On Non-invasive Network Measurement for Emergency Response Wireless Mesh Networks

B. S. Manoj*, Bheemarjuna Reddy Tamma†, Paul Blair††, and Ramesh Rao††

*Indian Institute of Space Science and Technology, Trivandrum, 695547 India, Email: bsmanoj@iist.ac.in
†Department of CSE, Indian Institute of Technology Hyderabad, Hyderabad, 502205 India, Email: tbr@iith.ac.in
††UCSD-CalIT2, University of California San Diego, San Diego, CA 92093 USA, Email: {pblair,rrao}@ucsd.edu

***Abstract*—In this paper, we present the challenges in gathering network traffic information from an emergency response network, discuss the non-invasive traffic sensing and analyzing infrastructure that we created and used for a real-world application, and present some of the performance observations made using our infrastructure. Network performance measurement and analysis is a challenging task for a large-scale emergency response network. We developed an infrastructure for non-invasive traffic monitoring that requires neither modifications to nor knowledge about the production emergency response network. Our non-invasive network measurement infrastructure was used for real-world emergency response drills such as the Golden Eagle drill conducted at California State University, San Marcos in May 2010. Performance observations obtained from our system show that non-invasive traffic monitoring is a scalable, efficient, and viable method for large-scale network monitoring and performance measurement.**

Keywords- wireless mesh network; emergency response network; performance evaluation; temporal dynamics

I. INTRODUCTION

Emergency response networking is a challenging activity. Furthermore, the challenges may be exacerbated when the network must support medical emergency response services, which typically require numerous additional activities. The Hurricane Katrina After Action Report [12] highlights the need for Local Area Network deployments in such affected areas for communication and coordination. One of the key challenges in providing communications at the disaster response area is the lack of interoperable communication facilities. Most importantly, quickly deployable and reconfigurable communications networks are essential for effective response coordination at Ground-Zero [10]. Ground-Zero is the typical name associated with the most impacted area of an incident or attack.

Wireless Mesh Networks (WMNs) [14] are fully distributed multihop wireless networks that provide easy deployment and reconfiguration capability, thereby making them effective for emergency response [11, 15, 16]. Examples for prototype WMNs designed to support medical applications and collection of medical sensors can be found in [11, 13]. These example networks are university-developed prototypes, however, which show promise in their use in Ground-Zero scenarios for emergency response. Examples of such medical response activities, conducted over emergency response WMNs, include the gathering of vital bio-medical parameters from the affected population using a collection of sensors, setting up of on-site infrastructure required to analyze the spatio-temporal data, and organizing quick logistics for the medical response. All the data and information may need to be transferred over the wireless mesh network deployed by the first responders.

In this paper, we present the design of a non-invasive network measurement infrastructure for performance measurement and analysis of emergency response wireless networks. Furthermore, we discuss the network that we deployed for a full scale emergency response drill, the challenges faced in implementing a non-invasive performance measurement infrastructure, and the traffic dynamics observed during the event.

The rest of the paper is organized as follows: Section II briefs the challenges in network performance measurement and what motivated us to pursue a non-invasive network performance measurement approach. Section III presents the network topology and associated systems that we deployed during Operation Golden Eagle in San Marcos, California during May 2010. In Section IV, we discuss the challenges in designing a non-invasive network infrastructure for performance measurement of large scale wireless mesh networks. Section V briefs the performance observations and the network and traffic dynamics that we observed during Operation Golden Eagle. Finally, Section VI summarizes the paper.

