Hybrid Wireless Mesh Network with Application to Emergency Scenarios

Raheleh B. Dilmaghani
University of California, San Diego, La Jolla, USA
rdilmaghani@ucsd.edu

Ramesh R. Rao
University of California, San Diego, La Jolla, USA
rrao@ucsd.edu

Abstract— **Establishing and accessing a reliable communication infrastructure at crisis site is a challenging research problem. Failure in communication infrastructure and information exchange impedes the early response efforts resulting in huge loss of lives and economical impacts. In this paper, we present the results taken over the wireless mesh network that had been deployed to provide first responders with an infrastructure for local communication on campus during the drill. Additionally the network was connected to the outside world through a wired backhaul. This infrastructure is quickly deployable, easily configurable and interoperable in a heterogeneous environment with minimum interdependencies. We present the measurements taken directly over the network by capturing operational network traces to evaluate network performance and identify the source(s) of bottleneck to improve performance and network resource usage for future deployments.**

Index Terms— **Mesh network, Emergency communication deployment, Real scenario measurements, Field data and Performance evaluation**

I. Introduction

This work studies different key factors in designing a robust communication infrastructure with applications for emergency response situations. A robust communication infrastructure must consistently detect and dynamically adapt to the changing network circumstances including different devices using various technologies joining and leaving the network. Additionally, the network should support distributed command and control systems to enable different first responders exchange information and collaborate. In most disaster scenarios such as 9/11, different organizations have not been able to communicate with each other [8] [20]. This is 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. Based on National Science and Technology Council Committee of environmental and Natural Resources, "a sustained emphasis on risk mitigation and public/private partnerships is essential throughout all aspects and at all levels of the community" [23].

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 [21] [22]. From technology and business perspectives, when there is a power failure, most markets are affected with an inevitable impact on the economy of the country as reported aftermath of blackout incidents recently.

There are many references about the lack of communication between Police and Fire department at the 9/11 disaster. 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 [5]. This incident confirms the necessity for a technology that is able to work with heterogeneous devices to send and receive messages across different systems. A robust communication infrastructure provides connectivity in a heterogeneous environment. We address the overall communication problem with existing infrastructures by deploying a mesh network to resolve issues such as interdependency, unreliability, and interoperability. Some of these shortcomings have been the main cause of existing communication infrastructure failure at many incidents [2]. This is why the problem of designing a robust communication technology is becoming crucial.

© 2008 ACADEMY PUBLISHER

The organization of the rest of this paper is as follows: section III presents the technical challenges in design and development of new technology, while section IV presents some of social implications of applying these new technologies. In section V we present the special requirements of a robust communication infrastructure at a disaster site by describing the communication infrastructure deployed over a drill on the UCSD campus. Section VI presents the results from measurements during the exercise, followed by an analytical discussion of network performance, and proposing solutions to improve network performance. Section VII provides a brief review of concerns surrounding secure communication and privacy issues with the rapid growth of communication technology and the Internet. Section VIII concludes this paper.

II. Related work

Recently Wireless Mesh Networks (WMNs) have become very popular research area for the use of unlicensed spectrum and low cost of IEEE 802.11b/a/g-based off-the-shelf devices. The mesh architecture provides easy configuration and high reliability by choosing alternative routes in case of link or node failure and provides an economic solution to extend network coverage by eliminating the need for high cost maintenance. Wireless mesh networks have been used as a solution to extend wireless coverage in many cities [36] [37] [38-41].

In [6] authors present a mobile Ad hoc network (MANET) where the nodes communicate via a blackboard structure. The humans and sensors provide information as data input to the nodes in this network. They have implemented their idea as a proof of concept to provide the users with the appropriate information based on data input.

In [27], 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 and show the network performance improvement obtained using two network interface cards versus one. They describe the channel assignment and routing in Hyacinth mesh architecture in [26]. In [28] the authors study the effect of multi-way interference in mesh network caused by simultaneous transmission of different nodes.

In [29], the authors present Mesh-DV routing protocol for wireless mesh networks and in [30] the importance of a cross-layer routing protocol and the gain enhancement in wireless mesh network is studied. In [31] real measurement results are presented studying the feasibility of mesh network for all-wireless offices. Another work by [32] presents measurements over an outdoor wireless mesh network. In [33] 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 [34].

