ECE 16:332:544 Communication Networks II

Dr. D. Raychaudhury & Dr. M. Ott

NETWORK ARCHITECTURE PAPER

Rapid deployment emergency infrastructure for a disaster site with multiple types of emergency personnel (police, fire, national guard, etc)

Soumya Das
(Student Id:149-11-7540)
WINLAB, Rutgers University
March 30, 2003

Rapid deployment emergency infrastructure for a disaster site with multiple types of emergency personnel (police, fire, national guard, etc)

Concept for a rapidly deployable network for emergency management

When an emergency occurs such as fire, hurricane, earthquake or terrorist activity, multiple types of emergency personnel are sent to the scene of emergency to perform operations like assess the situation, plan a response, and execute and monitor that response. In order to carry out these 'emergency management functions' [5] and to work remotely from the command headquarters the emergency personnel (police, fire, national guard, medical) have to rely on tools such as electronic mail, document sharing, web and database access to do their jobs. For example in the disaster relief scenario medics would like to retrieve patient history from hospital databases. However in the hours and in some cases days after the emergency, communication is restricted because the existing communication infrastructure may be partially or completely destroyed or the event might occur in an area where there is no existing infrastructure. It is often impossible for the emergency personnel to access remote databases, use web-based applications and communicate with headquarters or interact with personnel in another area of a large-scale disaster (for example using audio/video conferencing). Hence comes the requirement for designing a network that can be deployed rapidly in a disaster site for relief operations.

Features of a rapidly deployable network

There are some unique characteristics for rapidly deployable networks. For example, the components have to be portable and the deployment time is small so that the response time is kept as small as possible.

Characteristics for a rapid deployment network that distinguish it from a traditional (wired) network [5] are:

- Operation is robust in case of wireline technologies due to advance planning, while sub-optimal deployment and a frequently changing environment can decrease reliability of a rapidly deployable network
- Security may be available through limited physical access, encrypted links, or security gateways in wireline technologies. However use of wireless implies the potential for eavesdropping. Key management is difficult in a rapid deployment.
- System designs and deployments are usually highly sensitive to cost per user in wireline technologies. On the other hand, in rapidly deployable networks total system cost is still important, but cost per user is less important.

Requirements of a rapidly deployable network

Applications that are likely to run in a rapidly deployable network for disaster management are as follows:

- Applications such as document sharing and email are loss sensitive but delay tolerant and they generate bursty traffic.

- Web-based applications are delay sensitive due to human interactivity and loss – tolerant. However since the emergency personnel need to access the database for future course of action, this is less loss tolerant than other web access applications. This is characterized by transactional traffic.
- Applications like audio/video conferencing are loss tolerant, delay and delay variance sensitive. Bandwidth requirement is high for audio and relatively low for audio. Both will generate bursty traffic under the conditions specified. Transmission at 384kbps provides a clear and stable picture for scenes with minimal changes in picture content. However when there are major changes in the transmitted picture the quality of the received picture degrades and there is loss of resolution and noticeable blurring.

The number of users in such a network will depend on the type of emergency and the area affected by the emergency. However the number of users will be limited by the capacity of the proposed network. A majority of the users will be mobile in such an environment possibly with a few stationary users. It is desirable to have some QoS for applications like audio/video conferencing. Also reliability should be high in such emergency situations where the future course of action often depends on the communication between the command headquarter and field personnel in the disaster site. High reliability demands authentication but it has already been pointed out that key management is difficult in a rapid deployment scenario.

For audio streaming RTP (Real-Time Streaming Protocol) would be implemented. RTP is based on UDP and it is therefore a non-reliable protocol. It means that prospective lost packets will not be resend. For audio streaming it is not necessary to resend a data packet because of the new packets, which continuously arrive. Furthermore, the overhead of UDP is much smaller than the overhead of TCP. That is an advantage especially for the real-time data transmission.

