Challenges in Using of Distributed Wireless Mesh Networks in Emergency Response

B. Braunstein, T. Trimble, R. Mishra, B. S. Manoj, L. Lenert, and R. R. Rao
CalIT2-UCSD, University of California San Diego,
La Jolla, CA 92093-0436
{bbraunstein, ttrimble, ramishra, bsmanoj, llenert, and 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. 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. We observed that though there are several challenges that need to be solved, a WMN is a favorable choice for emergency response networking.

Keywords

Distributed wireless mesh networks, Performance evaluation, routing and topology control.

INTRODUCTION

Distributed Wireless Mesh Network (WMN) is a recently emerged networking paradigm which attracts 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 based emergency medical response application, during a simulated large scale homeland security drill.

NETWORK ARCHITECTURE

The motivation behind a new network architecture for emergency response stems from the fact that traditional wireless ad hoc networks, using a flat network topology, do not scale well enough to support large scale emergency operation and therefore, we propose a distributed and hierarchical 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 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. Here the users, though they appear connected to a regular wireless LAN, connect to a fully distributed WMN. The second plane is the WMN which is formed by UCSD CalMesh (see reference [1]) nodes. The third plane

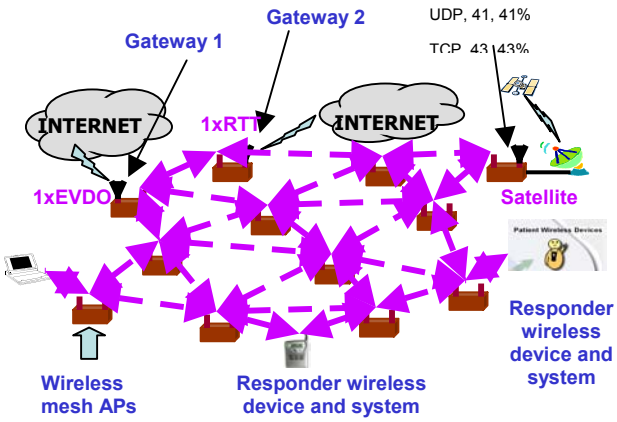

Figure 1. The ENS architecture.

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. 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. 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 medical emergency response application, WIISARD, an information system for providing medical emergency response. WIISARD is a client-server architecture that uses one central server repository and a large number of clients. Figure 2 shows the overall system diagram of WIISARD.
WIISARD system has five main 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 (see reference [2]). It provides visual indications on the patients' health for the first responders. 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 medical 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.

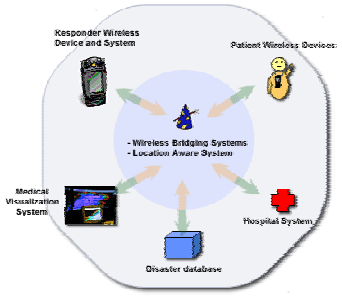

Figure 2. WIISARD system architecture.

Experimental Network Environment

San Diego County held a full scale home land security drill at the DelMar Fair Grounds, San Diego, during November 2005, where the ENS was deployed for the experiment as 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 presented are the zones where the victims are treated and other emergency coordinating activities are taken place. The network deployment topology is expanded 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 is 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. Here the actual network topology not only depends on the placement of nodes but also depends on the specific properties of the terrain.

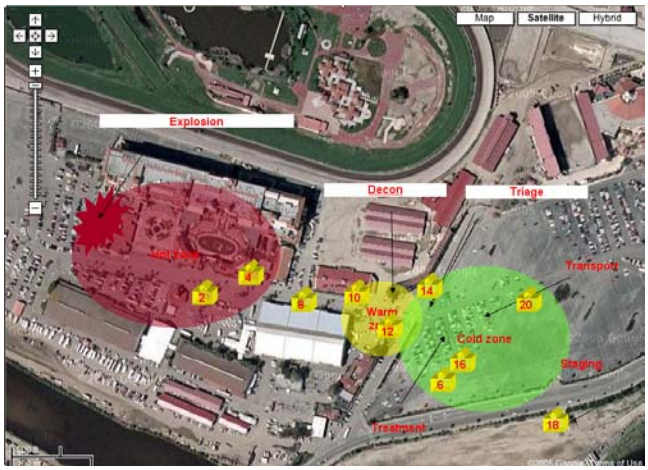

Figure 3. Network environment and ENS deployment.