We proposed a Hybrid Wireless Mesh Network (HWMN) for emergency situations which is a low-cost widely deployable infrastructure for the use of free unlicensed spectrum and IEEE 802.11b/a/g off-the-shelf devices in [1] [35]. This mesh network has been deployed with the particular application for emergency and crisis scenarios. In this paper we present the real network performance measurements obtained during a recent drill on campus to improve performance for the similar scenarios in future deployments.

III. Technical challenges in design and deployment of new technology

To design a robust communication infrastructure, there are a large number of technical factors to be considered. In the design of future communication technology, we need to reduce possible interdependencies to improve reliability and minimize the cost of loss [17]. 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 [19]. Details on the future of command and control for disaster response along with the theory can be found in [12].

The communication infrastructure needs to be reliable and interoperable with the existing responder organizations' devices in a distributed system. Additionally, it needs to be easily configurable and quickly deployable at low cost. 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. We have identified the following objectives in a chaotic deployment and provide the results and solutions in progress:

(1) Cross-Tier diversity effect

Real measurements over the network confirm the fact that the application performance and delay in a network with shared resources is not caused merely by one source. This has been experienced in the drills conducted in San Diego County and by people at Katrina [3][20]. This

© 2008 ACADEMY PUBLISHER

effect can be moderated by allocating network resources more efficiently based on real-life scenarios and measurements.

(2) Interoperability and network congestion

Interoperability in a heterogeneous system is required to enable collaboration among different organizations where different devices use different technologies such as WLAN (Wireless Local Area Network), Wi-Max (Worldwide Interoperability for Microwave Access), WWAN (Wireless Wide Area Network). In a chaotic environment all different systems share the same network resources, i.e. they communicate over the same network, share network media and resources therefore 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. During our measurements we noticed that when a cell phone is really close to the transmitting/receiving node, the throughput is considerably reduced [3]. Since there is not a single standard communication technology today we need to plan and provision interoperability capabilities in heterogeneous systems [18]. 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 as presented in section V. 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.

(3) Adapt and reconfigure network topology

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.

(4) Traffic management

Based on real measurements obtained in several drills and deployments, we selectively allow specific types of traffic depending on the application requirements to regulate traffic and transfer the most urgent type of traffic with a best effort service. 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.

(5) Reliability and Maintain network connectivity

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 scenarios 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.

IV. Social challenges in deployment of new technology

Emergency planning and response/recovery approaches to a disaster vary from one incident to the next depending on the scale and the nature of each disaster. The degree of urbanization or the geographic spread may require different actions for a specific respond. The degree of urbanization is determined by the number of people affected by the disaster, but the handling of these incidents is different from those that are spread over a wider non-urban area. Wild fires are a good example of a disaster that affect a very wide area such as national parks at a first stage, however if it does not get under control in a timely manner, it may eventually lead to a larger scale disaster and impact more people.

Another key factor in planning the emergency response is whether the disaster has been predicted or not. With 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, or in the case of the wildfire example above, before it spreads to populated areas. In designing and developing warning systems, the age and physical ability of those affected and their preference for methods of receiving information should be considered [15]. This may vary, depending on the time of day or the level of knowledge that the affected people have about the incident. The content of disseminated warnings should be very clear in explaining the nature of disaster and providing sufficient information for the recipient to avoid the disaster or reduce losses. When planning for emergency response, we should keep in mind that people may not follow instructions exactly, or may not evacuate to safe areas even if ordered to do so for different reasons such as family, belongings, and pets, or they may simply not trust the accuracy or the source of the warning.

Different organizations, public or private, may resist deploying new technology for different reasons such as cost and culture [7]. This might attribute to the cost of replacing/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.

There are additional cultural and traditional factors against using some technologies versus others. For example, although cell phones are widely used in a disaster by people to contact friends and family, it is not that common to communicate with work colleagues in an emergency situation. Another important factor 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 [14]. 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. These

© 2008 ACADEMY PUBLISHER

are some of the social implications that need to be addressed within the context of communication technology.