II. CHALLENGES IN EMERGENCY RESPONSE NETWORK PERFORMANCE MEASUREMNET

One of the biggest challenges in emergency response networks is the overhead involved in managing the operations of the network. The management of communication overhead is very complex once the network is deployed. This challenge is mainly due to the resource constraints which exist on the wireless routers due to their limited energy sources, computation power, and data storage resources. Operational management of an emergency response network includes: network performance measurement, network adaptation as the traffic demand varies, and handling network failures in a dynamic and self configurable manner. The network management overhead usually varies as the network is adapted due to traffic load changes. These challenges are exacerbated

978-1-4244-9825-3/11/$26.00 ©2011 IEEE

when the underlying emergency response WMN functions over an interference-prone wireless channel that has bandwidth constraints. In this paper, of the three tasks mentioned above, we focus on network performance measurement as well as the temporal dynamics of the network during a near real-world emergency response event. Temporal dynamics is defined as the changes in the network performance behavior as a function of the event progression in time. The network performance measurement task can be further split into three sub-tasks: (i) network traffic observation, (ii) storage and retrieval of the observed data, and (iii) real-time analysis of the stored data to make decisions.

We define two ways of implementing the above mentioned sub-tasks: (a) invasive network measurement approach and (b) non-invasive network measurement approach. In the case of invasive network measurement, the network performance measurement is carried out from within the production network whereas in the case of non-invasive network measurement, a parallel network measurement infrastructure is deployed to remove the measurement burden from the production network. That is, in an invasive network measurement system the production network, an emergency response WMN, is modified to additionally collect data about the network environment and the operation of the network. On the other hand, in the case of a non-invasive approach, the production network does minimal data collection and the major data collection burden is given to a separate network measurement infrastructure deployed in parallel with the production network.

In the case of an invasive network measurement approach, implementation of the above subtasks on the emergency response WMN routers is particularly challenging because the computation requirement for each of them is not trivial. For example, the network traffic observation requires the WMN routers to receive the data packets transferred over the channels of interest. However, emergency response WMN routers may have limited number of radio interfaces that may not be available to sense data packets from all the channels of interest. Besides, the WMN routers may be constrained of computing power such that receiving large amounts of packets and writing them to local storage can be challenging. Usually, the local storage of WMN routers shows high access time compared to more capable computers such as Laptops. Frequent writing and reading of data to and from such slow memory devices can further slow down the WMN router's other key functions such as packet forwarding. Finally, the analysis of data packets and other information, that is essential to make critical network configuration decisions, can take high computing power as well as display resources. Typically, most WMN routers may not be equipped with display resources. The lack of display resources and data analysis capability forces the WMN network to transfer the data to a central location in order to have the analysis done. Such transferring of large amounts of network data to a central location over a bandwidth-constrained production WMN can further burden the network. Therefore, invasive network measurement approach may substantially affect the performance of a production emergency response WMN.

The non-invasive network measurement infrastructure has many benefits as well as challenges. The main benefit is that it lessens the computing and communication resource demands placed on the production emergency response WMN. Besides, a failure of the network measurement software is unlikely to impact the operation of the production network in a substantial manner.

III. NETWORK TOPOLOGY OF THE EMERGENCY RESPONSE NETWORK FOR OPERATION GOLDEN EAGLE

Operation Golden Eagle, a full scale emergency response drill organized by Medical Metropolitan Strike Team (MMST) of San Diego County was conducted at California State University, San Marcos on May 18, 2010. As part of the WIISARD-SAGE project [1], we deployed a medical emergency response network. The topology of the network deployed is as shown in Figure 1. The wireless mesh network (WMN) deployed during the experiment was based on CalMesh 2.0 platform [2] developed in-house at the University of California, San Diego. The terrain of deployment was uneven with a low-lying football field surrounded by high-lying roads and parking lots. We employed one dozen CalMesh routers (R1 through R12 as shown in the network topology). Router R1 was connected with the backbone wireless link, operating in licensed spectrum, to the Internet. Only half the football field is shown in the figure (see the location of WMN routers R7, R9, and R11 in Figure 1).

Figure 1. Topology of the deployed WMN (WMN routers are numbered from R1 through R12).

