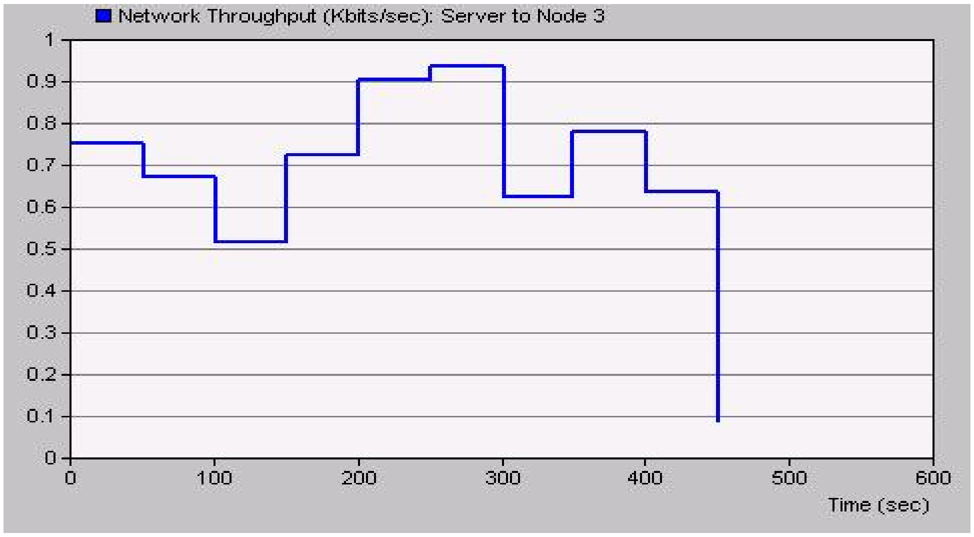

Figure 3. Network throughput from server to a mesh access node

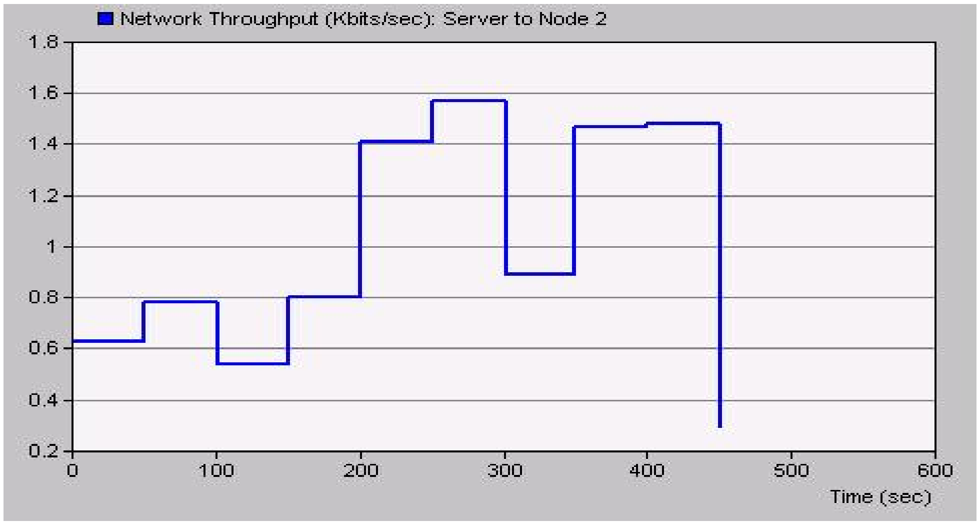

Figure 4. Network throughput from server to a mesh access node 2

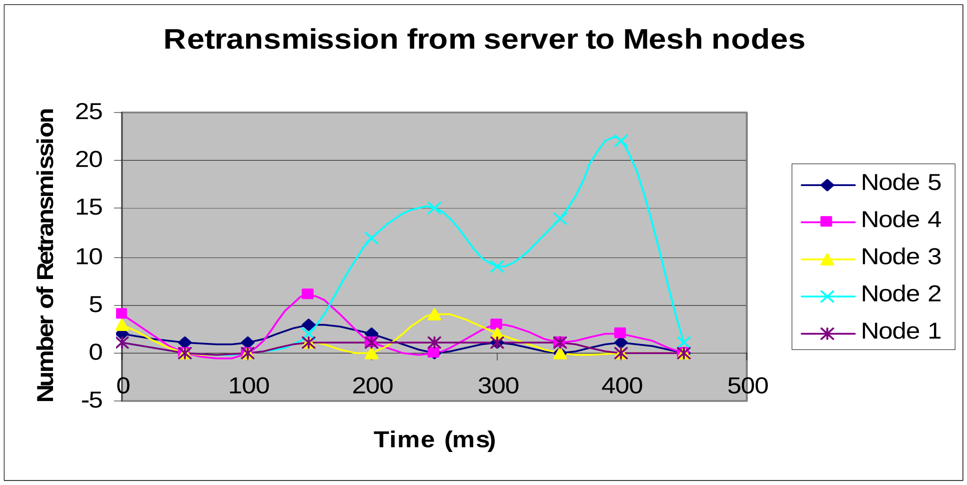

Figure 5. Retransmission from server to the mesh access nodes

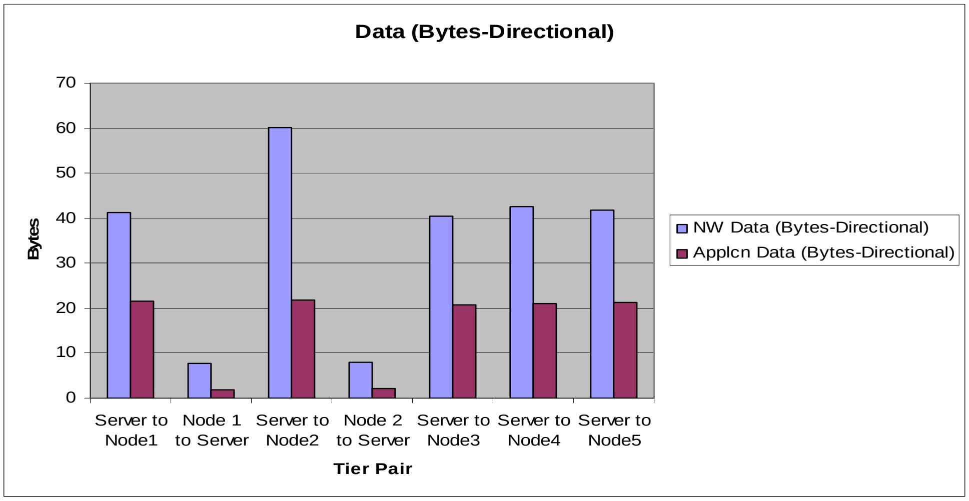

Figure 6. Application and Network Data from server to the mesh nodes (Bytes-Directional)

In disaster scenarios where responders communicate different types of data, video, digital maps, and voice over the same network, different types of services should be defined to meet each application needs specifically. Because of the QoS (Quality of Service) requirements of voice data, this type of traffic service prioritizes voice users over data users sending different types of data over the same network. Clearly the voice users should be guaranteed with a minimum amount of bandwidth at all times; therefore data users may experience a longer delay depending on the amount of Constant Bit Rate (CBR) traffic over the network. In this case, data users are provided by Available Bit Rate (ABR) service which means the available bandwidth is divided among the users, and there will not be any limits on the number of users in the network. Consequently the response time and end-to-end delay for data users might be increased as they can access a portion of bandwidth when there is high priority (or delay sensitive) traffic over the network.

Discussion

We have observed interference caused by cellular phones around wireless access nodes during the drill as most people, including responders, victims and observers, usually carry at least one. One possible problem with radio communications is the traffic abbreviation which might be crucial in some cases. For the above reason, some first responders may prefer face-to-face communications which in turn brings along its shortcomings such as the distance they need to walk or drive to reach the person, the delay, etc. This is a work in progress where we are investigating the flow of information among different response organizations. First responders need to exchange accurate information in a timely manner for efficient incident management. Delay in communication or resource allocation slows down the response and recovery efforts. At a crisis site, the real-time exchange of information over a shared reliable communication infrastructure plays an important role in increasing situational awareness, span of control, scalability, and efficiency of response. Different organizations and jurisdictions need to share the information and resources during the response. When an emergency occurs, depending on the type, there are different procedures to follow. Incident command center and MMST are there to ensure cooperation between different response organizations and facilitate the exchange of information. In scenarios involving bombs, chemicals, etc., the affected area (hot zone) needs to be cleared first by specialized organizations before other first responders can enter the site. Other scenarios such as wild fires or hurricanes are different in this regard. Accordingly, there is different information required by each organization. A shared infrastructure can help to distribute information and exchange data, images, etc. in a timely manner for a faster response and recovery efforts.

