On The Traffic Behavior of Distributed Wireless Mesh Networks

Brian Braunstein, Troy Trimble
CalIT2, UCSD Division,
La Jolla, CA 92093-0436
brian@bristyle.com,
trimble@ucsd.edu

Rajesh Mishra
CalIT2, UCSD Division
La Jolla, CA 92093-0436
ramishra@ucsd.edu

B. S. Manoj, Ramesh Rao
University of California, San Diego
La Jolla, CA 92093-0436
bsmanoj, rrao@ucsd.edu

ABSTRACT - Wireless Mesh Networks (WMNs) are formed by self-organized wireless nodes that use multi-hop wireless relaying. These networks are useable in a variety of situations ranging from fixed residential broadband networking based on rooftop wireless mesh nodes to emergency response networks for handling large scale disasters. Quick deployability, minimal configuration, broadband communication, and easiness of reconfigurability are the major characteristics that make WMNs a suitable choice for emergency applications. There exist several open research issues in using such WMNs for emergency response applications. One example is the deployment strategy which must be in accordance with the principal application and its topological requirements. We, in this paper, present a hybrid distributed wireless networking architecture, Extreme Networking System (ENS), and present large set of performance observations collected from a real distributed hybrid wireless mesh network used for supporting a medical emergency response application. We present the traffic behavior observed in our network when a client server medical emergency response application is employed. The performance observations on real-traffic scenarios for emergency response application underlines the need for focusing further research on topology control, reliability, service availability, and distributed management.

Keywords
Distributed Wireless Mesh Networks, Performance Evaluation, Routing and Topology Control

I. INTRODUCTION

Distributed Wireless Mesh Network (WMN) is a recently emerged networking paradigm which attracted significant research and industrial attention in the recent past. The primary reasons behind the success of this networking paradigm are the following: (a) very inexpensive network infrastructure due to the proliferation of IEEE 802.11 based devices, (b) easiness of deploying and reconfiguring the network, (c) broadband data support, and (d) the use of unlicensed spectrum. Due to these advantages, WMNs find many applications such as residential rooftop networks for Internet provisioning, municipal networks covering streets, towns, and business streets providing ubiquitous coverage, home networking by extending connectivity of DSL/Cable modem, campus networking in universities, law enforcement applications, and military applications. In this work, we focus on a new network architecture developed for homeland security applications and its application and behavior in a simulated disaster environment.

Our hybrid wireless networking architecture, Extreme Networking System (ENS), is designed to handle a variety of disaster situations during which the normal networking infrastructures are either destroyed or not operational. We briefly discuss the architecture and present the traffic behavioral observations made, with a client server model emergency medical response application, during a simulated large scale homeland security drill.

Organization of the rest of the paper is as follows: Section 2 describes the network architecture and network environment. The traffic behavioral observations and measurements are presented in Section 3. Section 4 concludes the paper.
II. NETWORK ARCHITECTURE

The network architecture used in our ENS architecture is hybrid in nature by utilizing multiple hierarchies for achieving reliable network connectivity to the external world in the event of emergencies or during critical events. In this architecture, there are three hierarchical levels: (i) the lowest level is the user access plane, (ii) the middle level is formed by a wireless mesh network plane, and (iii) the upper level is the backhaul connectivity plane. The user access plane is same as a typical wireless LAN connectivity mechanism with channel scanning, association, and authentication leading to user’s equipment connectivity. The second plane is the WMN which is formed by UCSD CalMesh [1] nodes. The third plane is the backbone plane which connects the wireless mesh plane to any of the available backbone networks. Example backbone networks are (i) wired networks, (ii) wireless LANs, (iii) cellular networks, and (iv) satellite networks. During a system deployment, such hybrid architectures can exploit any available backbone network for getting connected to the Internet. In the absence of any possible connectivity systems, the mesh plane would work as a local networking infrastructure providing network services to all the nodes connected to it. The use of multiple backbones raises demand for bandwidth aggregation and load balancing. This architecture utilizes basic session level bandwidth aggregation and coarse load balancing by diverting connections across available gateway nodes. Each gateway node has multiple network interfaces; one for the mesh network plane and other for the backbone plane. In Figure 1, an illustration of the ENS architecture is presented with three gateway nodes. The gateway nodes 1 and 2 have backbone connectivity over 1xEVDO and 1xRTT CDMA cellular networks, respectively. The Gateway 3 has a satellite receiver interface over which the WMN plane can connect to internet in the event that the disaster area has no cellular coverage. Due to the use a fully distributed WMN plane and the utilization of simultaneous multiple backbone planes, the ENS architecture could deliver very high reliability and availability for supporting critical applications.

