DESIGN AND IMPLIMENTATION OF A NETWORK TOOL: A STUDY

Vashu Kumar, Nirbhay Ahlawat and Manish Kumar Chauhan

Dept. of Computer Science Engineering,
Phonics Group of Institutions, Roorkee, Haridwar, Uttarakhand, India.
Corresponding author – vashu.narwal3@gmail.com

Objectives

The objective of this thesis is to get the deep understanding of wireless mesh networks and the routing protocols that can be used in it. Routing protocols in WMNs should be evaluated theoretically as well as through simulation to see which protocol gives best performance with reference to certain parameters. It is needed to analyze the results in the form of graphs that are obtained after the simulation. Initially in this thesis, all the necessary topics like wireless mesh networks, routing protocols and other relating material for these two topics are studied and discussed theoretically. After this the routing protocols are implemented in wireless mesh network, keeping in mind the conditions (traffic pattern, mobility rate, mesh node density and traffic load), through a simulation environment. This thesis also had a plus point that it could give the future researchers a clear idea that the routing protocols can be tested for other criteria also using this kind of simulation, and this could be of great interest for research in the field of wireless mesh networks. Aim of this thesis is to performance evaluate a suitable routing protocol for WMNs and to explore the area of applicability of such networks with different mobility models and mobility rates. Also this work provides general understanding of wireless networks and routing protocols and generates a simulation environment that could be used for further studies. **(INTERNATIONAL JOURNAL OF HIGHER EDUCATION AND RESEARCH, 5(2), 36-59, 2015).**

1.1 Overview

Wireless communication has an enormous use these days and is still becoming popular from times immemorial. This is because of the latest technological demands now a day's arising from laptops, wireless devices such as wireless local area networks (WLANs), etc. Because of its fast growing popularity day by day, it has led wireless communication data rates higher and prices cheaper. That is why wireless communication is growing so fast. Wireless communication can work between hosts by two methods; first is to allow the existing network carry data and voice, and second is to make ad hoc network so that hosts can communicate with each other [1]. Wireless Mesh Networks (WMNs) are one of the types of ad hoc networks. Ad hoc networks are also called as mobile ad hoc networks (MANETs). Companies use wireless mesh networks for making large coverage area of wireless local area networks. WMNs are the latest technology that has lot of things in common with MANETs. Basically WMNs are consisted of wireless nodes; each node with its own packet, these nodes can communicate with each other by forwarding the packets to one another. This is very similar to MANETs; each node acts as a host and a router, which is basically a wireless router. In WMNs, if clients want to communicate with routers, they use the networking interfaces like Ethernet 802.11 and Bluetooth. There are some cases when WMNs router lies inside the network card, then clients can use the networking interfaces like peripheral component interconnect (PCI) or personal computer memory card international association (PCMCIA) bus, for the sake of communication. WMN nodes can provide internet connectivity and these nodes are termed as gateways. There are lot of advantages of WMNs over different other technologies, one of them is its least deployment time and other includes reliability and market coverage [2]. Different companies like Nokia, Motorola, Ericson, and Siemens etc have great trust in WMNs technology as it provides full IP solution [3]. Because of the fast developments in the field of wireless communication (laptops and PDAs) the demand for getting internet access from anywhere, anytime has increased. Wireless stations are the current technology that can provide internet to wireless devices by making a route between them. These wireless stations are so called access points. Network is created by access points among wireless devices and provides a bridge between internet and this network. Access points have some coverage area; this coverage area can be extended by allowing wireless devices to pass packets towards access points. This kind of multi-hop wireless access networks are called WMNs [4]. Routing protocols have great importance in WMNs. Without routing protocols WMNs cannot be implemented. Routing protocols help routers in a network to know how they can communicate with each other. They work on the third layer of the Open System Interconnection (OSI). They prevent routing loops and select preferred routes. Routing protocols might encounter certain parameters during the communication process such as packet delivery ratio, throughput, latency and network load in WMNs which must be optimized. Researchers have been working on this issue, finding and developing a suitable and efficient protocol that can give best performance with respect to these parameters under certain conditions. Currently there does not exist any standard for a routing protocol for ad hoc networks, instead this work is in progress. Many problems remain to be solved before any standard can be determined. This thesis looks at some of these problems and tries to evaluate some of the currently proposed protocols for ad hoc networks in wireless mesh networks.

LITERATURE SURVEY

This chapter is a survey about the wireless technologies that allows us to have self-configured and self-organized networks. This chapter highlights the design factors, architectures, characteristics and the advantages of the self configured networks. Also a comparison between WMN and MANET is presented in this chapter. Application domain of WMN is discussed in the end of the chapter.

2.1 Wireless Networks

One of the most promising and discussed technologies in the last decade is the wireless technology which allows users to utilize devices that enable the access to information at any time any place. These needs make wireless networks the best solution for interconnecting devices and people. Unlike wired networks, which are comprised of devices that can communicate through wires, wireless networks are comprised of devices that communicate through media such as radio signals and infra-red. Wireless networks are generally classified into two categories: infrastructure-based and ad hoc wireless networks.

Infrastructure-based wireless network consists of base stations localized in convenient places, which provide wireless connectivity to devices within their coverage area. Such devices that provide wireless connectivity are called as access points (AP). Examples of this category are Wireless Local Area Networks (WLANs) and cellular networks. A WLAN is a flexible data communication system implemented as an extension to a wired LAN within a building or a campus.

On the other hand, ad hoc wireless networks do not have a pre-established infrastructure. Moreover, nodes connect to each other through automatic configuration when they are in transmission range and willing to forward data for other nodes. In this way, an ad hoc wireless network is formed which is both flexible and powerful. Therefore, these capabilities make wireless ad hoc networks suitable for many applications where one central node may not be convenient, and where minimal configuration and quick deployment is required in emergency situations. Wireless ad hoc networks can be further classified by their application in mobile ad hoc networks, wireless sensor networks, and wireless mesh networks [5].

2.2 The IEEE 802.11

In this section I present the basics of the IEEE 802.11 standard that specify the wireless communication. 802.11 specifies the physical and medium access layer adapted to the special requirements of wireless networks but offers same interface as the other standards to higher layers to maintain interoperability [6]. Many concepts and definitions are needed in order to better understand the standard. The specifications details can be found in [7].