Conclusion

Designing a robust communications infrastructure for emergency applications is a demanding effort. Such infrastructure should allow for reliable communication among different response organizations over a distributed command and control infrastructure. Additionally, it should facilitate the distribution of warning and alert messages to a large number of users in a heterogeneous environment. The new technology should be cost effective with minimum training requirements to efficiently operate the system to allow wide deployment. The well-known system dependency on power as the cause of many failures has been addressed by using battery operated wireless access nodes for emergency situations and having a back-up power supply for base stations. We addressed the problem of interoperability by deploying wireless Ad hoc mesh networking nodes with multiple interfaces to facilitate collaboration amongst different systems in a heterogeneous environment.

It is very important to consider social challenges in deploying new technology including, cost and culture. Traditionally, new technologies are not as readily adapted as they should be. For example, VoIP handsets are not as common as traditional handsets to talk to work partners and family in case of an emergency. The high quality of voice over landlines and cellular phones is not matched by VoIP technology; however, when there is a limit on network resources, an established alternative plan for emergency communications will help to speed up rescue and response efforts considerably. Additional design issues are yet to be addressed in the development of a more robust communication infrastructure. Ultimately, all these factors facilitate a better service for the flow of information and data with different qualities of service depending on the requirements of each application with minimum interference.

Extracting real scenario results over different network infrastructures is a valuable analysis tool which can ultimately help improve network survivability in emergency situations. We have presented the results directly extracted from field data measurements during a drill on the UCSD campus. We noticed that in this particular application, we should send fewer large packets to prevent bottlenecks across the network. Finally, we addressed the importance of a secure authentication mechanism in a hybrid communication infrastructure which we believe is inevitable in near future.

ACKNOWLEDGMENTS

Work described in this paper was funded by the RESCUE projects at UCSD, NSF award number #0331690. The authors would like to thank project researchers at UCSD division of Calit2 for the group discussions with special thanks to Maureen C. Curran for help with readability.

REFERENCES

1. R.B. Dilmaghani, B.S. Manoj, B. Jafarian, R.R. Rao (2005), 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.
2. S. Goel,S. Belardo, L. Iwan (2004), A Resilient Network that Can Operate Under Duress: To Support Communication between Government Agencies during Crisis Situations, *Proceedings of the 37th Hawaii International Conference on System Sciences*.
3. ITR-RESCUE: Responding to Crises and Unexpected Events, http://www.itr-rescue.org/, Jan. 2008.
4. CalMesh, http://calmesh.calit2.net/, Jan. 2008.
5. RSRB Overhead Information [Token Ring]- Cisco Systems, http://www.cisco.com/en/US/tech/tk331/tk660/technologies_tech_note09186a008009472b.shtml#intro, Sep. 2006.
6. G. Slack (2006), Bringing Firefighters Back Alive with Smart Technology, Research at Berkeley Articles, *UCB Research*, http://research.chance.berkeley.edu/page.cfm?id=11&aid=28.
7. P. Klapwijk,L. Rothkrantz (2006), Topology based infrastructure for crisis situations, *Proceedings of the 3rd International ISCRAM Conferenc*.
8. J.W. Morentz (1994), Can we talk, *Proceedings of the Fifth NI/USR Town Meeting and Information Systems Conference*, Rockville, Maryland, Natural Hazards library, University of Colorado, Boulder, http://ibs.colorado.edu/hazards/Library/, Jan. 2008.
9. R. B. Dilmaghani (2003), An Investigation to Fast Modular Multiplication and Exponentiation Techniques to Speed-up RSA-Like Crypto Systems, *MS Thesis*, Department of Electrical and Computer Engineering, Colorado State University.
10. M. L. Popovich, J.M. Henderson, J. Stinn (2002), Information technology in the Age of Emergency Public Health Response, *IEEE Engineering in Medicine and Biology Magazine*, volume 5.
11. J. Rosen, E. Grigg, J. Lanier, S. McGrath, et al. (2002), The Future of Command and Control for Disaster Response, *IEEE Engineering in Medicine and Biology Magazine*, volume 5.
12. Opnet (2007), Making Networks and Applications Perform, http://www.opnet.com/services/university,
13. H. Zimmerman (2006), Availability of Technologies versus Capabilities of Users, *Proceedings of the 3rd International ISCRAM Conference*.
14. R. Zimmerman (2001), Social Implications of Infrastructure Network Interactions, *Journal of Urban Technology*, Volume 8, Number 3.
15. M. Gerst, R. Bunduchi, R. Williams (2005), Social Shaping and Standardization: A case study from Auto Industry, *Proceedings of the 38th Hawaii International Conference on System Sciences*.
16. M. Turoff, M. Chumer, B. Van de Walle, X. Yao (2004), The Design of a Dynamic Emergency Response Management Information System (DERMIS), *Journal of Information Technology Theory and Application (JITTA)*, Volume 5, Number 4.