Since the network is designed to operate in a production mode during the drill, we need to limit the amount of processing power used for statistics collection, analysis, and storage. Besides, a data collection infrastructure within the network system may have limited capability to observe the entire wireless channel set. Therefore, we designed, implemented, and deployed a non-invasive, out-of-network traffic sampling system for performance evaluation of medium to large scale emergency response WMNs. Each CalMesh router has two radio interfaces, one for the backbone communication with other routers and another for the access communication with WMN clients. The backbone radio

interface operates on a fixed channel whereas the access channel operates on a dynamic channel, selected at the beginning of the device boot process. All the radio interfaces use IEEE 802.11 a/b/g capable NICs with Atheros chipsets.

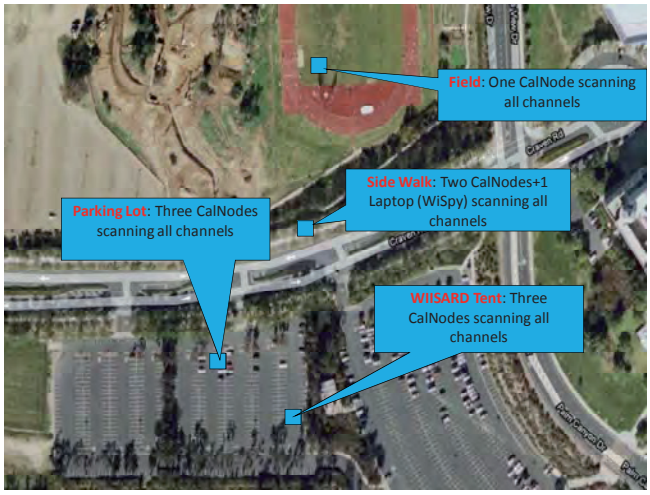

Figure 2. Location of CalNodes for non-invasive network performance measurement during Operation Golden Eagle.

Figure 2 shows the location of wireless traffic sensors, labeled as CalNodes [3], that we deployed in order to monitor the network's behavior without impacting the services of the WMN routers. Of the four locations in Figure 2, only one location had a single CalNode sensor. That is, the three remaining locations had multiple traffic sensors that were meant for redundancy. Each CalNode employed a time-based time-driven traffic sensing strategy for accurate sampling of all the 11 channels traffic in IEEE 802.11b/g spectrum [4]. We have found that time-based time-driven sampling is very accurate for multi-channel traffic sampling applications. One of the main benefits of our traffic sampling approach is that the amount of data collected using each traffic sensor is much less than the data typically gathered in full traffic capture.

A. Non-invasive network monitoring infrastructure

Technical specification of the CalNode device, shown in Figure 3, includes the following: ALIX 2c2 embedded system board (500MHz AMD Geode Processor) with 8GB Compact Flash Memory where two Atheros chipset-based embedded 802.11a/b/g wireless NICs having Omni-directional pigtail antenna for 2.4GHz/5.2GHz are used. The operating system employed is Voyage Linux 0.5.2 where TCPdump [5] and MadWiFi driver [6] were used for gathering the traffic and NIC information.

IV. CHALLENGES IN DESIGNING THE NON-INVASIVE NETWORK MEASUREMENT SYSTEM

There are many challenges in designing systems for non-invasive performance measurement of WMNs. First, the presence of multiple channels that most of today's WMNs utilize. Full traffic capture may result in huge amounts of data that can be neither easily managed nor inexpensive. Second, the time synchronization among the sensor nodes must be ensured. Finally, the infrastructure for automating the processing and reporting of large sets of data from multiple locations is very challenging.

Figure 3. Inside view of traffic sampling node, CalNode.

A. Multi-channel sampling

The complete capture on every channel of operation can be very expensive in a real-world network that spans dozens of nodes. We follow a multi-channel sampling approach where the monitoring radio device is made to sample all the channels of interest in the spectrum. While doing so, the most important aspect is the ability of the sampling mechanism to accurately represent the traffic characteristics. We used the time-based time-driven sampling approach proposed in [4], which is proven to be highly accurate.