2.2.1 IEEE 802.11 Architectures

The IEEE 802.11 architecture comprises several components and services that interact to provide wireless communication to stations which are any devices that incorporates the functionality of the IEEE 802.11 protocol and can connect to the wireless media. The IEEE 802.11 standard specifies three primary setups. The first setup is a Basic Service Set (BSS), which is defined as a group of stations that communicates with each other in a geographical area known as Basic Service Area (BSA). When these stations can communicate without the aid of an infrastructure network, they are referred to as an Independent Basic Service Set (IBSS) which is the formal name of an ad hoc network in the IEEE 802.11 standard. These stations operate in the “ad hoc mode” because they communicate directly with another station in their transmission range.

In comparison, in the "infrastructure mode", a station in a BSS communicates with another through a Base Station (BS) which is also called Access Point (AP) if it is connected to a wired network. The BSS operating with a BS is known as the Infrastructure Basic Service (IBS).

In addition, another setup known as Extended Service Set (ESS) can be formed. In this setup, BSs (or APs) provide the integration points for network connectivity among different BSSs. Therefore, a network backbone, also known as distribution system (DS), is formed. The DS is responsible for MAC level transport of MAC data units, and is implementation independent meaning that the DS could be a wired Local area network (LAN), Metropolitan area network (MAN), or another IEEE 802.11 wireless medium. In the infrastructure mode, a station needs to join a BSS to communicate. It obtains synchronization information from periodic beacons from the BS. It can either obtain this information by requesting it from the BS (active probing), or it can wait for the periodic beacon from the BS. Before being able to send and receive data, the station has to go through an authentication and association process. The IEEE 802.11 standard not only defines a Medium Access Control (MAC), but also the related management protocols and services, and the physical layer. Also, important timing intervals are specified by the standard and they are:

- Short Inter-frame space (SIFS): It is the shortest time interval. It is used between a frame and its acknowledgment. It is long enough for the sender to switch to the receiver mode.
- Slot time (Slot): A little longer than SIFS, it is the basic time unit for the binary exponential back-off algorithm spelled out in the standard.
- PCF inter-frame space (PIFS): It is equal to the SIFS plus one Slot. It is used by the Point Coordinator to get higher priority in accessing the medium.
- Distributed inter-frame space (DIFS): It is equal to the SIFS plus two Slots. It is used before starting a new transmission.

2.2.2 The Distributed Coordination Function (DCF)

The IEEE 802.11 MAC layer offers two types of service, the Distributed Coordination Function (DCF), and the Point Coordination Function (PCF). The DCF protocol allows stations to access the medium in a distributed manner. There is no central entity controlling the use of the shared channel. The DCF defines two access mechanisms: The Basic Access and the RTS/CTS.

2.2.2.1 Basic Access Mechanism

The Basic Access scheme is carrier sense multiple access with collision avoidance (CSMA/CA). When the MAC needs to transmit a frame, it physically senses the medium to check its status. If the medium is free, the station waits for an interval of DIFS to check that the medium remains free. If it is still free, the station sends its frame. Otherwise, the MAC selects a back-off value randomly from a contention window. Figure 2.1 shows this scheme. If a collision happens, the contention window is set to twice its size and a back-off value is chosen from the new interval. After a successful transmission, the contention window is reset to a pre-set minimum value. The random back-off is also called after each successful transmission and each retransmission to reduce probability of collisions. The IEEE 802.11 MAC uses a positive acknowledgment scheme to detect collisions. Each unicast frame sent by the MAC has to be acknowledged by the receiver; otherwise the frame is retransmitted by the MAC layer. Broadcast packets are not acknowledged. Also, retransmissions are limited to a maximum number of tries, after which a packet is dropped.

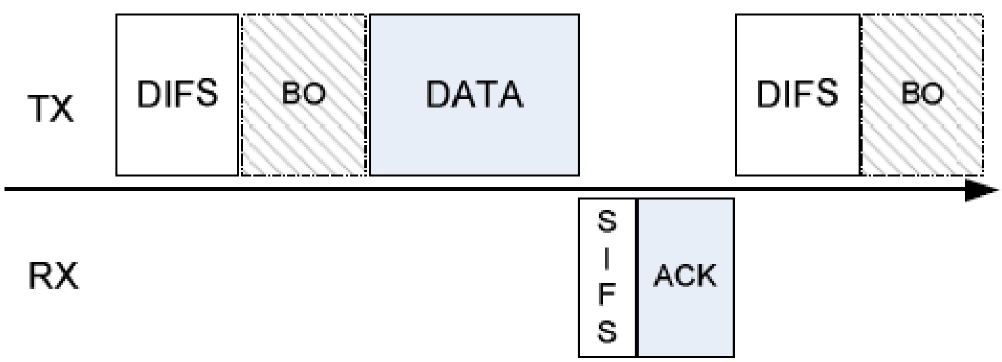

Figure-2.1 IEEE 802.11 DCF Basic Access Mechanism

2.2.2.2 The RTS/CTS Mechanism

In a wireless network, the sender node can not detect a collision because it occurs at the receiver side. When a packet collides at the receiver, the whole packet still needs to be transmitted and then retransmitted if an acknowledgment packet is not received. In addition, stations in the receiver's surrounding may not sense a transmission from the sender. If any of these stations transmits, there will be a collision at the receiver. This is referred to as the Hidden Terminal problem.