V. 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. 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. This wireless mesh infrastructure is quickly deployable with minimal configuration and has multiple interface cards to communicate in a heterogeneous environment with different technologies. In this architecture, only gateways are connected through wireless long haul links, which is considered advantageous, as fewer nodes need to be configured/re-configured.

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. 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 as long as there is a line of sight between nodes. These wireless access nodes allow users to communicate with each other when there is no wired configuration. Figure 1 shows the infrastructure of the mesh network deployed at a disaster scene which provides connectivity to the command center and throughout the disaster site.

We have deployed this 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). Recently, 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. A local wireless mesh infrastructure was established at the site to provide connectivity at the site, while the gateway was connected to the Internet through a backhaul link. Sensors and wireless patient tracking devices communicated data over this reliable network locally and to the Internet. Patients were tagged with wireless devices connecting them to Internet through the mesh nodes, communicating their medical status, treatment record, and vital information to medical personnel at the site of the disaster. We have captured traffic data during this drill to develop network performance studies and improve network resource usage for similar scenarios. This is a multi-tier architecture and the number of tiers varies depending on the location and the time. Wireless mesh nodes, laptops, medical record PDAs, patient tags (iTAG) [25], and cameras form the tiers of the network.

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 have analyzed the large amount of data obtained during the drill to ensure the mesh network infrastructure is capable of providing the best service possible for data in a timely manner such that network congestion is avoided. We will discuss some of these findings in next section.

VI. Measurement Results and Analytical Discussion

In this section we present a subset of the measurement results obtained from the drill [13]. This particular subset of data consists of 8 tiers: server, wireless mesh nodes: nodes 1 to 5, one laptop, and a gateway. The gateway was directly connected to the Internet via a wired network.

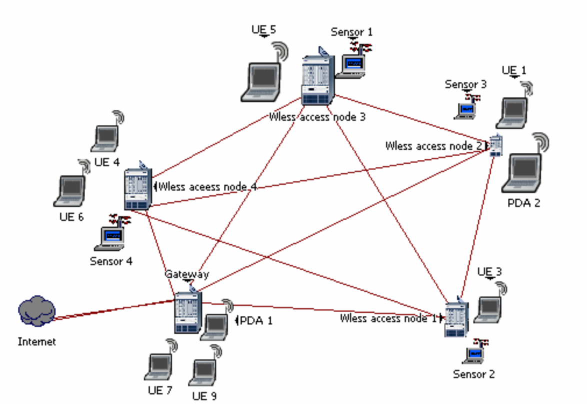

Figure 1- Mesh network infrastructure

For this particular work, we study the network behavior within the local mesh network. Figure 2 shows the total number of bytes sent at all network layers per direction.

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. Based on detailed study of the number of packets and the size of the packets, it is learned that the large number of small packets traveling over the network is the main source of bottleneck. This is verified by dividing the total number of messages sent by the number of packets exchanged in each direction. Table 1 shows the nodes in which processing delay can be a cause/potential cause of bottleneck in the network. Processing delay at the server appears to be the main source of delay which accounts for approximately 68.7% of total delay. In this particular data set, node 2 is the next potential bottleneck in terms of processing delay. Nodes 1 and 2 have the largest number of application turns which indicates the number of times the direction of communication changes between these two nodes. This can be optimized to improve performance in situations when larger amounts of traffic are transmitted. The large number of application turns between the nodes is one parameter that can be minimized for performance optimization. This will reduce the number of request/respond set of messages. The latency is insignificantly small in this example. Table 2 identifies bottlenecks and potential bottlenecks in the network. The main causes for these 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 2 shows the amount of application data transmitted between the server and mesh node number 2. Application throughput is approximately the same between server and all mesh nodes. However network throughput statistic includes all application data and network protocol overhead which is similar for all mesh nodes except node 2.