17. L. Wirbel (2006), Authorities Blamed for Communications Network Failure under Katrina’a Attack, http://www.globalsecurity.org/org/news/2005/050905-comm-failure.htm.
18. National Science Foundation, Science Daily (2006): Remembering Katrina: Studies Look At Multiple Facets Of The Hurricane's Devastation, http://www.sciencedaily.com/releases/2006/09/060901163625.htm.
19. Hurricane Katrina Recovery Information, Sep. 2005, http://www.tbr.org/katrina/kat_090705.htm, Sep. 2006.
20. Grand Challenges for Disaster Reduction, National Science and Technology Council, Committee on environmental and Natural Resources, http://www.sdr.gov/SDRGrandChallengesforDisasterReduction.pdf, Aug. 2006.
21. California Institute for Telecommunications and Information Technology (Calit2), http://www.calit2.net/, Jan. 2008.
22. iTAG, WIISARD project , UCSD Tests Intelligent Triage, Other Technologies in San Diego Disaster Drill, http://www.calit2.net/, Jan. 2008.
23. A. Raniwala, T. Chiueh (2006), Architecting a High-Capacity Last-Mile Wireless Mesh Network, http://www.cs.sunysb.edu/~raniwala/hyacinth-poster.pdf.
24. A. Raniwala, T. Chiueh (2005), Architecture and Algorithm for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network, *Proceedings of IEEE Infocom 2005*, http://www.cs.sunysb.edu/~raniwala/.
25. S. Das, D. Koutsonikolas, Y.C. Hu, D. Peroulis (2006), Characterizing Multi-Way Interference in wireless Mesh Networks, *ACM International Workshop on Wireless Network Test beds, Experimental evaluation and CHaracterization ACM WinTECH*.
26. L. Iannone, S. Fdida (2005), MeshDV: A Diastance Vector mobility-tolerant routing protocol for Wireless Mesh networks, *IEEE ICPS Workshop on Multi-hop Ad hoc Networks: from theory to reality (REALMAN).* Santorini (Greece), http://www-rp.lip6.fr/~iannone/, Nov. 2006.
27. L. Iannone, K. Kabassanov, S. Fdida (2006), The real Gain of Cross-Layer Routing in Wireless Mesh Networks, *Proceedings of Second International Workshop on Multi-hop Ad Hoc Networks: from Theory to Reality (ACM/SIGMOBILE RealMan'06)*. Florence (Italy).
28. J. Eriksson, S. Agarwal, P. Bahl, J. Padhye (2006), Feasibility Study of Mesh Networks for All-Wireless Offices, *International conference on mobile Systems, applications, and services*, ACM MobiSys.
29. G. Bianchi, F. Formisano, D. Giustiniano (2006), 802.11b/g Link Level Measurements for an Outdoor Wireless Campus Network, *Proceedings of the 2006 IEEE International Symposium on a World of Wireless, Mobile, and Multimedia (WoWMoM).*
30. A.A. Pirzada, M. Portmann, J. Idulska (2006), Evaluation of Multi-Radio Extensions to AODV for Wireless Mesh Networks, *Proceedings of the international workshop on Mobility management and Wireless access ACM MobiWac*.
31. V. Navda, A. Kashyap, S.R. das (2005), Design and Evaluation of iMesh: an Infrastructure-mode Wireless Mesh Network, *Proceedings of the 2005 IEEE International Symposium on a World of Wireless, Mobile, and Multimedia (WoWMoM).*
32. B. H. Walke, S. Mangold, L. Berlemann, IEEE 802 Wireless Systems: Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence, John Wiley & Sons, Ltd, 2006.
33. R.B. Dilmaghani, R.R. Rao (2007), Hybrid Communication Infrastructure and Social Implications for Disaster Management, *Proceedings of the 40th Hawaii International Conference on System Sciences*.
34. MIT Roofnet, http://pdos.csail.mit.edu/roofnet/doku.php, Nov. 2006.
35. Bay Area Wireless Users Group, http://www.bawug.org, Nov. 2006.
36. Champaigne-Urbana Community Wireless Network, http://www.cuwireless.net, Nov. 2006.
37. WiFi Mesh News, http://wi-fi-mesh-news.newslib.com/feed.xml, Nov. 2006.
38. Seattle wireless, http://www.seattlewireless.net, Nov. 2006.
39. Wireless leiden, http://www.wirelessleiden.nl, Nov. 2006.
40. brtcl, FAQ, http://openvpn.net/index.php/documentation/faq.html, Jan. 2008.