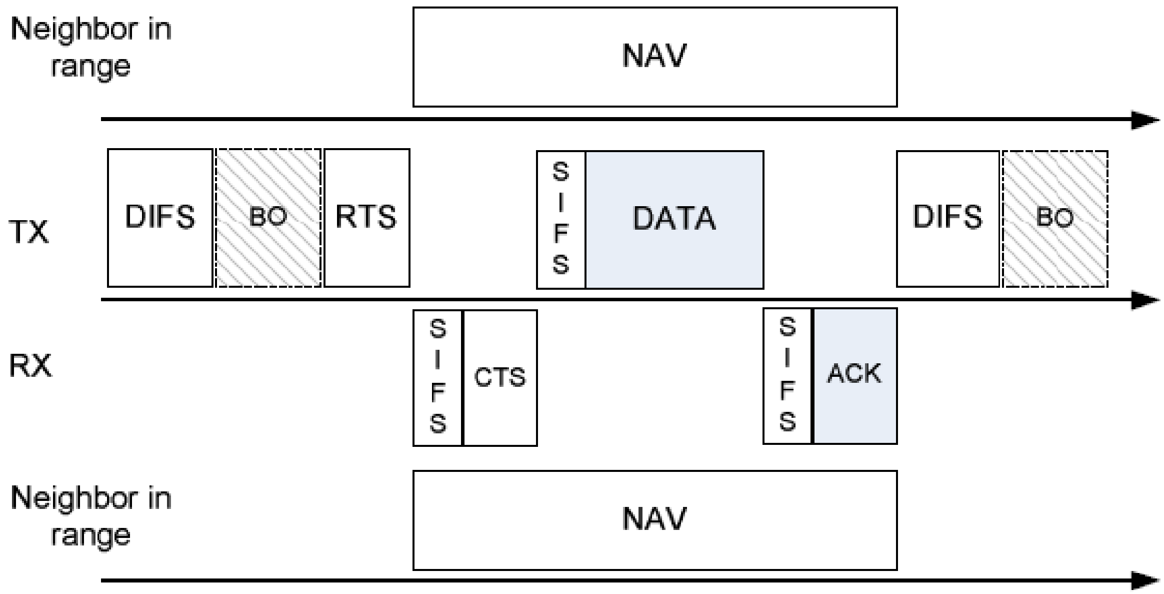

Figure-2.2 IEEE 802.11 DCF RTS/CTS Access Mechanism

To overcome this issue and enable faster collision detection, the MAC specifies a prior hand-shake. Whenever a station has data to send, it first sends a Request to Send (RTS) frame. The destination replies with a Clear to Send (CTS) frame. These two frames contain information about the duration of the next data frames. All neighbor stations hearing these frames set a variable called Network Allocation Vector (NAV) to keep track of the availability of the medium. Checking the NAV before a transmission is also called a Virtual Carrier Sense mechanism. This protocol is depicted in Figure-2.2.

2.3 Multi-Hop Wireless Networks

The Multi-hop Wireless Networks consist of wireless networks that primarily use multi-hop wireless relaying. The major categories in the multi-hop wireless networks are:

- Ad hoc wireless networks
- Wireless sensor networks
- Hybrid wireless networks
- Wireless mesh networks [8].

In the following subsections, we briefly describe the first three categories, and mainly focus on WMNs. Figure-2.3 shows a classification of multi-hop wireless networks.

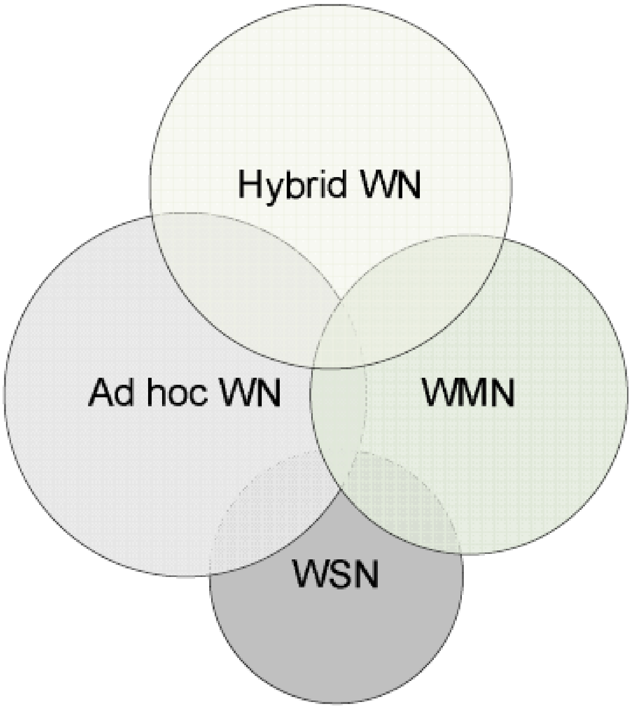

Figure-2.3 Multi-Hop Wireless Network Classification

2.3.1 Mobile Ad Hoc Networks (MANET)

In a MANET, devices are mobile nodes which provide the functionality required to connect users allowing them to exchange information in an environment with no pre-established infrastructure. Therefore, MANET is an infrastructure-less network with highly dynamic topology. Devices are free to move randomly and organize themselves arbitrarily; thus, the wireless network topology may change quickly and unpredictably. Also, some devices may be connected to other resources such as the Internet, file servers, etc., allowing users to gain access to these resources. In the past, these networks have been used for tactical network related applications in battlefield communications and survivability [9]. Military operations generally cannot rely on a fixed communication infrastructure, then MANET allows a suitable framework to overcome issues that radio signals and radio frequency present. In general, MANET also has problems due to wireless communication and wireless networks such as limited transmission range, hidden and exposed terminal problems etc.

2.3.2 Wireless Sensor Networks (WSN)

Wireless sensor networks are formed by spatially distributed tiny sensor nodes that cooperatively can gather and monitor physical parameters or environmental conditions and transmit to a central monitoring node. In addition, sensor nodes are equipped with a radio transceiver or other wireless communication device, a small microcontroller, and usually a battery as an energy source. WSN can use either single-hop wireless communication or a multi-hop wireless relaying [8]. At first, military application was the motivation for developing WSN. Currently, WSN are used in civilian applications such as environmental and habitat monitoring, traffic control, healthcare applications, home automation, etc.

2.3.3 Hybrid Wireless Networks (HWN)

A Hybrid wireless network is an ad hoc wireless network that contains a sparse wired network of base stations. The resulting network comprises regular nodes and wired connected base stations. In this way, we could have a traditional cellular network and an ad hoc network mixed together. The cellular network is an infrastructure based network where data is forwarded through its infrastructure. Here, base stations, unlike normal nodes, are neither data sources nor data receivers, but as relay nodes, they only engage routing and forwarding data for normal nodes. On the other hand, in an ad hoc network, nodes forward data in a multi-hop fashion [10]. Therefore, hybrid wireless networks utilize both single and multi-hop communications simultaneously within the traditionally single-hop wireless networks [8].

2.3.4 Wireless Mesh Networks (WMN)

Wireless Mesh Network (WMN) is a highly promising technology and it plays as an important architecture for the future wireless communications [1]. WMNs consist of mesh routers and mesh clients, and could be independently implemented or integrated with other communication systems such as the conventional cellular systems. In addition, WMN are dynamic, self-organized, self-healed and self-configured network that enables quick deployment. They provide easy maintenance, low cost, high scalability and reliable service. WMN is an ad hoc network extension and is becoming an important mode complimentary to the infrastructure based wireless networks because they can enhance network capacity, connectivity and resilience. We can define a WMN as a network that has either a partial or full mesh topology. In practice, WMNs are characterized by static wireless relay nodes which provide a distributed infrastructure for client nodes over the partial mesh topology. As WMN are self-organized and self-configured networks, the nodes in the network automatically establish an ad hoc network and maintain the mesh connectivity [1].