Network throughput statistic includes all application data and network protocol overhead. 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 [4]. 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. All network data is sent over Transport Control Protocol (TCP) which retransmits packets if they are lost or experience a long delay. This leads to a longer application response time. Figure 4 and 5 show the network throughput from server to node 3 (very similar to

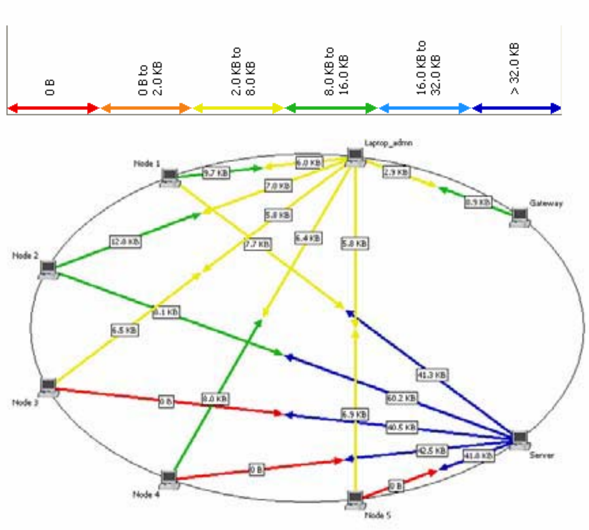

Figure 2- Network Data (Bytes) (Directional)