B. Time Synchronization

In any distributed measurement system, it is critical to have time synchronization between devices that monitor the network. In our scheme, the network monitoring system uses two time synchronization mechanisms. First, each sensor node may connect to an external Network Time Protocol (NTP) [7] server to synchronize. Second, synchronization is based on the relative time information that can be obtained from the timestamps, information contained in the packets such as the address fields and the sequence numbers. This information can be used to generate a relative time-based synchronization for correlating the events. A similar approach for achieving time synchronization is presented in [8]. In our approach,we attempted both, NTP and correlating the events, at different levels. For example, during the drill we used an NTP server to synchronize the devices, while during the data analysis process we depended on the packet contents to correlate the occurrence of events.

C. Infrastructure for Processing large sets of data

Processing large sets of network monitoring data is very challenging and we describe here the infrastructure that we

developed as part of the data analysis under the WIISARD-SAGE project. The steps in the process that we used are illustrated in Figure 4. The first stage is the Data Gathering process where, as discussed above, we employed multiple sensors each having a multi-channel wireless sampling strategy. The information gathered belongs to two categories: first, the packets observed by the CalNodes from each of the channels they monitor. The information contained in the packet header and limited information from the data is extracted for the second stage. In addition to the packet contents, the information from the wireless network interface card, such as the packet errors and signal quality, are gathered. The second stage is the Data Repositorizing phase where the collected binary data is parsed and stored in a MySQL database.

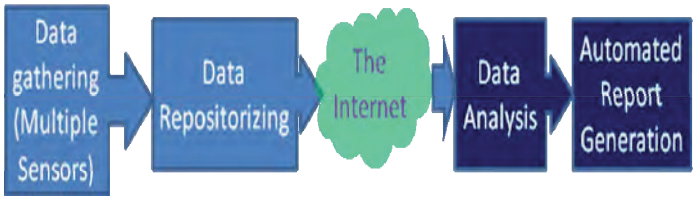

Figure 4. The flow diagram of the entire system including the network performance measurement, analysis, and automated documentation process.

Two kinds of database tables are designed for repositorizing the data gathered. First, as mentioned above, the information from the packets are stored in one set of database tables and the information derived from the NIC driver are stored in another set. Both sets of information from a single CalNode are synchronized by using local timestamps of the device. The third stage is the data analysis phase where we used Matlab-based tools to communicate with the database over the Internet. The analysis varies with the requirements on the performance observations. The Matlab code that we created was designed with the objective of maximally exploiting the processing capability of the MySQL database server. The final stage in the process of data analysis is report generation where a PDF document is generated with the observations and graphs from the data analysis system. Such an automated data analysis system can radically simplify the performance analysis of large scale WMNs.

We briefly present the method employed for automatic report generation shown in Figure 4. Since we used Matlab for data analysis, our tools for automated report generation was limited to only a certain formats that could be written in text format. However, at the time, we were challenged by the need to generate the report in popular formats such as Portable Document Format (PDF). Therefore, we used a combination of tools to generate PDF files, by employing a three step process: generation of (i) content, (ii) format, and (iii) final document.

In the first step, we used Matlab to produce the content required for the reports. Our focus was limited to producing graph images and corresponding text that presented report briefs, captions, and other descriptions of the observations. Once the content is generated, it is embedded in the document file format by using LaTeX format. The choice of LaTeX simplified the task as it could include the graph images as well as text into the graphics content. Once the data content is placed in the LaTeX source file, using Matlab, we compiled the LaTeX file to generate the postscript format output document. Finally, in the third step, the postscript file is converted to PDF format for distribution. Therefore, the automatic report generation provides a very convenient tool to generate and distribute the overall network performance behavior.

Note that the automatic report generation is an optional non-real time feature that reports the performance behavior of the entire emergency response event. The analysis stage of the entire process will generate visual performance analysis for real-time decision making.