Types of traffic	**Percentage of users generating traffic**	**Bandwidth requirement for *n* users**
www (web access and database access)	60%	$(n \times 0.6 \times 56) = n \times 33.6$ kbps
ftp	15%	$(n \times 0.15 \times 128) = n \times 19.2$ kbps
smtp	10%	$(n \times 0.1 \times 56) = n \times 5.6$ kbps
video conferencing	20%	$(n \times 0.2 \times 384) = n \times 76.8$ kbps

Table 1: Bandwidth requirement for different traffics

If we assume that there are n users in the system then from the above table we get that the bandwidth requirement is $(n \times 135.2)$ kbps. Here we assume that 100% of the users are

active all the time. If we consider that the number of users in the network is limited by the 11 Mbps 2.4 GHz point-to-point wireless link between the field office and HQ (described later) then the number of users is approximately $11 \times 10^3 \div 135.2 \approx 80$ .However assuming that the multiple hop ad-hoc wireless network has a capacity of 2 Mbps and the node which is forwarding packets is running a video conferencing application along with other applications then bandwidth requirement for this particular user will be $(384 + 56 + 128 + 56) = 624$ kbps. So bandwidth available for forwarding packets of other users is sufficient for 2 users who are also running all the applications. Assuming that a node has to forward 5 % of the total number of nodes' packets in the extreme case, then 5% of the users is equal to 2. This gives the number of users as 40.

Proposed Network

For the requirements listed above, I propose a mobile ad-hoc network (MANET) to be deployed in the disaster site.

An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. There can be different kinds of mobile devices like laptops, PDAs, as well as medical equipment, sensors, actuators, etc. Each node has a wireless access interface for communication and is free to enter or leave network at any time. Due to limited range of their wireless interface, multiple hops may be needed for communication. Since there is no infrastructure, the nodes themselves have to forward packets of other nodes, thus acting as hosts and routers at the same time. The characteristics of mobile ad-hoc wireless networks [10] are:

- Dynamic topology: nodes in the network are mobile and can change their location rapidly causing topology changes
- Limited bandwidth: typical bandwidth is between several hundreds kilobits per second and several megabits per second
- Limited power supply: mobile devices are battery driven so the power supply is limited;
- Limited transmitter range: transmitters in mobile devices typically cover from 10m to few hundred meters range
- Multiple radio hops: due to limited range one hop communications will not be possible between every two devices wishing to communicate, so multiple hops will be used;
- Nodes are both hosts and routers: since there is no infrastructure and multiple radio hops are used each node has to forward packets coming from other nodes to their destination.

These networks are useful for rescue operations after earthquake or other types of disaster in which a need for communication exists, but infrastructure does not or has been destroyed.

Each node in an ad-hoc network participates in an ad hoc routing protocol that allows it to discover "multi-hop" paths through the network to any other node. The idea of ad hoc networking is sometimes also called *infrastructureless networking*, since the mobile nodes in the network dynamically establish routing among themselves to form their own network "on the fly."