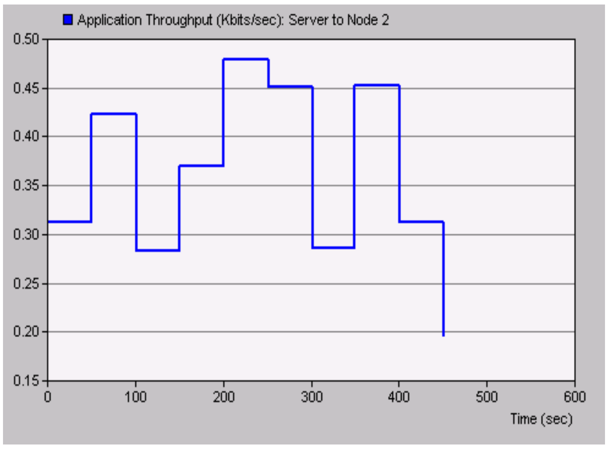

Figure 3. Application throughput from server to a mesh access node

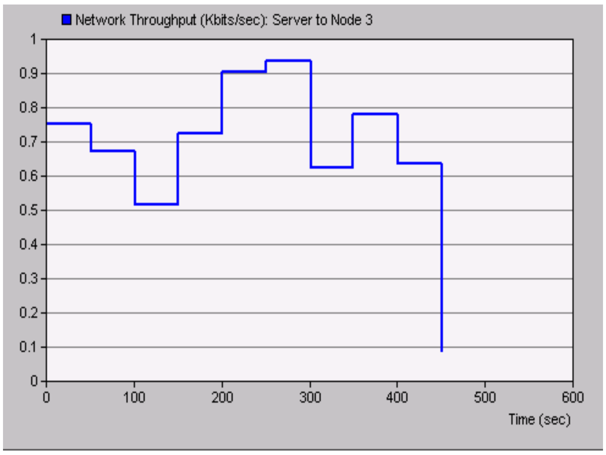

Figure 4. Network throughput from server to a mesh access node

© 2008 ACADEMY PUBLISHER

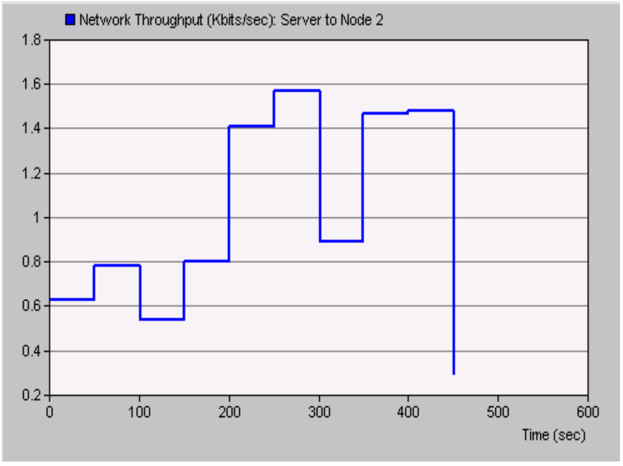

Figure 5. Network throughput from server to a mesh access node

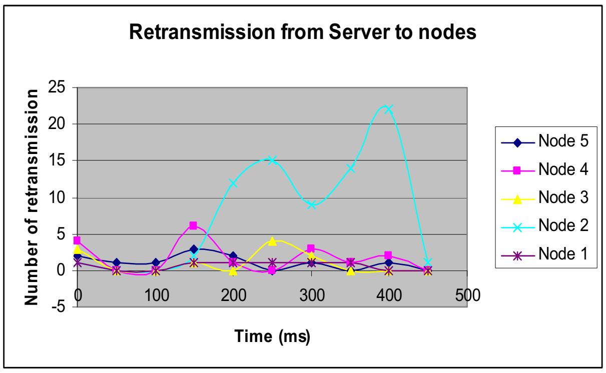

Figure 6. Retransmission from server to the mesh access nodes

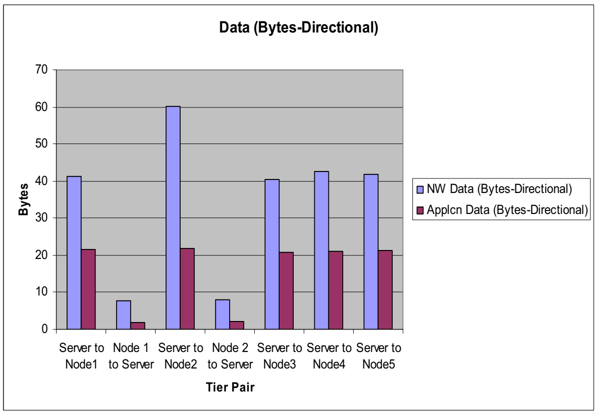

Figure 7. Application and Network Data from server to the mesh nodes (Bytes-Directional)

the network throughput between sever and node 1, 4 and 5) and node 2. Figure 6 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. Based on our measurements, server and node 2 are communicating over the network by sending a large number of small packets (about 42% of total packets) as RSRB messages (Remote Source Route Bridging) creating overhead [4].

Table 1- Delay over the network

	Server	Node 1	Node 2	Node 3	Node 4	Node 5	Gateway
Processing	Bottleneck	No Bottleneck	Potential Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck

Table 2- Network diagnosis for bottlenecks and potential bottlenecks

	Server <-> Node 2	Server <-> Node 1	Server <-> Node 3	Server <-> Node 4	Server <-> Node 5
Protocol Overhead	**Bottleneck**	**Bottleneck**	**Bottleneck**	**Bottleneck**	**Bottleneck**
Chattiness	**Bottleneck**	**Bottleneck**	No Bottleneck	No Bottleneck	No Bottleneck
Retransmissions	**Bottleneck**	Potential Bottleneck	**Bottleneck**	**Bottleneck**	**Bottleneck**
Out of Sequence Packets	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck
TCP Windowing (A → B)	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck
TCP Windowing (A ← B)	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck
TCP Nagle's Algorithm	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck	No Bottleneck

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.

Finally Figure 7 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

© 2008 ACADEMY PUBLISHER

verified by the signal strength measured during the drill.

Our goal is to extend this research to identify the main cause of this particular behavior and reduce the number of retransmission to reduce the occurrence of bottlenecks in the network. Additionally in future network studies we will enhance the network performance to transfer voice and data (video for example) with the best possible Quality of Service (QoS). Since in this particular application protocol overhead is a main source of bottleneck, network resources can be utilized by sending fewer larger application messages. Detailed study of Ad hoc performance measurement is crucial as it provides the test bed to experiment different topologies at different locations, for a variety of scenarios for an efficient network performance.

In voice applications over IP, voice is transmitted as packets over the Internet instead of bits over regular copper telephone wires. This application is very delay sensitive; therefore, QoS is important. Deploying VoIP over the mesh network provides local connectivity, enabling people at the disaster site to communicate with each other even without access to the Internet. When voice is transmitted over IP in a network with large packets, it would experience a larger delay which is not acceptable. Therefore, it becomes necessary to prioritize transmission of voice over data to reduce queuing delay. 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. In such scenarios, users sending voice are running a delay sensitive application which should be granted a Constant Bit Rate (CBR) service with a certain amount of bandwidth guaranteed at all time for that particular user while limiting the total number of users at any given time. Because of the QoS 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 are guaranteed with a minimum amount of bandwidth at all times; therefore data users may experience a longer delay depending on the amount of 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 are increased as they are left with a portion of bandwidth.