![Figure 1. The ENS architecture.](image-url)

We used a client-server architecture based medical emergency application, WIISARD, on top of our network architecture to study the traffic behavior.

*Wireless Internet Information System for Medical Response in Disaster (WIISARD)*

The results presented in this paper and the observations made on the traffic behavior of the ENS system are based on a specific application, WIISARD [2], an information system for providing medical emergency response. WIISARD is a client-server architecture that uses one server repository and a large number of clients. Figure 2 shows the overall system
WIISARD system architecture has five interlocking components. These are patient wireless devices, responder wireless device and system, medical visualization system, disaster data bases, and hospital system. The patient wireless device is an electronic tag attached to every disaster victim that monitors the patient’s health status using a variety of sensors such as Pulse Oximeter and updates it to a central repository [2]. It provides the disaster handling agencies a visual indication on the patients’ health. The responder wireless device and system includes wireless devices used by first responders such as Voice over IP based communication devices, palmtops, and laptop computers. Medical visualization systems provide critical facilities that include visualization and telemedicine. Certain sophisticated facilities cannot be taken to the disaster site which necessitates communication between nodes in the field and in hospitals. Disaster databases represent the central repository setup at the disaster site in order to keep track of the progress of the response activity. Disaster databases may also be replicated in the network and in the Internet, if sufficient bandwidth network connectivity is present. The last component in the WIISARD system is the hospital system with which the first responders, the visualization systems, and the central repository will communicate in order to obtain resources and support.

Experimental Network Environment

San Diego County held a full scale home land security drill at the DelMar Fair Grounds, San Diego, where the ENS deployed for the experiment is depicted in Figure 3. Here, the area marked Hot is the zone where the simulated attack took place. The areas marked Warm and Cold are the zones where the victims were treated and other emergency coordinating activities were taken place. The network deployment topology was elongated to serve the area depending on the geographical orientation of the field. Though the network topology appears linear in the area close to the Hot zone and in between Hot zone and Warm zone, each node in the network was connected over multiple links. The overall network topology in emergency response depends mainly on how the emergency network deployment is planned, how the response actions are ordered, how the terrain is, and what the predominant application scenario is.
between those two nodes. The use of such weak links leads to a very low link data rate and hence we used a spanning tree based wireless distribution system to forward packets over only strong links. In addition, the weak links very often face full outage as well. Therefore, the effect of topology and the topology variation would seriously interfere in a disaster response scenario. In such situations, the primary objective for utilizing the multihop nature of the WMNs is the increase in throughput by using multihop relaying. For example, in Figure 4, the link data rate achieved over link between nodes 2 to 18 is 1 Mbps whereas a multihop path between nodes 2 and 18 through nodes 10 and 16 provides a better throughput. This is because, at every link in the path 2-10-16-18, the data rate will be much higher than the direct single hop link between nodes 2 and 18. In our experiments, we used a routing mechanism that utilizes signal strength as the routing metric and we obtained about 2-3 times increase in throughput when compared to shortest path routing scheme.

From the signal strength view from node 2 (Figure 4), it is noted that there exists no direct connectivity between nodes 2 and 16. This is due to the physical obstruction present in between these nodes. From node 2, nodes 4, 8, and 10 are reachable with fairly good signal strength. Node 12 is reachable over a moderately strong link. The remaining nodes (6, 14, 18, and 20) are reachable over a very weak wireless link. Important observation noted is that these link quality parameters are not bidirectional and the use of these weak links is not useful for getting good performance. In this situation, our network architecture and routing protocol are designed to force the multihop operation in order to improve reliability and performance. This is an example of the real situation in disaster response where the network deployment time is very short and in most cases, the deployment process is carried out in an unplanned way.