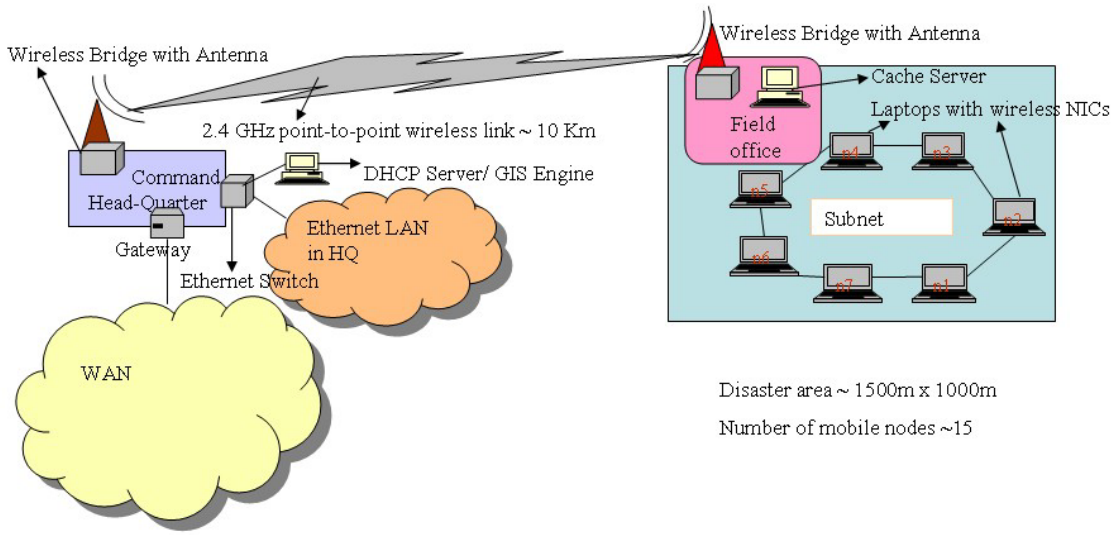

Fig 1: High level diagram of the proposed network

Fig 1 is a high level network diagram of the proposed rapidly deployable network. In the figure n1-n7 are the mobile nodes which represent the mobile emergency personnel (fire tenders or ambulances moving within the disaster site or to the field office). The number of mobile nodes is 40. The field office is the stationary node which is located within the disaster site. The mobile nodes and field office communicate with each other using the 2.4GHz Wireless LAN thus forming an ad-hoc mobile network. Due to limited range of the wireless interfaces of the mobile nodes, multiple hops may be needed for communication and the intermediate nodes have to forward the packets. Also there are a few forwarding nodes in the disaster site, their total number being 14. There is a cache server in the field office where frequently accessed web sites and databases are cached and the mobile nodes can access it. The field office is connected to the Command Head-Quarter (HQ) by a long distance point-to-point wireless. The point-to-point link between the field office and HQ does not interfere with the radio interfaces of the mobile (or fixed) nodes. The HQ is connected to existing telecommunications infrastructure, for example via an existing 100 Mbps Ethernet. The field office also has a GPS Reference Station which sends GPS corrections to nodes in the ad-hoc network. The HQ has GIS

engines to provide rapid resource estimation and the ability to recommend relocation of the remote units. Emergency management personnel in the disaster site can use standard GIS applications in the field and access databases or GIS engines in HQ.

The mobile nodes can each be implemented using an IBM ThinkPad and a GPS unit. They will also carry an 802.11b NIC (Agere ORiNOCO NIC). The silver PC card is used and it comes with the Wired Equivalent Privacy (WEP) security using a 64 bit key. It plugs into the laptop type II PCMCIA slot. To enable the moving nodes to determine their location, each of them carry a Trimble 7400 GPS receiver with GPS antenna. For video conferencing applications the mobile nodes will also carry Logitech Quickcam Pro 4000 web cameras. The field office has a CISCO Aironet 350 Multifunction Wireless Bridge. It can support 11 Mbps data rate and has a maximum range of 18 miles (29 Km approximately). The Aironet 350 Multifunction Bridge will operate in point-to-point mode with another CISCO Aironet 350 Multifunction Bridge in the HQ. The Aironet Bridges will use a CISCO 21 dBi solid dish omni directional antenna AIR-ANT3338. Its approximate range at 11 Mbps is 11.5 miles (18.5 km) and at 2 Mbps is 25 miles (40 Km). Its diameter is 24 inches and weight is 11 lbs (5 kg) and is suitable for outdoor medium/long-range directional connections.