V. PERFORMANCE OBSERVATIONS

In this section, we present the network performance observations made by our system. We compare the observations made by our non-invasive collection of sensors to the network's known character to validate our system's capability. First, let us describe the amount of data that we gathered for a comprehensive analysis of the system during the Operation Golden Eagle drill. The five hour drill, that covered a geographical area requiring a dozen WMN routers, resulted in only 5GB of captured data using our system. This amount of data is substantially less compared to full traffic capture that other approaches may use. A typical system for full capture may require several tens of GB of data for such a drill.

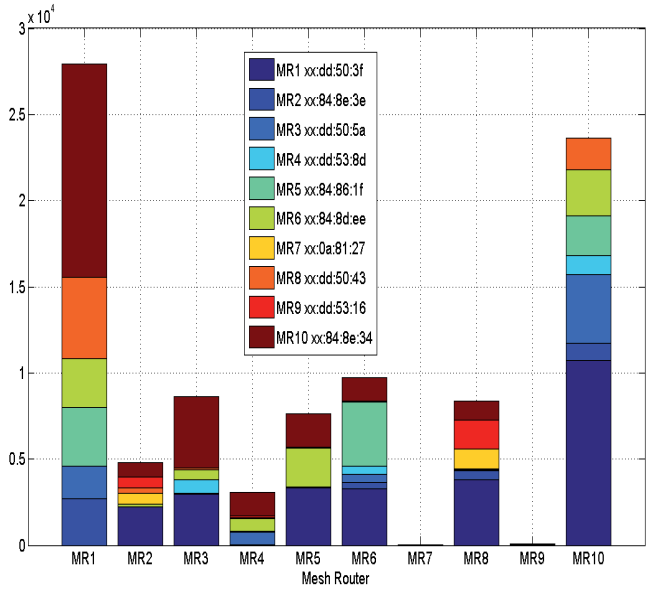

Figure 5. Inter-router traffic (Y-axis: packets per unit time, X-axis: routers. The labels MR# refers to Mesh Router # that corresponds to the router R# in Figure 1).

Figure 5 shows the Inter-router traffic in the CalMesh network deployed by the WIISARD-SAGE project. According to our performance observation evaluations, we found that the router MR1 seems the most heavily loaded router in the network. From the network topology, it can be seen that this

router is central to the network and is also the gateway to the Internet. Therefore, our system made the correct observation. Furthermore, the link between routers MR1 and MR10 is the heaviest loaded link in the network. Again, from the network topology, it can be noticed that the router MR10 is one hop away from the router MR1 in the direction of the soccer field from where the victims were moved to the triaging area. Therefore, the system, using non-invasive multi-channel sampling, could make a clear estimation of the relative link level traffic within the network topology.

Figure 6 shows the traffic in terms of packets per second for all the 11 channels in 802.11 b/g spectrum averaged per minute during the drill hours (9am-2pm).

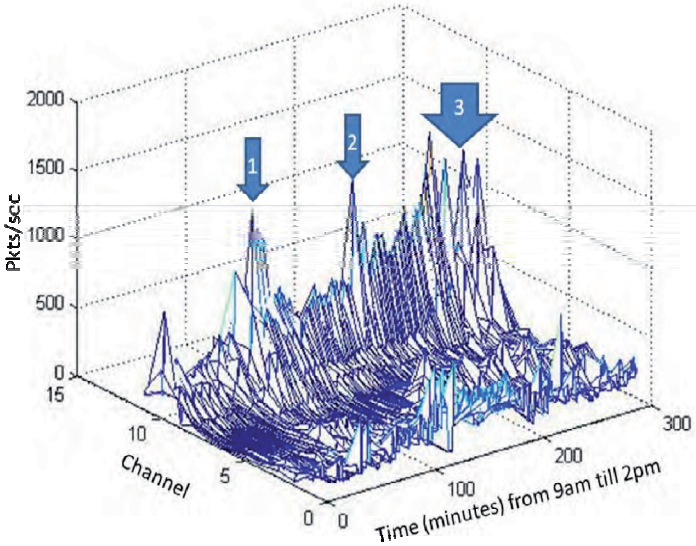

Figure 6. Packet arrival rate Vs channel Vs time.