The emergency response exercise and our experimental setup followed the sequence: (i) a real car bomb blast was carried out; (ii) 125 human victims were simulated, (iii) first responders arrived at the scene, (iv) ENS backbone network was then deployed, (v) the WIISARD network application was then deployed, and (vi) network monitoring was turned on when the medical response application uses the network. The network monitoring was done near the node 16 where the central repository of WIISARD system was situated.

### III. PERFORMANCE OBSERVATIONS AND DISCUSSION

Our experimental setup has collected large number of data packets during the drill and the collection statistics is shown in Table 1. The following sections provide detailed traffic observations made on the ENS infrastructure.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data capture duration</td>
<td>15549.115s</td>
</tr>
<tr>
<td>Number of packets</td>
<td>210727</td>
</tr>
<tr>
<td>Avg. packets/sec</td>
<td>13.552</td>
</tr>
<tr>
<td>Avg. packet size</td>
<td>269.547 bytes</td>
</tr>
<tr>
<td>Bytes</td>
<td>56,800,903</td>
</tr>
<tr>
<td>Avg Bytes/sec</td>
<td>3652.999</td>
</tr>
</tbody>
</table>

Figure 5 shows the packet share of the major traffic categories in the network. The main share of the packet-wise traffic is contributed by ICMP traffic which generated 35% of the total packet traffic. The increase in ICMP is contributed by
the design of WIISARD system which uses a keep alive mechanism using ICMP packets for all electronic sensor tags attached to victims/patients. The number of victim tags ranged from 100-125. ICMP is followed by TCP and UDP with 27% and 20% respectively. In addition, ARP traffic contributed to 18% of the traffic. This is due to the network design where the ARP packets are broadcasted to the whole wireless mesh network.

The byte-wise bandwidth share (see Figure 6) of the total traffic does not scale proportionally to the packet-wise bandwidth share of the respective traffic categories. In the byte-wise share of the bandwidth, TCP dominates with 43% of the traffic followed by UDP with 41% of the bandwidth. Other control traffic including ICMP, ARP, and others constitutes about 16% of the total bytes transferred over the network.

Figure 7 shows the total observed UDP traffic resulting from the WIISARD application on our ENS architecture. The total UDP packets formed about slightly more than 20% of the total packets and approximately 9% of the total packets were found to be carrying UDP data. In addition, we noted that the total UDP bytes carried in the network is about 41% and UDP data bytes constitute 20% of the total traffic. Though the UDP packet share is less, the byte share is more significant. Similar relation exists for TCP traffic as noted from Figure 8 which presents the TCP traffic’s share in the total traffic. TCP packets formed about 26% of the total packet traffic with an 11% share for TCP data packets. Interestingly, the 11% packet share lead to a staggering 36% of the total byte traffic in the network. The total TCP bytes traffic remained at 42%.

Figure 8 shows the HTTP traffic statistics with majority of the HTTP requests met a success response.
One important type of traffic in the network was video streaming over Real-Time Protocol (RTP) and we noticed the worst case performance, over the longest path in the network, experienced an end-to-end delay of less than 500ms. The end-to-end delay jitter remains approximately 50ms. The bandwidth variation for a single RTP stream showed that the average bandwidth per stream is about 45kbps. The total traffic variation compared to the TCP traffic with time is shown in Figure 10.

IV. CONCLUSIONS

In this paper, we describe reliable network architecture, Extreme Networking System (ENS), for supporting robust communication networking during emergency situations. Such a networking infrastructure experiences network traffic patterns and behavior which depends on the type of application and deployment scenario. We deployed our network infrastructure for supporting a simulated disaster response activity as part of a homeland security event and observed the traffic and network behavior when WIISARD, a client-server based medical emergency response application, was applied. We presented a detailed traffic and performance observation study in such an environment.

V. ACKNOWLEDGMENTS

Work described in this paper was funded by the RESCUE project at UCSD, NSF award #0331690, and the Responsphere project, NSF award #0403433.

VI. REFERENCES