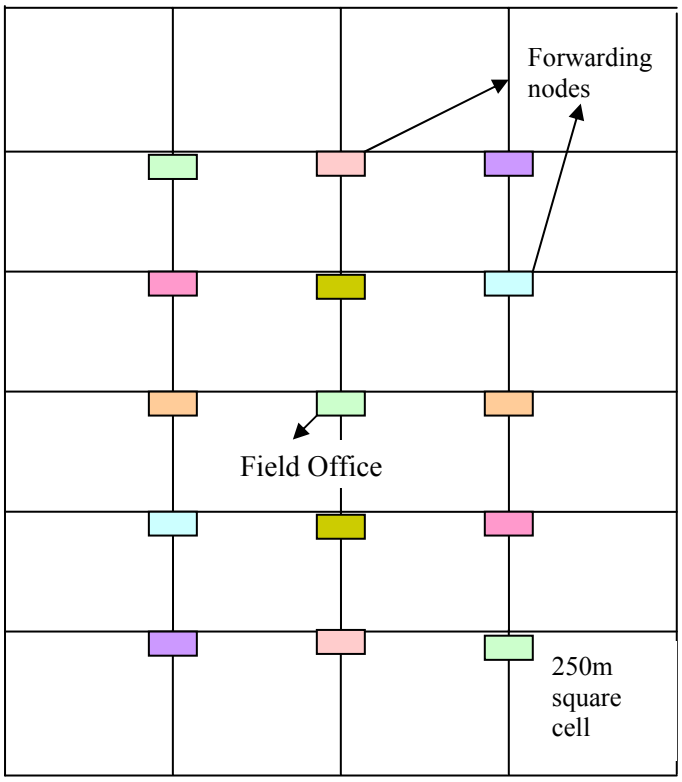

Fig 2: Rectangular grid representing the disaster area and position of forwarding nodes

The rapidly deployable network which I propose will serve a geographical area of about 1500m x 1000m. It is assumed that the range of the radios of the mobile nodes is approximately 250m and the nominal channel capacity is 2Mbps. Considering the disaster area to be a rectangular area it can be divided into square cells with sides 250m. Then there will be $6 \times 4 = 24$ cells and to cover the whole disaster area the number of forwarding nodes required will be $(6-1) \times (4-1) - 1 = 5 \times 3 - 1 = 15 - 1 = 14$.

The above configuration is very similar to the scenario when the HQ represents a Tactical Operations Center in military operations, the field camp a battlefield command post and the mobile nodes a convoy of trucks carrying ammunitions. Similarly in a civil disaster relief scenario, the HQ and field camp can represent the regional and local command centers and the mobile nodes could be ambulances or fire tenders moving within the disaster site.

Network Architecture for the proposed network

The OSI (Open Systems Interconnection) Reference Model is a standard reference model for communication between two end users in a network. The model is called ISO OSI Reference Model because it deals with connecting open systems - that is, systems that are open for communication with other systems