It can be noticed that channel 10 experienced the heaviest traffic. That is mainly due to fact that the backbone channel of the deployed CalMesh network was fixed on channel 10. Further, it can be noticed that the peak traffic was observed at three instances, marked 1, 2, and 3 in the figure, during the drill. The third instance resulted from the throughput test conducted, by our researchers, using ***iperf*** tool [9] after the drill was formally concluded.

The throughput test across the WMN routers sets the upper limit of the network's capacity in terms of packet/second or bits/second metrics. Corraborating this measured observation, it was observed that during the middle of the drill, we had faced network congestion as a result of large number of small packets. Therefore, we can conclude that the network was at least congested by small packets, or reached its packets/sec capacity, twice during the drill. That also means the network was fairly underutilized for a substantial duration of the drill.

Figure 7 shows the network traffic in terms of bits per second for all channels during the drill. However, in comparison to Figure 6, it can be noticed that the bits/sec capacity of the network is low during most of the drill period except near the end of the drill.

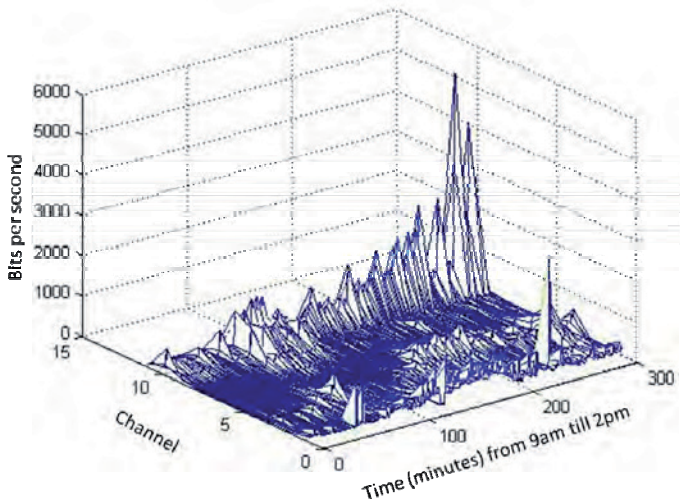

Figure 7. Network traffic in bits/s Vs Channel Vs Time.

As discussed above, during the conclusion of the drill, we conducted a large number of manual file transfer experiments for performance stress test of the WMN. Clearly, the results in Figures 6 and 7 show the network capacity in wireless mesh network for disaster response, used for medical response, can be defined into packets/sec as well as bits/sec. Most importantly, these two performance measures behaved differently during the response drill.

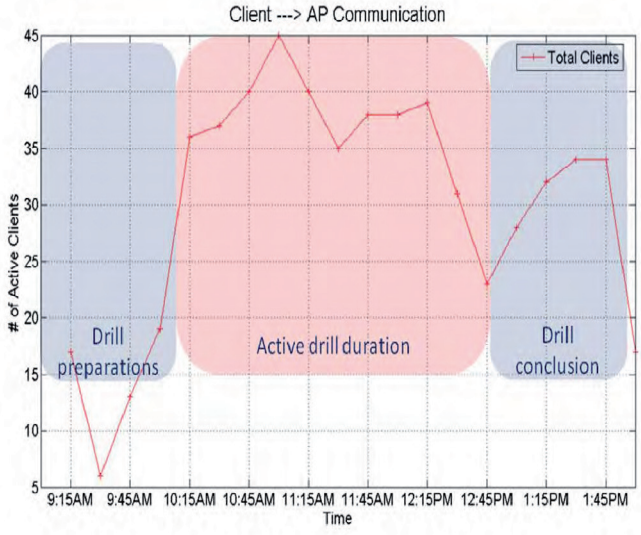

Figure 8. Temporal dynamics of Client-Network communication.