VII. Security and privacy issues

In an emergency application all different organizations communicate over the same network at some point in time. A secure communication is necessary for future communication networks to ensure that each organization receives only the data that is meant for them. In emergency scenarios with medical applications [11], patients' medical data can be accessed only by the medical team as part of personal privacy requirements established by HIPPA. It is very important to keep classified information away from mass media, which are always present at a disaster site. Cellular phones location detection might play a crucial role in life threatening emergency scenarios while in many other scenarios may conflict with privacy and the desired anonymous communication objectives.

In many scenarios, data should be encrypted to ensure that the right information reaches only the right people. Each data object has to be encrypted for the designated recipients so that only they are able to decrypt the message and access the information. There are several group communication protocols in traditional security systems addressing this type of security. In the applications with urgent need to access an operational infrastructure immediately, a feature should be implemented in the network enabling operators to turn encryption on or off. Depending on the special requirements of an application, an authenticating mechanism should ensure that only the right people access the information. Designing an appropriate authentication mechanism to provide secure communication over future hybrid networks is a demanding task considering the dynamic nature of the network. There has been a lot of research in identification mechanisms for Ad hoc networks [9].

Message integrity is another key feature that needs to be provisioned within the system. Furthermore, if in some scenarios the general public is providing the response organizations with potentially critical information, there should be ways to verify the accuracy of information and find out if it is trustworthy. Some existing group communication protocols have been briefly discussed in [10]. It is important to keep the size of such messages reasonable, as the number of people sharing the same information is increased. It is important in a group communication protocol to keep the changes transparent; therefore, when a user leaves or joins the group, this should be seamless to the other people sharing the same information to facilitate the well-known key distribution and key management problems in group communication. These are all real concerns that are becoming more of an issue as the communication technology evolves.

VIII. Conclusion

Designing a robust communications infrastructure for emergency applications is a demanding effort. It 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 communication technology should be cost efficient with minimum training requirements to effectively operate the system to allow wide deployment. 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 [1]. The power dependency as the cause of many tower failures has been

© 2008 ACADEMY PUBLISHER

addressed by using battery operated wireless access nodes for emergency applications and planning a back-up power supply.

The important role of social artifacts and tradition has been mentioned in developing and deploying new technologies. Devices using new technologies are not as convenient and widely used as regular ones. However an established alternative plan for emergency communications will help to speed up rescue and recovery efforts considerably and make a more efficient use of network resources. For example the use of VoIP handsets needs to be encouraged although they may not have the high quality of voice over landline handsets and cellular phones. Traffic management is achieved by prioritizing voice over data traffic to meet time-sensitivity requirements of voice applications.

We have presented measurements obtained over the real mesh test bed deployed on campus which is a valuable analysis tool to improve network survivability in emergency situations. In this paper we have explored and evaluated the network performance based on the real test bed measurements to identify vulnerabilities of the system off-line and to develop what-if scenarios to improve network survivability for disaster scenarios. We noticed that in this particular application, we should send fewer large packets to prevent bottlenecks across the network. By reducing the overhead caused by exchanging too many small control packets the network performance and application response time will be improved.

ACKNOWLEDGMENT

Work described in this paper was funded by the RESCUE projects at UCSD, NSF awards #0331690. The authors would like to thank the other project researchers at UCSD division of Calit2 for the group discussions.

REFERENCES

[1] 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.

[2] S. Goel,S. Belardo, L. Iwan, “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, January, 2004.

[3] ITR-RESCUE: Responding to Crises and Unexpected Events, http://www.itr-rescue.org/, Sep. 2006.

[4] RSRB Overhead Information [Token Ring]- Cisco Systems, http://www.cisco.com/en/US/tech/tk331/tk660/technologies_tech_note09186a008009472b.shtml#intro, Sep. 2006.