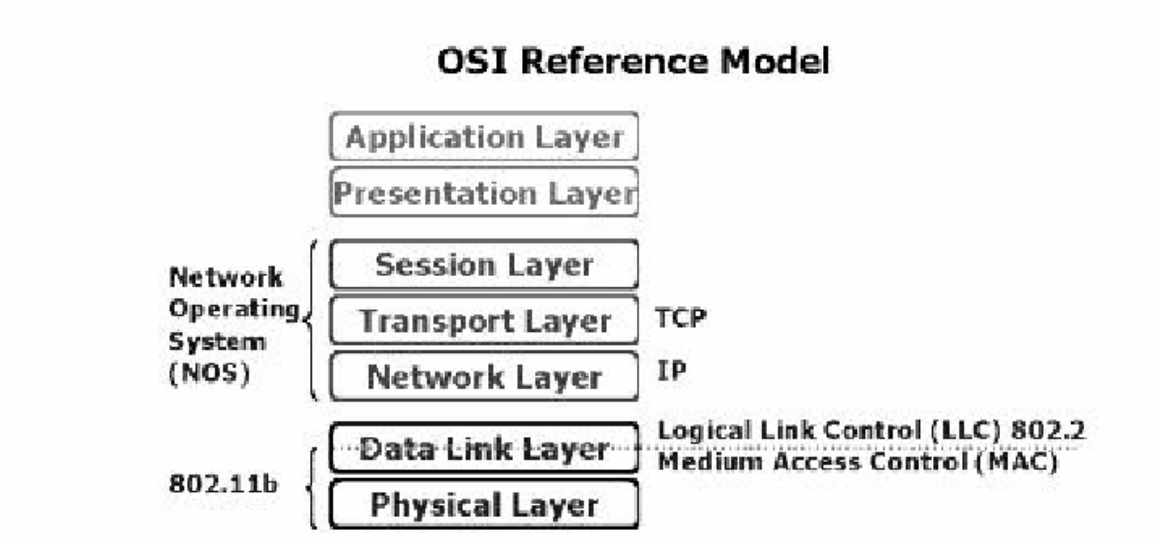

Fig 3: 7 Layer OSI Reference Model

Physical Layer (PHY) and Media Access Control Layer (MAC)

The IEEE 802.11b standard defines only the bottom two layers of the OSI reference model, the Physical Layer and Data Link Layer (MAC sub-layer). The 802.11b physical layer (PHY) is the interface between the MAC and the wireless media where frames are transmitted and received. 802.11b defines 11 Mbps and 5.5 Mbps data rates (in addition

to the 1 and 2Mbps rates) utilizing an extension to DSSS called High Rate DSSS using 11-bit chipping sequence (HR/DSSS).

The 802.11b MAC layer provides functionality to allow reliable data delivery for the upper layers over the wireless PHY media. The 802.11 MAC provides a controlled access method to the shared wireless media called *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA).Security is provided by the authentication services and by *Wireless Equivalent Privacy* (WEP), which is an encryption service for data delivered on the WLAN.

Routing Protocol in the proposed rapidly deployable network

There are a number of multi-hop ad hoc wireless network routing protocols: Destination-Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), and Ad Hoc On-Demand Distance Vector (AODV). Of these the first one is a proactive protocol while the other two are reactive protocols. As reactive protocols adapt to increased mobility i.e. topology changes better than proactive protocols, in the proposed network AODV-LL (link layer) [4] a variant of AODV will be implemented, as the routing protocol. AODV-LL uses *only* link layer feedback from 802.11 as in DSR, completely eliminating the standard AODV HELLO mechanism thereby reducing the packet overhead.

Basic Mechanism of Ad Hoc On-Demand Distance Vector (AODV)

AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV.

When a node S needs a route to some destination D, it broadcasts a ROUTE REQUEST message to its neighbors, including the last known sequence number for that destination. The ROUTE REQUEST is flooded in a controlled manner through the network until it reaches a node that has a route to the destination. Each node that forwards the ROUTE REQUEST creates a *reverse route* for itself back to node S. When the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPLY that contains the number of hops necessary to reach D and the sequence number for D most recently seen by the node generating the REPLY. Each node that participates in forwarding this REPLY back toward the originator of the ROUTE REQUEST (node S), creates a *forward route* to D. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing. In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbor is taken as an indication that the link to the neighbor in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbors. When a link goes down, any upstream node that has recently forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPLY containing an infinite metric for

that destination. Upon receipt of such a ROUTE REPLY, a node must acquire a new route to the destination using Route Discovery as described above.

Assignment of IP address to nodes in the disaster area

In traditional networks, hosts rely on centralized servers like DHCP for configuration, but this cannot be extended to MANETs because of their distributed and dynamic nature. Many schemes have been proposed to solve this problem. Some of these approaches try to extend the IPv6 stateless auto configuration mechanism to MANETs, some use flooding the entire network to come up with a unique IP address, and others distribute IP addresses among nodes (using binary split) so that each node can independently configure new nodes. In the proposed rapidly deployable network, the problem of configuration can be simplified by assigning fixed IP addresses (within a single subnet) to each node in the ad-hoc network beforehand. This seems rational because the number of nodes in the network is already known.

Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is the most prevalently used transport protocol on the Internet. Most current network applications that require reliable transmission use TCP as their transport protocol. However TCP is not entirely suitable for wireless ad hoc networks due to the inappropriateness of TCP congestion control schemes. The TCP sender concludes that there is network congestion upon detecting packet losses or at time-outs. However, in wireless ad hoc networks, links are often broken as a result of node mobility and hence some time is needed to perform route reconfiguration. During this time, packets could be lost or held back. Hence, the TCP sender could mistake this event as congestion, which is untrue. A route disconnection should be handled differently from network congestion. TCP performance can be improved in a wireless ad hoc network where each node can buffer ongoing packets during a route disconnection and re-establishment. In addition to distinguishing network congestion from route disconnection due to node mobility, new measures can also be incorporated to deal with reliable transmission of important control messages and exploitation of TCP fast recovery procedures. There are a few variants of TCP that can handle the above-mentioned problem viz., TCP implementations (Tahoe, Reno, New-Reno, and SACK).

Protocol stacks used in the rapidly deployable network

The protocol stacks at the different components of the rapidly deployable network are shown in the following diagram. For the field office, AODV has been used as a virtual interface residing below the IP layer in order to abstract mobility from the normal protocol stack.

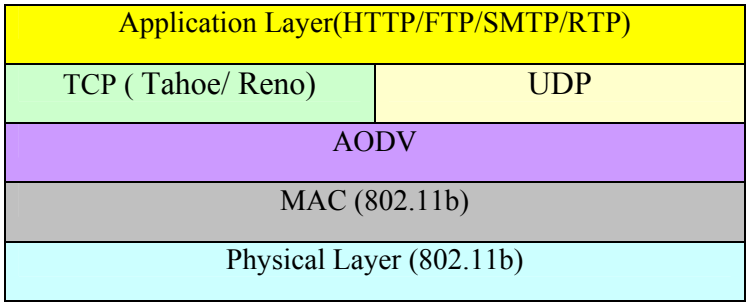

Fig 4a: Protocol Stack at the mobile nodes in the disaster area

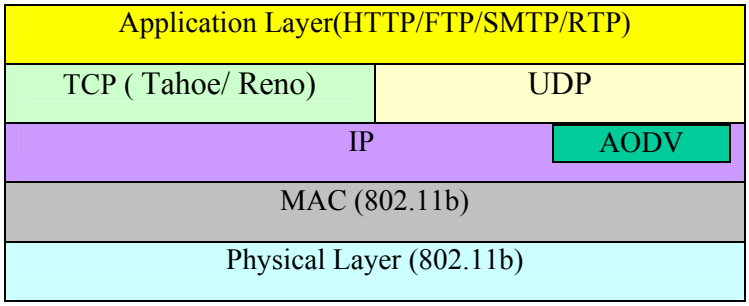

Fig 4b: Protocol Stack at the Cache Server in the field office

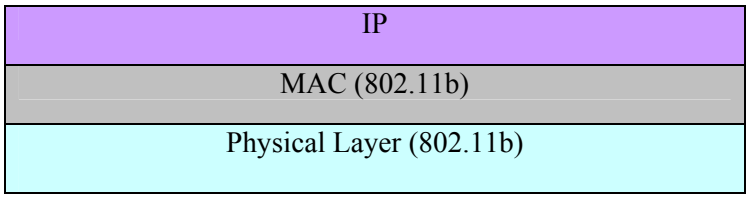

Fig 4c: Protocol Stack at the wireless bridges in the field office and HQ

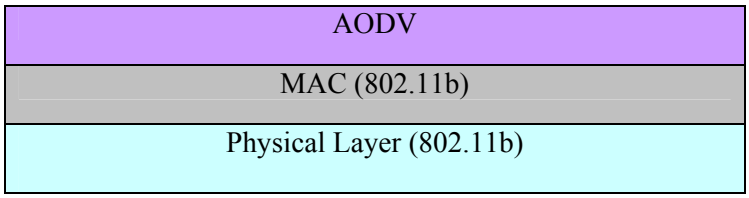

Fig 4d: Protocol Stack at the forwarding nodes in the disaster site

Application Layer(HTTP/FTP/SMTP/RTP)	
TCP	UDP
IP	DHCP
MAC (802.3)	
Physical Layer (802.3)	

Fig 4e: Protocol Stack at the DHCP Server (GIS Engine) of the central head-quarter

Performance and Cost Evaluation

Quality of service (QoS): When building QoS support into mobile ad-hoc networks the mechanisms should consume minimal bandwidth in operation and react promptly to changes in the network-state i.e. changes in network topology. The following are a few of the quantitative metrics that must be taken care of for this particular scenario:
a) High end-to-end data throughput.
b) Low latency.
c) Low route acquisition time.