Network topology and node connectivity

Figure 4 shows the signal strength view of the network from node 2. Note that this view is only from node 2 and there can be an altogether different view from other nodes. Though the nodes 2 and 18 are placed nearly more than a mile apart, the geographical properties of the terrain somehow provided a very weak (-88 dBm) connectivity between those two nodes. However, the use of such weak links leads to a very low link data rate and hence we used a modification of 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 frequency reuse is not the primary objective for utilizing the multihop nature of the WMNs, rather the increase in throughput by using multihop relaying. This is because, 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 would provide a better throughput. This is because at each link, the data rate will be much higher than the direct single hop link. In such case, the routing mechanism that utilizes signal strength based multi-level routing metric achieves better performance. In our experiments, we obtained about 2-3 times increase in throughput when compared to shortest path routing scheme.

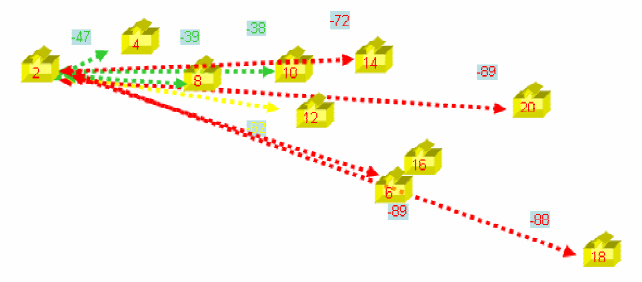

Figure 4. Signal strength view from Node 2.

From the signal strength view from node 2 (Figure 4), we noted that there exists no connectivity between nodes 2 and 16. This is due to the physical obstruction, a building, present in between these two nodes. From node 2, nodes 4, 8, and 10 are reachable with fairly good signal strength (less than -50dBm). Node 12 is reachable over a moderately strong link (less than -65 dBm). The remaining nodes (6, 14, 18, and 20) are reachable over a very weak wireless link (greater than -80 dBm). An important observation noted here is that these link quality parameters are not bidirectional and using these weak links are not useful for getting good network throughput performance. In this situation, our network architecture and routing protocol are designed to force the multihop operation even in the presence of single hop connectivity in order to improve reliability and performance. This is an example of the real situations 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) victims (25 dead and 100 injured) were simulated, (iii) first responders arrived at the scene, (iv) ENS backbone was then deployed, (v) the WIISARD network was deployed, and (vi) network monitoring was turned on when the medical response application uses the network. The network monitoring is done near the node 16 where the central repository of WIISARD system was attached. In this simulated emergency network deployment, the network deployment took about half hour to complete the node placement and operation which was followed by 3-4 hours of emergency response drill.

PERFORMANCE RESULTS AND DISCUSSION

Our experimental setup has collected large number of data packets during the drill and the collection statistics is shown in Table 1 which is self explanatory. The following sections provide detailed traffic observations made on the ENS infrastructure. The behavior of data collected in our setup has been influenced by the design of application as well. 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 tags connected to victims/patients. Therefore, we noted that the first challenge is in designing a system with minimal control overhead. The high control overhead has two implications: (a) high bandwidth consumption by the control packets and (b) increased contention and collision for the data packets in the network. The number of victim tags ranged from 100-120. 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.

Item	Value
Data capture duration	15549.115s
Number of packets	210727
Avg. packets/sec	13.552
Avg. packet size	269.547 bytes
Bytes	56,800,903
Avg. Bytes/sec	3652.999

Table 1

The byte-wise bandwidth share of the total traffic does not scale proportionally to the packet-wise bandwidth share of the respective traffic categories as depicted in Figure 6. 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.