Along with the routing capability for gateway/bridge functions existing in a conventional wireless router, a mesh router supports additional routing functions to provide a platform for mesh networking. Using multi-hop communications, the coverage can be extended by a mesh router with much lower transmission power requirements. To further enhance the adaptability of mesh networking, a mesh router is normally equipped with multiple wireless interfaces built on either the same or different wireless access technologies [1]. Mesh routers generally have minimal mobility and their purpose is basically the formation of mesh backbone for the mesh clients [1]. The gateway/bridge functionalities in mesh routers enable the integration of WMNs with various other networks. Wireless mesh routers enable conventional nodes equipped with wireless network interface cards (NICs) to connect directly to WMNs [1]. Ethernet can be used to access WMNs by connecting to wireless mesh routers when wireless NICs are not available. WMN caters to the need of the users to be always on line anywhere, anytime [12]. Instead of being another type of ad hoc networking, WMNs diversify and enhance the capabilities of ad hoc networks.

The devices like laptops, mobile phones, wireless mouse, wireless keyboards, PDA etc come under the category of mesh clients. Even though mesh clients can also work as a router, the hardware platform and software for them can be made simpler than those for mesh routers. For instance, communication protocols for mesh clients can be light-weight, as gateway or bridge functions are not needed by mesh clients. Only a single wireless interface is often needed in a mesh client [3].

In many ways WMNs have become preferable over MANETs, as they have advantages such as low installation costs, easy network maintenance, robustness, service coverage that can be relied on . Today, WMNs are a widely accepted technology in the traditional application areas of ad hoc networks, and they are also undergoing rapid commercialization application scenarios such as broadband home networking, community networking, building automation, high-speed metropolitan area networks, and enterprise networking etc .

Problem Statement

As the purpose of wireless mesh networks are that they are dynamically self- organized and self-configured wireless systems, and consisting of mesh clients and mesh routers, several issues exists which are not in other networks . The objective of this thesis is to evaluate proposed routing protocols for WMN based on performance. This evaluation is done through simulation. WMNs are becoming famous for their applicability too. So it was very much necessary to prove it using various scenarios in the simulation and compare the results based on above mentioned parameters.

Facilities required for proposed work

SIMULATION ENVIRONMENT

This chapter presents an overview of Network simulator ns-2 that I have used for simulation in this thesis. First section gives an introduction to the simulator and its environment and then discusses its architecture and usage process. Next the structure of mobile node is discussed. An introduction to mobility models used for simulation in this thesis and traffic generation process is discussed next. Final section of this chapter defines and explains the performance metrics that I have computed after simulation to evaluate the performance of routing protocols in WMN.

4.1 Network Simulator version 2

The Network Simulator Version 2 (ns-2) is a deterministic discrete event network simulator, initiated at the Lawrence Berkeley National Laboratory (LBNL) [39] through the DARPA funded Virtual InterNetwork Testbed (VINT) project. Although there are several different network simulators available today, ns-2 is one of the most common. It has support for both wired and wireless networks and can simulate several network protocols such as TCP, UDP, multicast routing, etc. Ns-2 differs from most of the others by being open source software, supplying the source code for free to anyone that wants it. The release of the source code helps users to create their own functions and subprograms, but also makes it easier to implement them into the ns-2 environment. In addition, many existing ad hoc routing protocols modules have already been implemented in ns-2 which includes AODV, DSR, DSDV, TORA and AOMDV. However, OLSR was not implemented in ns-2. It was necessary to acquire a compatible version of OLSR from the University of Murcia (Spain) website and install the necessary modules so that ns-2 can use OLSR protocol for network simulation.

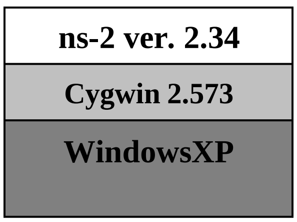

Figure-4.1 ns-2 on Windows XP

The standard ns-2 distribution runs on Linux. However, a package for running ns-2 on Windows, Cygwin (Linux Emulation for Windows) is available. In this mode, ns-2 runs in the Windows environment on top of Cygwin as shown in the Figure-4.1. The simulations performed (discussed in following sections) have been run in this environment.

4.1.1 Cygwin

Cygwin is a Linux-like environment for Windows. It consists of a DLL (cygwin1.dll), which acts as an emulation layer providing substantial POSIX (Portable Operating System Interface) system call functionality, and a collection of tools, which provide a Linux look and feel. The Cygwin DLL works with all x86 versions of Windows since Windows 95. The API follows the Single UNIX Specification as much as possible, and then Linux practice. Two other major differences between Cygwin and Linux are the C library (newlib instead of glibc) and default **/bin/sh**, which is **ash** on Cygwin but **bash** on most Linux distributions [40].

With Cygwin installed, users have access to many standard UNIX utilities. They can be used from one of the provided shells such as **bash** or from the Windows Command Prompt. Additionally, programmers may write Win32 console or GUI applications that make use of the standard Microsoft Win32 API and/or the Cygwin API. As a result, it is possible to easily port many significant UNIX programs without the need for extensive changes to the source code. This includes configuring and building most of the available GNU software (including the development tools included with the Cygwin distribution). Running bash with the development tools and user tools in place, Windows 9x and NT look like a flavor of UNIX from the perspective of the GNU configure mechanism [40]. Self-hosting was achieved as of the beta 17.1 release in October 1996. The entire Cygwin toolset was available as a monolithic install. In April 2000, the project announced a New Cygwin Net Release, which provided the native Win32 program setup.exe to install and upgrade each package separately. Since then, the Cygwin DLL and **setup.exe** have seen continuous development [40].

4.1.2 Operating System and Memory

NS-2 is both compatible for Linux and Window environment. Cygwin is required to be installed on the Windows system before installing the ns-2 software. We require a hard disk of around 40-45GB to store the simulation files. This is because of the fact that simulation of network of 30-60 nodes run for 200 seconds for various routing protocols could create NAM and trace files of about 100's of MB's. I performed simulations on a computer system with Intel Core-2 Duo processor and 2 GB of RAM loaded with Windows XP. Ns-2 has been found to run on configurations lower then this as well.

4.1.3 The NS-2 Structure

Ns-2 is made up of hundreds of smaller programs, separated to help the user sort through and find what he or she is looking for. Every separate protocol, as well as variations of the same, sometimes has separate files. Though some are simple, still are dependent on the parental class [39]. As shown in the simplified user's view of Figure-4.2, ns-2 is an Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network set-up (plumbing) module libraries.