The performance of the proposed rapidly deployable network can be measured by the ability of the protocol stack to react to network topology change and a variety of workload while continuing to successfully deliver data packets to their destinations. The performance of the proposed network can be simulated on 'ns2' by varying parameters like speed of mobile nodes, sizes of packets, number of users and the amount of traffic in the network. In the short time frame for this network architecture project, I have not been able to simulate this environment in 'ns2'. However I plan to do the same in future.

The performance of the network may be evaluated according to the following metrics:

- *Packet delivery ratio*: The ratio between the number of packets originated by the "application layer" and the number of packets received at the final destination affects the maximum throughput that the network can support.

- *Routing overhead*: The total number of routing packets transmitted during the simulation measures the scalability of a protocol and the degree to which it will function in congested or low-bandwidth environments, and its efficiency in terms of consuming node battery power.

Cost of the proposed network

Components	Cost per unit	No. of units	Total Component Cost
Cache Server	$1,000	1	$1,000
Forwarding Nodes	$300	14	$4,200
Agere ORiNOCO NIC (silver PC card)	$39.72	40	$1,588.80
Logitech QuickCam Pro 4000	$76.00	40	$3,040
Cisco Aironet 350 Series Multifunction Bridges	$462.95	2	$925.9
CISCO 21 dBi solid dish antenna AIR-ANT3338	$669.79	2	$1,339.58
Total cost of proposed network			$12094.28

Table 2: Cost evaluation of the proposed network (* does not include the cost of Trimble 7400 GPS Receiver)

Annual recurrence maintenance cost would be roughly 10% of the initial set up cost. So annual recurrence maintenance cost is $1210. With 40 emergency personnel in the disaster area, and assuming the rapidly deployable network to be deployed once a year, the cost per user per year becomes $30.25.

Conclusion and Further Work

The network I have proposed is simple and consists of a number of mobile nodes (40), a stationary field office and a number of forwarding nodes (14) which form a multiple-hop ad-hoc wireless network. Packets are routed between these nodes using AODV protocol. The field office has a point-to-point wireless link with the head-quarter. There is a wireless bridge (with solid dish antenna) at both the ends of the point-to-point wireless link. The proposed network seamlessly integrates with the outside world via the wireless bridge at the head-quarter. An interesting aspect to look into would be the scalability factor in such rapidly deployable emergency infrastructure which is dependent on the equipments that support long-range outdoor wireless communication. The MAC and link layer protocols may have to be modified because 802.11 MAC is not suitable for long distance wireless link because RTS/CTS only add one more round trip delay and career sensing is not of much use.