Another observation that we made using the non-invasive network monitoring infrastructure is the key network parameters such as WMN Client to WMN AP communications per unit time as a function of time during the Operation Golden Eagle drill. An example result that illustrates the temporal dynamics of client-network communication is shown in Figure 8. As shown in the figure, during the beginning of the drill, the network saw as few as 20

clients connected to the network which, however, grew to as many as 45 clients during the active drill duration that spanned from 10:15AM until 12:30PM. The maximum number of clients was noticed about 45 minutes after the simulated disaster that was triggered at 10:15AM. During the conclusion phase of the drill, when the network data transfer measurement experiments were conducted, we noticed an increase, albeit smaller, of the number of active clients. Therefore, the temporal dynamics of the connectivity can be captured using the non-invasive network performance measurement approach.

VI. SUMMARY

In this paper, we presented an architecture and example implementation for non-invasive network performance monitoring and analysis for large to medium scale emergency response management networks. According to our system architecture, a set of multi-channel wireless network sampling devices are placed in the area of network deployment. The data gathered by the sensor devices are then repositorized in a MySQL-based database repository which can be analyzed and studied further. We presented the challenges in the design of such performance measurement systems and briefed the performance observations we made during the Operation Golden Eagle drill conducted at California State University, San Marcos in May 2010. Future work in this direction may include real-time visualization and management of the network by implementing the data repositorizing and analysis carried out online during the event.

ACKNOWLEDGMENT

This work was supported in parts by the WIISARD-SAGE project and the ARO-High School Apprenticeship program (HSAP) at the UCSD division of CalIT2. Financial support for Travel and Registration for presenting this work was provided by the Indian Institute of Space Science and Technology, Trivandrum, India.

REFERENCES

[1] WIISARD-SAGE WEBSITE: HTTP://WWW.WIISARD.ORG/

[2] CalMesh 2.0, 2010. HTTP://CALMESH.CALIT2.NET/

[3] CalNode 1.0, 2010. HTTP://CALNODE.CALIT2.NET/

[4] B. R. Tamma, N. Baldo, B. S. Manoj, R. R. Rao "Multi-Channel Wireless Traffic Sensing and Characterization for Cognitive Networking," PROCEEDINGS OF IEEE ICC 2009, JUNE 2009.

[5] TCP DUMP TOOL: HTTP://WWW.TCPDUMP.ORG

[6] MADWIFI DRIVER: HTTP://MADWIFI.ORG

[7] NETWORK TIME PROTOCOL. HTTP://WWW.NTP.ORG

[8]. Cheng, Y.-C. ET AL. "Jigsaw: Solving the Puzzle of Enterprise 802.11 Analysis," Proceedings of ACM SIGCOMM 2006, 2006.

[9] IPerf tool: http://sourceforge.net/projects/iperf/

[10] B. S. Manoj and A. Hubenko-Baker, "Communication Challenges in Emergency Response," Communications of the ACM, Vol. 50, No. 3, pp. 51-53, March 2007.

[11] B. Braunstein, T. Trimble, R. Mishra, B. S. Manoj, Ramesh Rao, and L. Lenert, "Feasibility of Using Distributed Wireless Mesh Networks for Medical Emergency Response," Proceedings of AMIA 2006, September 2006.

[12] Hurricace Katrina: After Action Report. Avilable from http://www.bt.cdc.gov/disasters/hurricanes/katrina/pdf/katrina-aar.pdf December 2005.

[13] T. Gao et al, "Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results," Proceedings of IEEE HST 2008.

[14] Y. S. Zhang et.al., *Wireless Mesh Networks Architectures, Protocols, and Standards,* CRC Press, 2006.

[15] M. Gao, F. Zhang, and J. Tian, "Wireless Mesh Network for Emergency Response System Based on Embedded System," In Proceedings of the 2008 International Conference on Embedded Software and Systems Symposia (ICESSSYMPOSIA '08), pp. 361-365, 2008.

[16] A. Yarali, B. Ahsant, S. Rahman , "Wireless Mesh Networking: A Key Solution for Emergency & Rural Applications," Proceedings of Advances in Mesh Networks 2009 (MESH 2009), pp.143-149, June 2009.