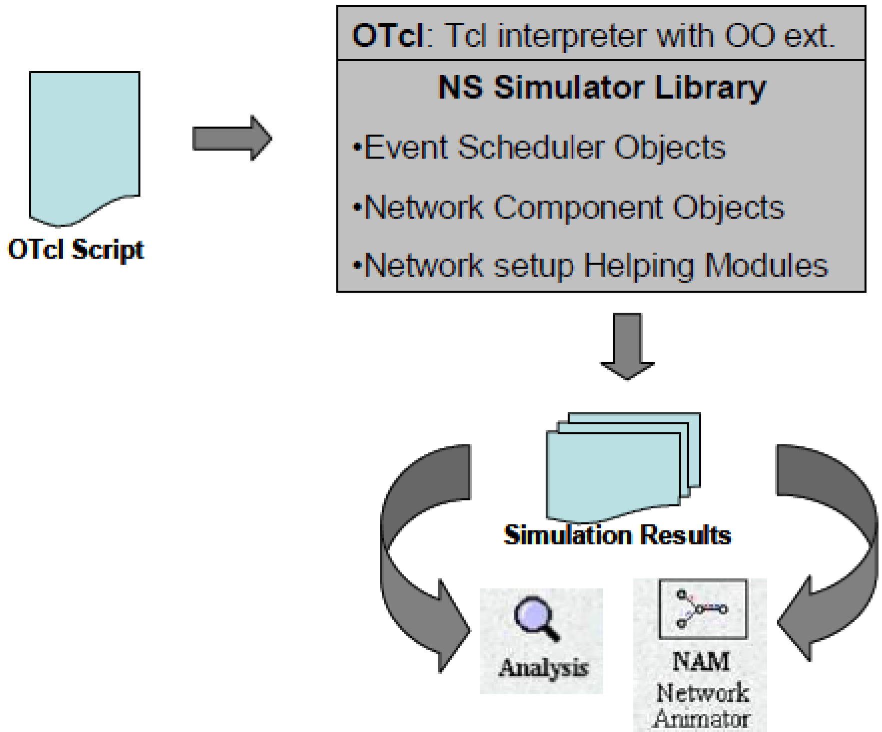

Figure-4.2 Simplified User's View of ns-2

To use ns-2, a user programs in the OTcl script language. An OTcl script initiates an event scheduler and set up the network topology using the network objects. It also tells traffic sources when to start/stop transmitting packets through the events scheduler. A user can add OTcl modules to ns-2 by writing a new object class in OTcl. These then have to be compiled together with the original source code.

Another major component of NS besides network objects is the event scheduler. An event in ns-2 is a packet ID that is unique for a packet with scheduled time and the pointer to an object that handles the event. The event scheduler in ns-2 organizes the simulation timer, fires events in the event queue and invokes network components in the simulation. Network components communicate with one another by passing packets. However, this does not consume actual simulation time. All the network components that need to spend some simulation time handling a packet (i.e. need a delay) use the event scheduler by issuing an event for the packet and waiting for the event to be fired to itself before doing further action handling the packet (Figure-4.3).

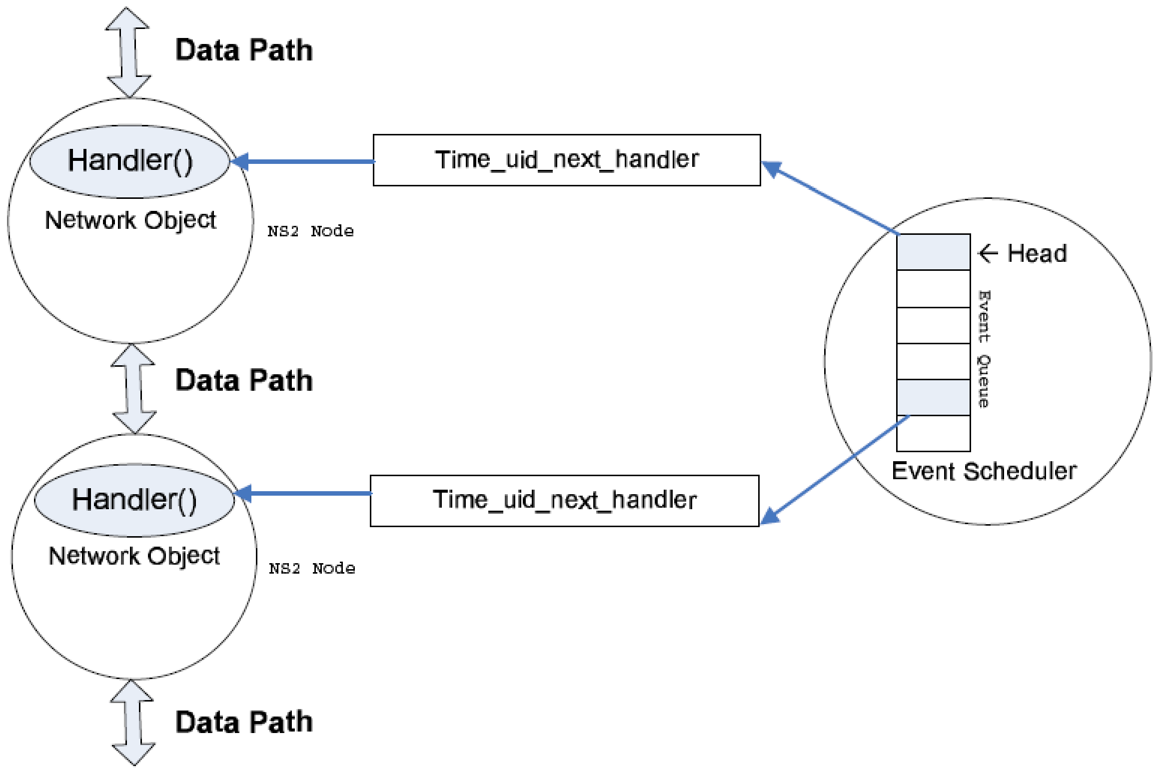

Figure-4.3 NS-2 Event Scheduler

NS-2 provides a split-programming model. That is the simulation kernel is implemented using C++, while the Tcl scripting language is used to express the definition, configuration and the control of the simulation (Figure-4.4). This split-programming approach has proven benefits over conventional programming methods.