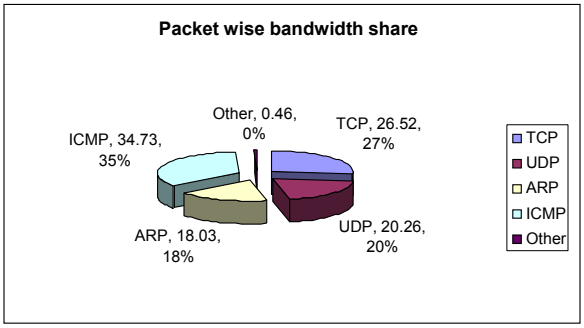

Figure 5. Packet share in the network

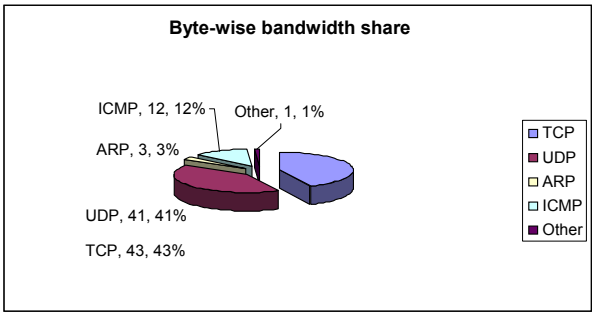

Figure 6. Byte share bandwidth consumed in the network

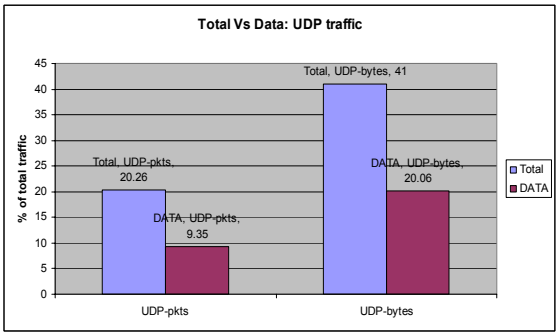

Figure 7. Observed total UDP traffic Vs UDP data traffic

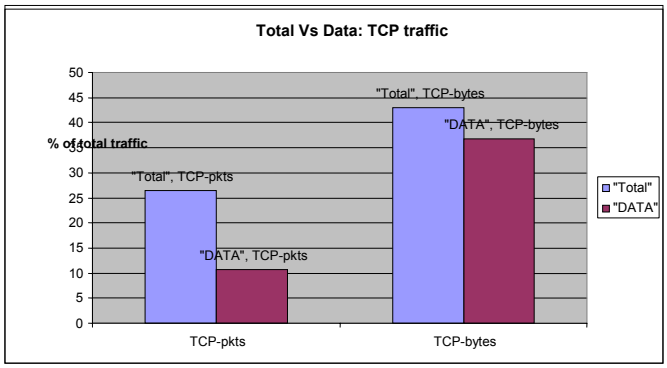

Figure 8. Observed total TCP traffic Vs TCP data traffic

Figure 7 shows the total observed UDP traffic resulting from the WIISARD application on our wireless mesh network. 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%.

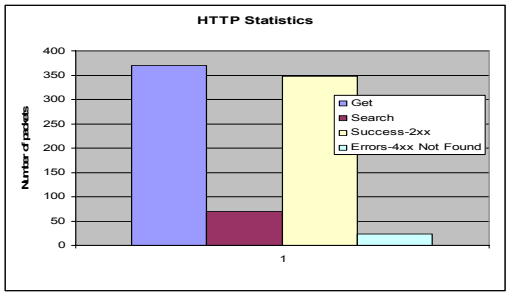

Figure 9. HTTP traffic statistics.