[5] G. Slack, “Bringing Firefighters Back Alive with Smart Technology”, Research at Berkeley Articles, UCB Research, http://research.chance.berkeley.edu/page.cfm?id=11&aid=28, Sep. 2006.

[6] P. Klapwijk,L. Rothkrantz, “Topology based infrastructure for crisis situations”, Proceedings of the 3rd International ISCRAM Conference, May 2006.

[7] K. Tierney, J. Sutton, “Cost and Culture: Barriers to the Adoption of Technology in Emergency Management”.

[8] J.W. Morentz, “Can We talk”, Proceedings 1994.Rockville, Maryland.

[9] F. Kargl, S. Schlott, M. Weber, “Identification in Ad hoc Networks”, Proceedings of the 39th Hawaii International Conference on System Sciences, January, 2006.

[10] R. B. Dilmaghani, MS Thesis, “An Investigation to Fast Modular Multiplication and Exponentiation Techniques to Speed-up RSA-Like Crypto Systems”, Department of Electrical and Computer Engineering, Colorado State University, 2003.

[11] M. L. Popovich, J.M. Henderson, J. Stinn, “Information technology in the Age of Emergency Public Health Response”, IEEE Engineering in Medicine and Biology Magazine, volume 5, 2002.

[12] J. Rosen, E. Grigg, J. Lanier, S. McGrath, et. al., “The Future of Command and Control for Disaster Response”, IEEE Engineering in Medicine and Biology Magazine, volume 5, 2002.

[13] Making Networks and Applications Perform, http://www.opnet.com/services/university, Sep. 2006.

[14] H. Zimmerman, “Availability of Technologies versus Capabilities of Users”, Proceedings of the 3rd International ISCRAM Conference, May 2006.

[15] Hazard Workshop, University of Colorado at Boulder, Natural Hazard Center, http://www.colorado.edu/hazards/, 2005.

[16] R. Zimmerman, “Social Implications of Infrastructure Network Interactions”, Journal of Urban Technology, Volume 8, Number 3, 2001.

[17] M. Gerst, R. Bunduchi, R. Williams, “Social Shaping and Standardization: A case study from Auto Industry”, Proceedings of the 38th Hawaii International Conference on System Sciences, January, 2005.

[18] M. Turoff, M. Chumer, B. Van de Walle, X. Yao, “The Design of a Dynamic Emergency Response Management Information System (DERMIS)”, Journal of Information Technology Theory and Application (JITTA), Volume 5, Number 4, Summer 2004.

[19] L. Wirbel, “Authorities Blamed for Communications Network Failure under Katrina’a Attack”, http://www.globalsecurity.org/org/news/2005/050905-comm-failure.htm, Sep. 2006.

[20] National Science Foundation, Science Daily: Remembering Katrina: Studies Look At Multiple Facets Of The Hurricane's Devastation, http://www.sciencedaily.com/releases/2006/09/060901163625.htm, Aug. 2006.

[21] Hurricane Katrina Recovery Information, Sep. 2005, http://www.tbr.org/katrina/kat_090705.htm, Sep. 2006.

[22] Grand Challenges for Disaster Reduction, National Science and Technology Council, Committee on environmental and Natural Resources, http://www.sdr.gov/SDRGrandChallengesforDisasterReduction.pdf, Aug. 2006.

[23] A. Futch, C. Soares, 2001 Duke L. & Tech. Rev. 0038, Enhanced 911 Technology and Privacy Concerns: How has the Balance Changed since September 11, Oct. 2001, http://www.law.duke.edu/journals/dltr/articles/2001dltr0038.html, Aug. 2006.Kauffman, R.J. and Mohtadi, H. Proprietary and open systems adoption in e-procurement: a risk-augmented transaction cost perspective. Journal of Management Information Systems, 21, 1 (2004), 137-166.

© 2008 ACADEMY PUBLISHER

[24] California Institute for Telecommunications and Information Technology (Calit2), http://www.calit2.net/.

[25] iTAG, WIISARD project , "UCSD Tests Intelligent Triage, Other Technologies in San Diego Disaster Drill", http://www.calit2.net/, Nov. 2006.