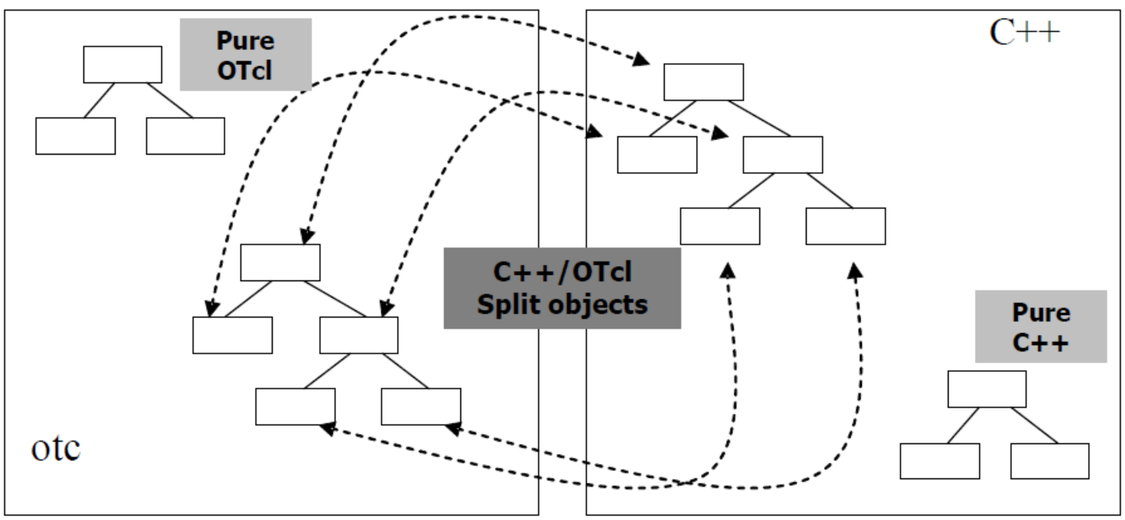

Figure-4.4 Split Programming Model

4.1.4 C++

C++ is the predominant programming language in ns-2. It is the language used for all the small programs that make up the ns-2 hierarchy. C++, being one of the most common programming languages and specially designed for object-oriented coding, was therefore a logical choice for what language to be used. This helps when the user wants to either understand the code or do some alterations to the code or want to write new protocols using existing ones.

4.1.5 OTcl

Object Tcl (OTcl) is object-oriented version of the command and syntax driven programming language called Tool Command Language (Tcl). This is the second of the two programming languages that ns-2 uses. OTcl is used as a front-end interpreter in ns-2 linking the script type language of Tcl to the C++ backbone of ns-2. Together these two different languages create a script controlled C++ environment. This helps when creating a simulation, simply writing a script that will be carried out when running the simulation. These scripts will be the recipe for a simulation and is needed to set the specifications of the simulation itself. Without a script properly defining a network topology as well as the data-rows, both type and location, nothing will happen. For a more in depth presentation of these scripts we can have a closer look at the introduction and related chapters in the ns-2 manual.

4.1.6 Wireless Support in ns-2

In ns-2, the Distributed Coordination Function (DCF) mode of IEEE 802.11 for wireless LANs is used as the MAC layer protocol. The radio model uses characteristics similar to a commercial radio interface, Lucent's WaveLAN [41]. WaveLAN is modeled as a shared-media radio with nominal bit rate of 2Mb/s and a nominal radio range of 250 meters. The signal propagation model combines both a free space propagation model and a two-ray ground reflection model.

4.1.7 NAM

The Network Animator (NAM) is a graphic tool used with ns-2. It requires a nam-trace file recorded during the simulation and then show a visual representation of the simulation. This gives the user the possibility to view the traffic, packet by packet as they move along the different links in the network. NAM offers the possibility of tracing a single packet during its travel and the possibility to move the nodes around for a user to draw up his network topology according to his own wishes. Since the simulation has already been performed there is no possibility for the user to change the links or any other aspect of the simulation except the representation. NAM is dependant on the existence of an X-server in order to be able to open a graphical window. Therefore there has to be a version of X running if NAM is to work.

4.1.8 Usage Process

The aim of this simulation tool is to allow researchers to study the extent of protocol interactions in the context of current and future network protocols. The bulk of the simulation tool is written in the C++ programming language. To write a simulation script, the user must use OTcl to define wireless mobile nodes in an enclosed network, the amount of traffic that is flowing, and which routing protocol is used. In addition, it is necessary to trace the mobility model used as well as the type of traffic at which level: routing, MAC or application. There are usually two types of output files: a trace file and NAM file that are created during simulation. Trace files contains the events traces that can be further processed to understand the performance of the network. A NAM file allows the user to visually appreciate the movement as well as the interactions of the mobile nodes. Figure-4.5 depicts the overall process of how a network simulation is conducted under NS2. Output files such as trace files have to be parsed to extract information. The parsing can be done using the awk command or Perl scripts. The results can be analyzed using Excel or Matlab or gnuplot to plot graphs.

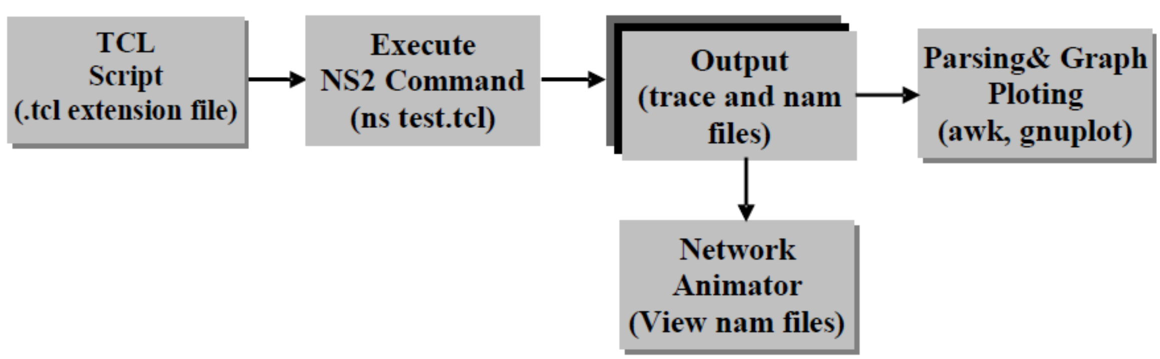

Figure-4.5 NS-2 Simulation Process

4.2 Mobile Node Model

A node is exactly what it sounds like, a node in the network. A node can be either an end connection or an intermediate point in the network. All agents and links must be connected to a node to work. There are also different kinds of nodes based on the kind of network that is to be simulated. The main types are node and mobile node, where node is used in most wired networks and the mobile node for wireless networks (ad hoc or mesh). The wireless networking node essentially consists of the MobileNode class at the core with additional supporting features as shown in Figure-4.6. It is derived from the basic Node class. MobileNode has with added functionalities like movement and the ability to transmit and receive on a channel that allows it to be used to create mobile, wireless simulation environments. The mobility features, including node movement, periodic position updates, and maintaining topology boundary is implemented in C++. However, other network components within MobileNode itself (like classifiers, dmux, LL, Mac, and Channel) have been implemented in OTcl. MobileNode consists of a network stack. The network stack for a mobile node consists of a link layer (LL), an Address Resolution Protocol (ARP) module connected to the LL, an interface priority queue (IFq), a media access control (MAC) layer, a network interface (netIF), all connected to a common wireless channel. Each mobile node makes use of a routing agent for the purpose of calculating routes to other nodes in the ad hoc network. An application such as TCP source packet or constant bit rate (CBR) packet is bound to a particular node and together with the routing agent; a path is determined to direct the data packet to its destination. This packet is passed onto the link layer, which also uses address resolution protocol (ARP) to obtain the neighbors' physical addresses, i.e., the MAC address. The packet is then queued until a positive signal is received from the MAC layer for transmission to the channel. Upon successful RTS/CTS signals at the MAC layer, the packet is delivered into the network interface. The packet is then duplicated and sent to all the network interfaces. Each network interface will provide the packet with receiving network interface information and then the propagation model is called upon.