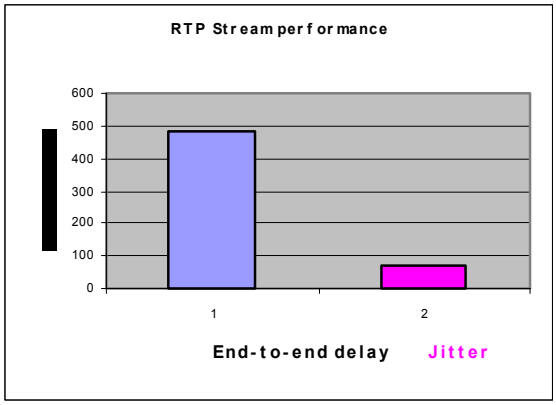

Figure 9. VoIP performance over ENS.

Figure 9 shows the HTTP traffic statistics with majority of the HTTP requests met a success response. Another important type of application traffic in the network was video streaming and we noticed the worst case performance provides an end-to-end delay of less than 500ms. The end-to-end delay jitter remains approximately 50ms. The bandwidth variation for a single video stream is shown in Figure 10 which depicts that the average bandwidth per stream is about 43kbps.

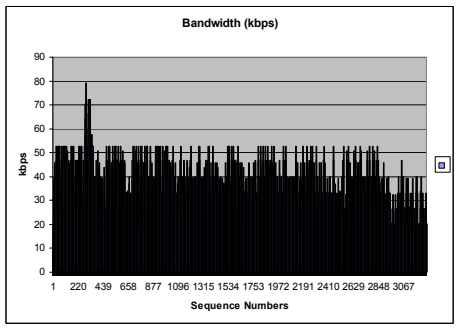

Figure 10. Bandwidth variation on VoIP traffic.

Figure 11 shows the variation of TCP and UDP packet traffic with control traffic such as ICMP and ARP. It shows that the network faces occasional bursts of traffic which peaks a couple of times during our three hour experiment as part of the simulated emergency drill. In addition, the control overhead matched the data traffic at least for 50% of the duration of the experiment. During this drill, our objective was to learn the real network behavior when a near realistic emergency response application was used. Therefore, the network was not subjected for arbitrarily high traffic to conduct a stress test. Later, during our in laboratory experiments, we subjected the network to a throughput stress test during which we noticed higher throughput than what we saw from this drill.

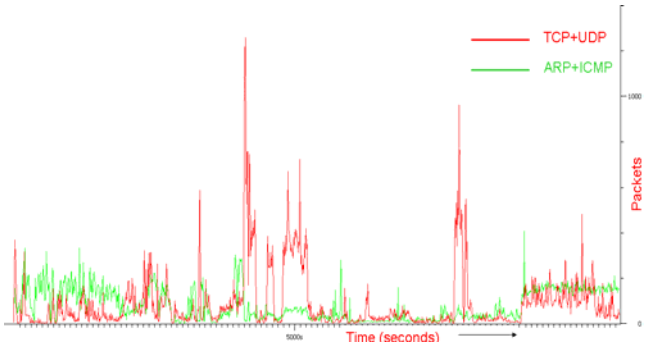

Figure 11. TCP and UDP packet traffic compared to ICMP and ARP packet traffic.

Challenges in using a wireless mesh network for emergency response

From our experiment, we identified the following challenges for emergency networking using wireless mesh networks.

DEPLOYMENT ISSUES: The network deployment is constrained both by time and resources. During our drill, the network deployment took about 30 minutes. Therefore, in most cases, deploying a network with an optimized topology is difficult; rather, optimizing protocol parameters based on the network topology is preferred when using a WMN for emergency networks. Therefore, adaptive topology management and topology-oriented protocols can help enhance the achievable capacity and scalability.