Designing rapidly deployable networks for military or civil disaster relief operations has been receiving increasing attention from researchers in the last few years and a number of works are going on in this direction. MANET Technology when suitably combined with satellite based information delivery can provide an extremely flexible method for establishing communications for fire/safety/rescue operations and other scenarios that require rapidly deployable networks [2]. Satellites offer a method of long distance communication when other means such as land line or cellular telephone service are

either non existent or have been destroyed by disaster. Satellite communication in such a case requires use of an array of multiple non-geostationary satellites in Low Earth Orbit (LEO). Since LEO satellites are much closer to Earth than geostationary satellites, power requirements are reduced and hand held terminals about the size and weight of portable cellular telephones are adequate for communicating via satellite. In the context of disaster communication, portable communication via satellite could offer immediate communications for disaster responders, regardless of the severity and magnitude of the surrounding damage.

The utility of such devices had been demonstrated in the wake of Taiwan's worst earthquake in 1999 when portable LEO phones were used to support search and rescue efforts in areas most affected by the Earthquake. The system, capable of operating independently of local terrestrial infrastructure, was the only communications system to be unaffected by this earthquake which caused a major power and telephone exchange outage.

Researchers in University of Kansas have developed a prototype for a Rapidly Deployable Radio Network (RDRN) [12] which is an ATM based support for data communications over established point-to-point links.

Researchers of Center for Wireless Telecommunications (CWT), Virginia Tech [11] have proposed another solution. They have developed a small prototype system for emergency relief operations. The system comprises of a base station and two field units which are built around commercial Local Multipoint Distribution Service (LMDS) equipment.

References

[1]Experiences Designing and Building a Multi-Hop Wireless Ad Hoc Network Test bed-Maltz, D., Broch, J., Johnson, D., CMU School of Computer Science Technical Report, CMU-CS-99-116, March 1999.

[2]Communications and Information Tools for the 21st Century: Changing the Face of Disaster Response and Humanitarian Assistance - Victoria Garshnek, Frederick M. Burkle, Jr.

[3]Autonomous Tactical Communications Possibilities and Problems- Lars Ahlin, Eva Englund ,Christian Jönsson, Ingrid Söderquist , Jens Zander, Gerald Q. Maguire

[4]A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols - Josh Broch, David A. Maltz, David B. Johnson, Yih Chun Hu, Jorjeta Jetcheva - Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98), October 25–30, 1998, Dallas, Texas, USA. Copyright 1998 ACM

[5]Rapidly Deployable Broadband Wireless Communications For Emergency Management-Scott F. Midkiff, Charles W. Bostian- Center for Wireless Telecommunication, Virginia Polytechnic Institute and State University

[6]Lecture Notes of ECE544: Communication Networks II, Rutgers University – Dr. D Raychaudhury, Dr. Max Ott

[7]IEEE 802.11 Wireless LAN Specs (http://standards.ieee.org/getieee802/802.11.html)

[8]IP address assignment in a mobile ad hoc network- Mansoor Mohsin, Ravi Prakash, The University of Texas at Dallas

[9]Internet Draft- Ad Hoc Address Auto configuration - Perkins, et. al (MANET mail archive)

[10]Ad-hoc networking- C. Perkins, Wiley & Sons, 2000

[11]Demonstrating Rapidly Deployable Broadband Wireless Communications for Emergency Management - Charles W. Bostian, Scott F. Midkiff, Center for Wireless Telecommunications, Virginia Tech - Presented at the National Digital Government Research Conference (2002)

[12]RDRN: A Prototype for a Rapidly Deployable Radio Network-Ricardo J. S´anchez, Joseph B. Evans, Gary J. Minden, Victor S. Frost, K. Sam Shanmugan - Information and Telecommunication Technology Center, Department of Electrical Engineering & Computer Science ,University of Kansas

[13]Internet Engineering Task Force (IETF) MANET working group (http://www.ietf.org/html.charters/manetcharter.html)

[14]Computer Networks-A Systems Approach- Larry L. Peterson, Bruce S. Davie Morgan Kaufmann 1996