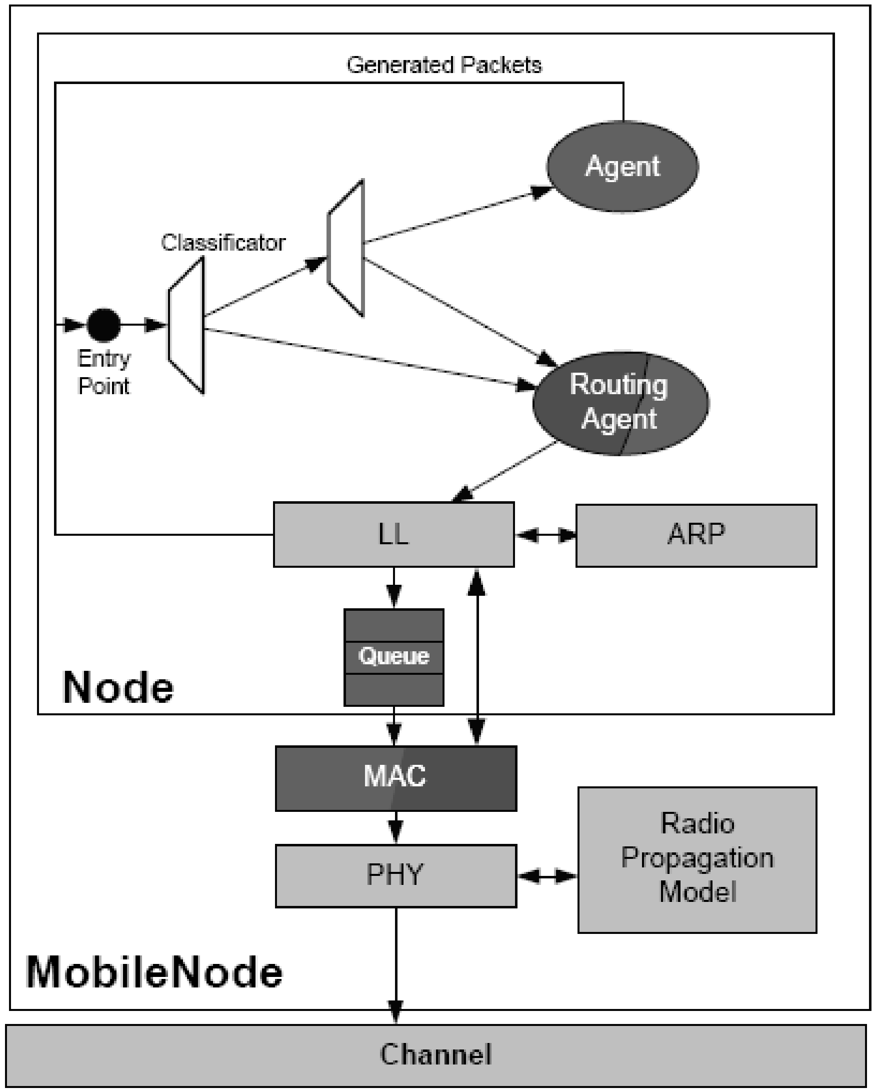

Figure-4.6 Mobile Node

Following are certain specifications of the Mobile node model in ns-2:

- 802.11 MAC Protocol: In ns-2, there are two MAC layer protocols implemented for mobile networks: 802.11 and TDMA.
- Radio Propagation Model: The radio propagation model uses Friss-space attenuation at near distances and an approximation to two-ray ground at far distances, which assumes specular reflection off a flat ground plane.
- Antenna: An omni-directional antenna having unity gain is used by a mobile node that broadcasts the packet in all directions.

- Network Interfaces: The Network Interface layer [42] serves as a hardware interface, which is used by a mobile node to access the channel. The wireless shared media interface is implemented as a sub-class WirelessPhy (wireless physical medium) of the Phy (general physical layer) Class. The interface stamps each transmitted packet with information related to the transmitting interface such as the transmission power and wavelength. This is used by the propagation model in receiving network interface to determine if the packet has minimum power to be received and/or captured and/or detected (carrier sensed) by the receiving node. The model approximates the Direct Sequence Spread Spectrum radio interface.
- Agents: An agent is the collective name for most of the protocols you can find in the transport layer. In the ns-2 manual they are defined as the endpoints where packets are created and consumed [42]. The agents in ns-2 are all connected to their parent class, simply named Agent. This is where their general behavior is set and the offspring classes are mostly based on some alterations to the inherent functions in the parent class. The modified functions will overwrite the old and thereby change the performance in order to simulate the wanted protocol.
- Routing Agents: All the packets from the source to the destination get passed through the address demultiplexer so that they could be forwarded to their respective destination agents. The mobile nodes also use a default-target in their address demultiplexer. In the event a target is not found for the destination in the classifier, when the destination of the packet is not the mobile node itself, the packets are handed over to the default target, which is the routing agent. The routing agent sends the packet to the next node.

4.3 Mobility Model

A mobility model specifies the movement pattern of the mobile nodes in an ad hoc or mesh network. The mobile nodes may move freely or their movement may be constrained. Mobility models I used in this thesis for simulation are discussed in this section.

4.3.1 Random Waypoint Mobility Model

In this mobility model each host is initially placed at a random position within the simulation area. As the simulation progresses, each host pauses at its current location for a determinable period called the pause time. Pause time is used to overcome abrupt stopping and starting in the random walk model. Upon expiry of this pause time, the node will arbitrary select a new location to move towards it at a randomly selected velocity between a minimum and maximum value, which are stated at the start of the scene generation. Every host will continue this type of behavior throughout the entire duration of the simulation. Using this model, the hosts appear to move randomly within a confined compound. The random waypoint model is selected for its simplicity. This simplistic modeling should be sufficient to capture the essence of the human mobility to make protocol evaluation academically meaningful. Taking a snapshot of a random number of people and observing their movement patterns in a chosen city area can make it possible to observe a certain state of randomness in their movement patterns.