APPLICATION SURVIVABILITY: In our drill at Del Mar, we noticed that the WIISARD system, a client-server design, failed to operate when the network got partitioned. This happened when, for a short while, the network got split into two partitions due to the presence of heavy vehicles such as fire trucks that lead to blocking the line of sight between wireless mesh network nodes. Therefore, the application should consider possibility of network partitioning and thereby utilizing the design approaches on surviving network partitions. One design approach towards a survivable medical emergency response application is to employ a hierarchical client server approach instead of a pure client-server approach.

TIME SENSITIVE TRAFFIC SUPPORT: While high bandwidth communications are important, the network infrastructure for a medical emergency response application must provide support for time sensitive traffic. For example, the pulse-oximeter readings from a victim's sensor node may need to be transported to the central repository for quick response action. In such cases, a coordinated action with support from both network layer and MAC layer need to be made.

ROBUST BACKHAUL CONNECTIVITY: In any disaster site, critical information for management of the disaster resides on computer systems that are on the Internet. Transmission of data offsite, on casualties, resources, and hazards, will be important in coordinating regional response efforts. These requirements make connectivity to the Internet a critical functionality for network solutions. Reliance on any one type of communication backhaul can be risky in a disaster, as the disaster may destroy vital infrastructure. Multiple gateway nodes within the subnetwork increase the robustness of internet connectivity.

BANDWIDTH AGGREGATION AND LOAD BALANCING: When there are multiple gateways supporting a WMN for emergency response, it is essential to aggregate the bandwidth available through each of them. Since the applications that use TCP as the transport layer protocol are sensitive to packet mis-ordering, bandwidth aggregation has to be carefully handled to minimize the packet mis-ordering. An important issue to be considered when using bandwidth aggregation or when using multiple gateways simultaneously is the load balancing across available gateway nodes. This is because, in most cases, the backhaul links are bandwidth constrained and therefore, load balancing can significantly improve the network performance.

NETWORK SURVIVABILITY: While the use of an open spectrum with widely used public networking standard poses certain challenges to secure network operations. The security of 802.11 networks and the understanding of the potential faults are far greater threats for 802.11 than many other protocols. An important aspect of any WMN design is its compatibility with existing tools and algorithms for ensuring network survivability in extreme situations of noise, channel impairments, and potential attacks. Therefore, a WMN design should consider a multi-layer approach to ensure network infrastructure survivability and security in the presence of high interference and potential malicious nodes, respectively. In our case, our network experienced high interference from another video broadcasting source operated by San Diego police. Therefore, the network design must consider operation in the presence of high interference.

CONTROL OVERHEAD: The medical response applications such as WIISARD should focus on designing with minimal control overhead. In our drill, we noticed significant amout of control packets which consumed a large fraction of bandwidth. In situations of large scale crisis, such high overhead may cause network scalabiltiy issues and therefore, response application should particularly be designed for minimal control packet overhead.

CONCLUSION

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 the San Diego county home land security full scale drill and observed the traffic and network behavior when WIISARD, a client-server based medical emergency response application, was used. We presented a detailed traffic and performance observation study in such an environment. We also presented a number of potential challenges identified for further research and study in designing WMN-based emergency networks. In conclusion, we noted that even with the existence of several open challenges, WMNs are good choices for emergency response networking.

ACKNOWLEDGMENTS

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

REFERENCES

1. http://calmesh.calit2.net
2. www.wiisard.org
3. DeCouto, Aguayo, Chambers, B., Morris, R., (2002) Performance of Multihop Wireless Networks: Shortest Path is not Enough, MIT Roofnet Group
4. Draves, R., Padhye, J., Zill, B., (2004) Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks, *Proceedings of ACM, Mobicom 2004*.
5. Adya, A., Bahl, P., Padhye, J., Wolman, A., Zhou, L., (2004) A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks, *Proceedings of IEEE BROADNETS 2004*.
6. www.cwti.net/encinitasmain.htm
7. www.dailywireless.org
8. www.itr-rescue.org
9. www.responsphere.org
10. www.corante.com/mobilemesh