[26] A. Raniwala, T. Chiueh, "Architecting a High-Capacity Last-Mile Wireless Mesh Network", http://www.cs.sunysb.edu/~raniwala/hyacinth-poster.pdf, Nov. 2006.

[27] A. Raniwala, T. Chiueh, "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/, Nov. 06.

[28] S. Das, D. Koutsonikolas, Y.C. Hu, D. Peroulis, "Characterizing Multi-Way Interference in wireless Mesh Networks, ACM International Workshop on Wireless Network Test beds, Experimental evaluation and CHaracterization ACM WinTECH 2006.

[29] L. Iannone, S. Fdida, "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), July 2005, http://www-rp.lip6.fr/~iannone/, Nov. 2006.

[30] L. Iannone, K. Kabassanov, S. Fdida, "The real Gain of Cross-Layer Routing in Wireless Mesh Networks", In Proceedings of Second International Workshop on Multi-hop Ad hoc Networks: from Theory to Reality (ACM/SIGMOBILE RealMan'06). Florence (Italy), May 2006, Nov. 2006.

[31] J. Eriksson, S. Agarwal, P. Bahl, J. Padhye, "Feasibility Study of Mesh Networks for All-Wireless Offices", International conference on mobile systems, applications, and services, ACM MobiSys 2006.

[32] G. Bianchi, F. Formisano, D. Giustiniano, "802.11b/g Link Level Measurements for an Outdoor Wireless Campus Network", Proceedings of the 2006 International Symposium on a World of Wireless, Mobile, and Multimedia (WoWMoM), IEEE 2006.

[33] A.A. Pirzada, M. Portmann, J. Idulska, "Evaluation of Multi-Radio Extensions to AODV for Wireless Mesh Networks", Proceedings of the international workshop on Mobility management and wireless access ACM MobiWac 2006.

[34] V. Navda, A. Kashyap, S.R. das, "Design and Evaluation of iMesh: an Infrastructure-mode Wireless Mesh Network", Proceedings of the 2005 International Symposium on a World of Wireless, Mobile, and Multimedia (WoWMoM), IEEE 2005.

[35] R.B. Dilmaghani, R.R. Rao, "Hybrid Communication Infrastructure and Social Implications for Disaster Management", Proceedings of the 40th Hawaii International Conference on System Sciences, January, 2007.

[36] MIT Roofnet, http://pdos.csail.mit.edu/roofnet/doku.php, Nov. 2006.

[37] Bay Area Wireless Users Group, http://www.bawug.org, Nov. 2006.

[38] Champaigne-Urbana Community Wireless Network, http://www.cuwireless.net, Nov. 2006.

[39] WiFi Mesh News, http://wi-fi-mesh-news.newslib.com/feed.xml, Nov. 2006.

[40] Seattle wireless, http://www.seattlewireless.net, Nov. 2006.

[41] wireless leiden, http://www.wirelessleiden.nl, Nov. 2006.

Raheleh B. Dilmaghani received her B.S. in Electrical Engineering from the Univ. of Tehran, Iran. After which, she worked for Moshanir Electrical Engineering Consulting Firm for four years. She received her M.S. degree in Electrical and Computer Engineering from Colorado State Univ. and is currently pursuing her Ph.D. in Electrical and Computer Engineering at the Univ. of California, San Diego. While a graduate student, she has also been engaged in industry as an intern with Hewlett Packard (Roseville, CA 2002), Cisco (San Jose, CA 2007) and Google (London, UK 2007); each for approximately three months. Her current areas of research and interest are in communication networking, hybrid mesh networks, algorithms, Petri Nets, and privacy/security.

Ramesh Rao is a faculty member in the department of Electrical and Computer Engineering at the University of California, San Diego, where he is currently Director of the San Diego Division of the California Institute for Telecommunications and Information Technology (Calit2). In April 2004, he was named Qualcomm Endowed Chair in Telecommunications and Information Technology. His research interests include architectures, protocols and performance analysis of wireless, wire line and photonic networks for integrated multi-media services. Prior to his appointment as the Director of the San Diego Division of Calit2, he served as the Director of the UCSD Center for Wireless Communications (CWC) and was the Vice Chair of Instructional Affairs in the Department of Electrical and Computer Engineering.