4.7 Performance Metrics

Performance of routing algorithms and hence the performance of the WMNs can be evaluated based on the various information obtained from the trace files after simulation. The information can be the number of packets sent and received, the number of routing packets generated, number of packets dropped or forwarded etc. Following are the performance criteria that I have examined during my simulation study.

4.7.1 Packet Delivery Ratio (PDR)

The packet delivery ratio is expressed as the percentage of CBR data traffic that has been received by all destinations (sinks) over the total number of packets sent by all the sources within the period of simulation. The packet delivery ratio can be interpreted as the loss ratio that will be experienced at the routing layer which in turn has an impact on the overall throughput of what the network can support. It is a fundamental characterization of the performance of routing protocols.

4.7.2 Throughput

The rate at which the data is transferred from one node to another node in a communication network is known as throughput. The unit of throughput is bits/sec. Throughput is usually referred with a symbol λ. It is acceptable [44] if all the nodes in a network send data at a rate of $\lambda > 0$ bits/sec to the destination node.

4.7.3 Average End-to-end Delay (AED)

End-to-end delay is the time it takes for a packet to travel through the network from source to destination. The average end-to-end delay is the summation of all end-to-end delays divided by total data packets arrived at destination. End-to-end delay is an important routing performance metric since voice and video on-demand type of applications are especially dependent on low latency to perform well. End-to-end delay is to some extent dependent on PDR. That is because if fewer packets are delivered then the average is calculated from fewer samples. As the path length increases between source and destination, the probability that a packet will drop also increases. In networks with a low PDR, samples with short paths are favored and thus the delay will be low. Calculation of the average end-to-end delay includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times.

4.7.4 Routing Overhead (ROH)

The routing overhead is the total amount of control data packets sent by the routing protocol throughout the duration of the simulation. Each time a packet is forwarded over multiple hops, routing overhead is counted as many packets as there are hops. The amount of routing overhead is a significant factor to determine the efficiency of the routing protocol. Highly efficient routing protocols have lower routing overheads so as to maintain faster route convergence, and thereby, lower overall delay. Such protocols whose routing overheads are low will enable the protocol to scale better and consume less energy. If more control packets are sent by routing agents, the chance of collision for the transmission channels increases, and thus causes the delay of the application to increase indirectly.

4.7.5 Normalized Routing Load (NRL): Normalized routing load is the number of routing packets transmitted per data packet delivered to the destination. Each hop-wise transmission of a routing packet is counted as one transmission. This metric is also highly correlated with the number of route changes which occurred in the simulation. The PDR and average end-to-end delay metrics are the most important for best effort traffic. The routing overhead and the normalized routing load metrics evaluate the efficiency of the routing protocol. Highly efficient routing protocols have lower routing overhead so as to maintain faster route convergence, and thereby, lower overall delay.

References

[1] A Survey on Wireless Mesh Networks, Ian F. Akyildiz, Georgia Institute of Technology, Xudong Wang, Kiyon, Inc, *IEEE Radio Communications* September 2005 page s23-s80.Kapleer, accessed via the web: http://www.kapleer.com.

[2] Wireless Mesh Network Solution Brief, http://products.nortel.com/.

[3] ABI, State of the Art Analysis of Wireless Mesh Technologies 2008, T. Huovila, P. Lassilay, J. Manner, and A. Penttinen, University of Helsinki, Helsinki University of Technology.

[4] A comparison of MANETs and WMNs: Commercial feasibility of community wireless networks and MANETs, *ACM International Conference Proceeding Series, 2006*, Sahibzada Ali, Sahibzada Ali, Shoiab khan, Hamed Al- Raweshidy, Brunel university, west London.

[5] Wikipedia. 2008. http://en.wikipedia.org/wiki/Wireless_ad-hoc_network.

[6] Jochen Schiller. Mobile Communications. Pearson Education Asia, 2009.

[7] 802.11 Working Group of the LAN/MAN Committee, Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE P802.11s/D0.03, August 2006.

[8] Luo J. Zhang, Y. and H. Hu, editors. Wireless Mesh Networking: Architectures, Protocols and Standards. Auerbach Publications, 2007.

[9] Chlamtac I., Conti M., and Liu J. Mobile ad hoc networking: imperatives and challenges. 2003.

[10] Z.; Towsley-D Liu, B.; Liu. On the capacity of hybrid wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, volume 2, pages 1543 – 1552. IEEE, 30 March-3 April 2003.

[11] Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network (A Raniwala) *Appears in proceedings of IEEE Infocom '05*

[12] http://www.nortel.com/corporate/news/newsreleases.

[13] Akyildiz, I.F., Wang, X., and Wang, W., *Wireless mesh networks: a survey*. In *Computer Networks*, 2005. 47(4): p. 445-487.

[14] Tzu-Jane, T. and Ju-Wei, C. *IEEE 802.11 MAC protocol over wireless mesh networks: problems and perspectives*. in Proceedings of *19th International Conference on Advanced Information Networking and Applications*. 2005. Taipei, Taiwan: IEEE Comput. Soc.

[15] Groups Hope to Avoid Mesh Standard Mess, Greg Goth, IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922©2005 Published by the *IEEE Computer Society Vol. 6*, No.9; September 2005.

[16] Ho Ting Cheng, H.J.W.Z., *Distributed medium access control for wireless mesh networks.* In *Wireless Communications and mobile computing*, 2006. 6(6): p. 845-864.

[17] Institute of Electrical and Electronics Engineers, *Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TG*. 2006, Institute of Electrical and Electronics Engineers.

[18] Securing wireless mesh networks, Ben Salem, N.; Hubaux; *Wireless communications, IEEE*[see also IEEE Personal Communications, Volume 13, Issue 2, April 2006 Page(s):50–55.

[19] R. Songwu Lu; Bharghavan, V.; Srikant. Fair scheduling in wireless packet networks. In IEEE, editor, Networking, IEEE/ACM Transactions on, volume 7, pages 473 – 489, 1999.

[20] Zhang Yan, Zheng Jun, Hu Honglin. "*Security in Wireless Mesh Networks*".

[21] A novel channel assignment algorithm based on topology simplification in multi-radio wireless mesh networks, Leiming Xu;Yong Xiang; Meilin Shi *Performance, Computing, and Communications Conference*, 2006 IPCCC 2006 25th IEEE International Volume, Issue, 10-12 April 2006 Page(s): 8 pp.